**МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ УКРАЇНИ**

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кавун С. В.
Пилипенко А. А.
Ріпка Д. О.

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ У СИСТЕМІ КОНСОЛІДОВАНОЇ ІНФОРМАЦІЇ

Навчальний посібник

Харків. Вид. ХНЕУ, 2013

УДК 004.056(075.8)
ББК 32.973Я73
К12

Рецензенти: докт. екон. наук, професор, заступник директора з наукової роботи та міжнародних зв'язків Харківського інституту банківської справи Університету банківської справи НБУ України *Азаренкова Г. М.;* докт. екон. наук, професор, заступник директора Науково-дослідного центру індустріальних проблем розвитку НАН України *Іванов Ю. Б.;* докт. екон. наук, професор, зав. кафедри економічної кібернетики Харківського національного економічного університету *Клебанова Т. С.*

Рекомендовано до видання рішенням вченої ради Харківського національного економічного університету.

Протокол № 7 від 26.03.2012 р.

Авторський колектив: канд. техн. наук, доцент Кавун С. В. – розділи 7, 8, п. 9.1, п. 9.2, розділи 10, 11; докт. екон. наук, професор Пилипенко А. А. – розділ 6, п. 9.3 – 9.6; канд. екон. наук, доцент Ріпка Д. О.– розділи 1 – 5.

Кавун С. В.

К12 Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х. : Вид. ХНЕУ, 2013. – 364 с. (Укр. мов.)

Подано теоретичний і методичний матеріал із сучасних проблем інформаційної та економічної безпеки. Розглянуто методичні та наукові рішення щодо підвищення рівня знань студентів у сфері інформаційної та економічної безпеки в системі консолідованої інформації.

Рекомендовано для аспірантів, науковців і студентів, а також для фахівців із систем інформаційної та економічної безпеки.

ISBN

УДК 004.056(075.8)
ББК 32. 973Я73

Вступ

Розвиток нових інформаційних технологій і загальна комп'ютеризація призвели до того, що інформаційна та економічна безпека підприємств не тільки стає обов'язковою, вона ще й одна з характеристик системи консолідованої інформації. Існує досить великий клас систем консолідованої інформації, при розробці яких фактор безпеки відіграє першорядну роль (наприклад, банківські інформаційні системи, системи обліку персональних даних, системи аудиту фінансової та інших видів діяльності).

Практично за всіма визначеними світовою практикою пороговими значеннями показників економічної та інформаційної безпеки Україна подолала небезпечну межу. Показник зниження валового внутрішнього продукту (ВВП) щодо базового періоду (1990 р.) перевищує максимальне порогове значення у 2001 р. і становить 12,9 % [108]. Зниження обсягів виробництва має постійну тенденцію коливання біля критичної межі, низьке його фізичне зростання до базового періоду. Деформація галузевої структури виробництва характеризується зменшенням обсягу продукції галузей, які визначають ступінь науково-технічного та соціально-економічного розвитку країни.

Низький рівень стану інформаційної та економічної безпеки обумовлений неефективністю державного управління, його недостатньою зорієнтованістю на захист національних інтересів в економічній і соціальній сферах, а також непослідовністю та безсистемністю у здійсненні економічних реформ, недосконалістю національного законодавства щодо забезпечення економічної безпеки та ефективного управління економікою; недостатнім рівнем кваліфікації державних службовців із питань забезпечення національної безпеки; корупцією в управлінських структурах.

Негативні тенденції в економічній та інформаційної сфері національної безпеки та потреби їх подолання визначили актуальність і пріоритетність цього напряму наукових досліджень. Вітчизняні фахівці працюють над розв'язанням цих проблем. Серед них – Амітан В. Н., Амоша О. І., О. Барановський, І. Бінько, З. Варналій, О. Власюк, В. Геєць, Б. Губський, О. Ємельянов, М. Єрмошенко, Я. Жаліло, В. Мунтіян, Г. Пастернак-Таранушенко, С. Пірожков, А. Сухоруков, М. Чумаченко, В. Шле-

мко, О. Кириченко, С. Шкарлет, О. Ареф'єва, Т. Клебанова, Г. Козаченко, М. Куркин, Є. Олєйніков, О. Черняк, В. Пономаренко, О. Кизим, О. Раєвнева. Крім того, цим питанням займалися провідні російські вчені – Л. Канторович (лауреат Нобелевської премії у 1975 р.), В. Ярочкин [157; 156], О. Шаваєв, В. Шликов, Л. Абалкін, В. Мак-Мак, Д. Зегжда, А. Щеглов, А. Лукацкий, В. Сенчагов, П. Хорев [146], також закордонні автори – Ф. Модильяні (лауреат Нобелевської премії у 1985 р.), Ж. Дебре (лауреат Нобелевської премії у 1983 р.), Д. Канеман (лауреат Нобелевської премії у 2002 р.), С. Бармен, Р. Найт, Д. Дж. Прітті, Б. Хаттер, М. Пауер, Ф. Рейнхардт, І. Митрофф, Р. Манн, Р. Реддеуей, Б. Хант, Еппен Г. Д., К. Смоллмен, М. Стоун, М. Фентон-О'Криві та ін.

Активізація наукових досліджень із проблем інформаційної та економічної безпеки обумовила формування самостійного наукового напряму, який передбачає сполучення та взаємозв'язок двох підсистем державного управління – національної безпеки та економічної політики. Саме вирішенню цих питань і присвячене проведене наукове дослідження.

Основними завданнями в процесі проведення досліджень є: одержання знань з основоположних принципів побудови та функціонування систем консолідованої інформації; одержання знань про механізми забезпечення інформаційної та економічної безпеки, функціональні складові аудиторської та облікової інформації; підготовка до подальшого поглибленого вивчення спеціальних дисциплін; вироблення навичок самостійного вивчення різних систем консолідованої інформації та проведення їх порівняльного аналізу при забезпеченні інформаційної та економічної безпеки аудиторської та облікової інформації.

Економічну та інформаційну безпеку підприємства можна розглядати як практичне використання таких принципів сучасного менеджменту, як своєчасна реакція на зміни в зовнішньому середовищі, бачення підприємства, тобто чітке подання про те, що воно повинно собою представляти, а також одного з основних положень сучасної теорії управління – ситуаційного підходу до керування, який означає важливість швидкості й адекватності реакції, що забезпечують адаптацію підприємства до умов його існування. Звідси економічну та інформаційну безпеку підприємства слід розглядати як еволюційний розвиток ситуаційного підходу до керу-

вання. Економічна та інформаційна безпека викликають все більшу зацікавленість підприємств, які стикаються із труднощами при реалізації принципово нових підходів до керування підприємствами, при організації керування підприємством у ринкових умовах.

Компетенції, яких набувають після вивчення посібника:

здатність прогнозувати й критично оцінювати можливі напрями розвитку підприємства в умовах ризику та невизначеностей обліку та аудиту;

вміння розробляти плани обліку та аудиту з урахуванням небезпек та загроз його діяльності;

здатність визначати тактичні та оперативні плани обліку та аудиту через забезпечення відповідного рівня його економічної безпеки;

спроможність передбачати напрями розвитку зовнішнього середовища та пов'язані з цим загрози обліку та аудиту;

здатність передбачати й запобігати економічним ризикам;

вміння збирати та обробляти первинну інформацію, яка використовується під час прийняття управлінських рішень;

здатність володіти методами та засобами прийняття управлінських рішень в системі економічної безпеки підприємства;

базові уявлення про економічну інформацію і інформаційний обмін між суб'єктами та об'єктами підприємства;

здатність планувати й реалізовувати заходи щодо підвищення рівня автоматизації підприємства в сфері економічної та інформаційної безпеки.

У централізованій економіці економічна та інформаційна безпека підприємства забезпечувалася вертикально побудованими методами керування, які стали неприйнятними в умовах ринкової економіки, оскільки в ринковому середовищі з урахуванням її специфіки механізми безпеки розосереджуються за багатьма суб'єктами і напрямами економічної, фінансової, законодавчої, правоохоронної діяльності, коли організаційно починає зростати горизонтальна складова системи захисту [92]. Існуючі в цей час недоопрацювання з питання економічної та інформаційної безпеки підприємства в системі консолідованої інформації як у теорії, так і на практиці необхідно доопрацювати.

Розділ 1. Організація економічної безпеки підприємства

1. Поняття та основні категорії економічної безпеки

1.1. Поняття та мета економічної безпеки.

1.2. Об'єкт, предмет та суб'єкти економічної безпеки.

1.3. Чинники, що формують відповідний рівень економічної безпеки.

1.4. Загрози економічній безпеці та джерела їх виникнення.

1.5. Ризики як фактори, що несуть загрози економічній безпеці підприємства, та управління ними.

2. Індикатори та складові економічної безпеки підприємства

2.1. Структура економічної безпеки підприємства та поняття індикаторів економічної безпеки.

2.2. Складові економічної безпеки та управління ними.

2.3. Оцінка безпеки економічного простору функціонування підприємства.

3. Система економічної безпеки підприємства

3.1. Поняття та основні складові системи економічної безпеки підприємства.

3.2. Теоретичні положення з формування системи управління економічною безпекою підприємства.

3.3. Концепція безпеки підприємства.

3.4. Оцінка ефективності функціонування системи управління економічною безпекою підприємства.

4. Особливості діяльності служби безпеки підприємства

4.1. Служба безпеки як складова підприємства.

4.2. Структура та функції служби безпеки підприємства.

4.3. Організація праці та функції менеджера з економічної безпеки.

5. Недобросовісна конкуренція та захист комерційної таємниці підприємства

5.1. Сутність комерційної таємниці підприємства.

5.2. Обґрунтування переліку інформації, що становить комерційну таємницю.

5.3. Недобросовісна конкуренція та методи викрадення таємниць підприємства.

5.4. Економічне шпигунство та його особливості.

5.5. Налагодження охорони комерційної таємниці суб'єктів господарювання.

6. Ділова розвідка

6.1. Передумови виникнення та актуальність ділової розвідки.

6.2. Особливості ділової розвідки.

6.3. Роль ділової розвідки у бізнесі.

Розділ 1. Організація економічної безпеки підприємства

1. Поняття та основні категорії економічної безпеки

1.1. Поняття та мета економічної безпеки

Економічна, організаційна і політична системи суспільства безпосередньо залежать від його господарської діяльності. Незалежно від суб'єктів господарювання економічна безпека має багатоаспектне тлумачення. На будь-якому рівні ієрархії виробничо-господарської діяльності можуть виникати ситуації, які безпосередньо впливають на стан виробництва, часто незалежно від самого товаровиробника.

Поняття економічної безпеки підприємства можна розглядати з кількох позицій. З позиції різних агентів ринку, що взаємодіють з підприємством (споживачів, суміжників, податкових, кредитних органів і та ін.), оцінка має дати відповідь на запитання щодо надійності підприємства як партнера в економічних відносинах і доцільності продовження цих відносин. У цьому разі можна визначити, що економічна безпека підприємства є комплексним відображенням ступеня надійності підприємства як партнера у виробничих, фінансових, комерційних та інших економічних відносинах за певний проміжок часу.

З позиції самого підприємства оцінка економічної безпеки полягає у визначенні рівня захищеності його потенціалу (виробничо-технічного, фінансового, соціального та ін.) і тенденцій його зміни. При цьому під економічною безпекою підприємства слід розуміти захищеність його потенціалу (виробничого, організаційно-технічного, фінансово-економічного, соціального) від негативної дії зовнішніх і внутрішніх чинників, прямих або непрямих економічних загроз, а також здатність суб'єкта до відтворення.

Рівень економічної безпеки підприємства залежить від того, наскільки ефективно його керівництво та фахівці зможуть уникнути можливих загроз і ліквідувати шкідливі наслідки певних негативних складових зовнішнього та внутрішнього середовищ.

Отже, економічна безпека – це стан і здатність економічної системи протистояти небезпеці руйнування її оргструктури і статусу, а також пе-

решкодам у досягненні мети розвитку. Її можна окреслити як стан підприємства в межах граничних значень і здатність протидіяти загрозам та забезпечувати реалізацію економічних інтересів.

Економічну безпеку організації слід розглядати як стан і властивість соціально-економічної системи та її функцію.

Стан безпеки організації можна визначити через відповідні критерії і показники (індикатори). Вони сигналізують, з одного боку, про зону безпеки, а з другого – про розвиток небезпеки внаслідок реалізації загрози.

Безпека як функція (діяльність) організації передбачає виконання суб'єктами і силами безпеки конкретних видів діяльності, спрямованих на протидію, тобто на запобігання загрозам і припинення їх [47, с. 11–12].

Джерелами негативних впливів на економічну безпеку підприємства можуть бути:

1) свідомі чи несвідомі дії окремих посадових осіб і суб'єктів господарювання (органів державної влади, міжнародних організацій, підприємств-конкурентів);

2) збіг об'єктивних обставин (стан фінансової кон'юнктури на ринках певного підприємства, наукові відкриття і технологічні розробки, форс-мажорні обставини тощо). Залежно від суб'єктної зумовленості негативні впливи на економічну безпеку можуть бути об'єктивними і суб'єктивними. Об'єктивними вважаються негативні впливи, які виникають не з волі конкретного підприємства або його окремих працівників. Суб 'єктивпі впливи можливі внаслідок неефективної роботи підприємства в цілому або окремих його працівників (передовсім керівників і функціональних менеджерів) [47, с. 12].

Головна мета економічної безпеки підприємства полягає у тому, щоб гарантувати його стабільне й максимально ефективне функціонування тепер та високий потенціал розвитку в майбутньому.

Основною функціональною метою економічної безпеки є:

забезпечення високої фінансової ефективності роботи, фінансової стабільності та незалежності підприємства;

забезпечення технологічної незалежності та досягнення високої конкурентоспроможності того чи того суб'єкта господарювання;

досягнення високої ефективності менеджменту, оптимальної та ефективної організаційної структури управління підприємством;

досягнення високого рівня кваліфікації персоналу та його інтелектуального потенціалу, належної ефективності корпоративної діяльності;

мінімізація руйнівного впливу результатів виробничо-господарської діяльності на стан навколишнього середовища;

якісна правова захищеність усіх аспектів діяльності підприємства;

забезпечення захисту інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів підприємства та відділів організації;

ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів [23, с. 7–8; 47, с. 11–12].

Зазначені функціональні завдання зумовлюють формування необхідних структуроутворюючих елементів і загальної схеми організації економічної безпеки.

Основними заходами безпеки є загальні та спеціальні. Загальні – запобігання можливим загрозам розроблення і дотриманням нормативів безпеки (здійснює управлінський персонал); спеціальні – припинення загрози конфіденційними методами і методами роботи в надзвичайних ситуаціях (здійснюють працівники).

Основною метою загальних заходів безпеки є запобігання виникненню можливих загроз та їх здійснення розробленням і дотриманням так званих нормативів безпеки, починаючи з режиму і закінчуючи регламентацією й мотивацією поведінки працівників організації. У розробленні й виконанні загальних заходів економічної безпеки беруть участь керівники різних рівнів управління та структурних підрозділів, управлінці й рядові працівники, для яких цей вид діяльності передбачений у посадових обов'язках або є складовою їх роботи, але не є їх основною діяльністю.

Основною метою спеціальних заходів безпеки є припинення дії загрози на будь-якій стадії її реалізації конфіденційними методами та методами роботи в надзвичайних ситуаціях. Реалізацією спеціальних заходів безпеки займаються працівники, для яких це є предметом діяльності і основною роботою [47, с. 16].

1.2. Об'єкт, предмет та суб'єкти економічної безпеки

Об'єкт і суб'єкт системи забезпечення економічної безпеки підприємництва тісно взаємопов'язані. Об'єктом системи виступає стабільний економічний стан суб'єкта підприємницької діяльності в поточний і перспективний періоди. Конкретними ж об'єктами захисту виступають ресурси: фінансові, матеріальні, інформаційні, кадрові. Суб'єкт системи гаран-

тування економічної безпеки підприємництва має складніший характер, оскільки його діяльність зумовлюється не тільки особливостями і характеристиками об'єкта, а й специфічними умовами зовнішнього середовища суб'єкта підприємницької діяльності. Виходячи з цього, можна виділити дві групи суб'єктів, що гарантують економічну безпеку підприємництва: зовнішні і внутрішні.

До зовнішніх суб'єктів належать органи законодавчої, виконавчої і судової влади, покликані гарантувати безпеку всіх без винятку законослухняних учасників підприємницьких відносин, причому діяльність цих органів не можуть контролювати самі підприємці. Ці органи формують законодавчу основу функціонування і захисту підприємницької діяльності в різних її аспектах і забезпечують її виконання.

До внутрішніх суб'єктів належать особи, що безпосередньо здійснюють діяльність із захисту економічної безпеки певного суб'єкта підприємництва. Суб'єктами можуть виступати: працівники власної служби безпеки фірми (підприємства) та запрошені працівники із спеціалізованих фірм, що надають послуги із захисту підприємницької діяльності [47, с. 87–88].

1.3. Чинники, що формують відповідний рівень економічної безпеки

Гарантування економічної безпеки передбачає виокремлення, аналіз і оцінку існуючих загроз з кожної функціональної складової та опрацювання на їх основі системи протидійних і застережних заходів.

Чинники, що формують відповідний рівень економічної безпеки підприємства, різноманітні і в кожній галузі виробництва мають свою специфіку. Однак є загальні, типові чинники, що впливають на рівень економічної безпеки підприємства незалежно від форм власності та галузі виробництва, а саме:

1. Безпосередні чинники виробництва – основні чинники, які безпосередньо забезпечують діяльність виробництва. До них належать: безпосереднє розміщення підприємства (територія); наявні природні ресурси та умови їх розміщення на цій території, доступність використання та якісні показники; наявність трудових ресурсів, їх освітньо-кваліфікаційний рівень; наявна виробнича інфраструктура, можливий обсяг її використання; соціально-економічна інфраструктура і рівень матеріального достатку населення.

2. Стабільний попит на продукцію – чинник, який також відіграє важливу роль у рівномірному розвитку виробництва. Він охоплює: укладені довготермінові контракти на реалізацію продукції з її споживачами; рівень конкурентоспроможності продукції, що виробляється; якісно-гарантійні показники виробів; обґрунтовані прогнози щодо стабільності ринку певного виду продукції; державне та регіональне замовлення на виготовлену продукцію.

3. Надійність постачальників, передусім тих, що забезпечують постачання основної сировини і матеріалів. Для цього потрібно: мати довготермінові договори на поставку необхідної сировини і матеріалів, враховуючи терміни постачання та їх якісні показники; знати можливості постачальників і не допускати монопольності в їх поставках, для цього, як правило, потрібно мати 3 – 4 і більше постачальників сировини та матеріалів, щоб була гарантія стабільної цінової політики щодо сировини, матеріалів та інших комплектуючих.

4. Зовнішня конкуренція на продукцію, призначену на експорт. Ця продукція має: відповідати міжнародним стандартам; за якісними показниками і сервісним обслуговуванням бути конкурентоспроможною; мати обґрунтовану та прогнозовану перспективу; бути конкурентоспроможною щодо продукції, яка імпортується в нашу країну, з метою скорочення ввезення в Україну продукції, яку можуть виготовляти вітчизняні підприємства.

5. Державне економічне регулювання діяльності підприємства, яке полягає: у захисті власного товаровиробника незалежно від форм власності на засоби виробництва; регулюванні державної податкової політики; сприянні виробництву, враховуючи економічні, територіальні та інші аспекти; сприянні виробництву продукції, яка ввозиться як критичний імпорт; державному замовленні на товари, які фінансуються за рахунок бюджету і скорочення імпорту на ці товари.

6. Надійний захист комерційної таємниці. Держава має гарантувати таємницю на науково-технічні досягнення, розроблення нових технологій, інтелектуальну власність, ноу-хау, в тому числі й комерційні таємниці.

7. Компетентність керівництва підприємства. Найважливіші чинники, які можуть найбільш активно впливати на рівень економічної безпеки підприємства, – це високий професіоналізм керівництва і команди його менеджерів (висококваліфіковані кадри; система їх підготовки і форми навчання; створення для них відповідних виробничих і соціально-економічних умов).

Є ще й інші чинники економічної безпеки підприємства, які не пов'язані з безпосередньою виробничою діяльністю, але істотно впливають на стан виробництва. Вони пов'язані з поведінкою окремих людей, їх мораллю, духовністю (розкрадання, шахрайство, обдурювання, убивство тощо) [47, с. 14–16].

Усі перелічені чинники потрібно реалізовувати відповідно до чинного законодавства, спрямовувати їх на здійснення виробничої стратегії, досягнення належного рівня економічної безпеки кожного суб'єкта господарювання.

1.4. Загрози економічній безпеці та джерела їх виникнення

Загрози економічній безпеці – це дія дестабілізуючих природних факторів і/або суб'єктивних, пов'язаних з недобросовісною конкуренцією та порушенням законів і норм, що може спричинити потенційні або реальні втрати для організації.

Види загроз економічній безпеці підприємства [49, с. 16]:

за місцем виникнення: внутрішні; зовнішні;

за природою виникнення: політичні; кримінальні; конкурентні; контрагентні;

за ймовірністю виникнення: явні; приховані;

за наслідками: загальні; локальні;

за відношенням до людської діяльності: об'єктивні (зумовлені стихійними природними явищами: землетруси, повені тощо); суб'єктивні (зумовлені діяльністю людини);

за об'єктами посягань: інформація; матеріальні і нематеріальні активи; персонал; ділова репутація;

за можливістю прогнозування: прогнозовані; непрогнозовані;

за ймовірністю настання: катастрофічні; значні; незначні;

за сферами виникнення: економічні; фізичні; психологічно-інформаційні.

Усі чинники ризику, небезпеки і загроз можуть бути згруповані за різними класифікаційними ознаками. Так, за можливістю їх прогнозування слід виділити небезпеки або загрози, які можна передбачати, і непередбачувані. До передбачуваних належать ті, котрі, як правило, виникають у певних умовах, тобто відомі з досвіду господарської діяльності, своєчасно виявлені й узагальнені економічною наукою.

Небезпеки і загрози економічній безпеці підприємства залежно від джерела виникнення поділяють на об'єктивні і суб'єктивні. Об'єктивні виникають без участі й без волі підприємства або його службовців і не залежать від ухвалених рішень, дій менеджера. Це стан фінансової кон'юнктури, наукові відкриття, форс-мажорні обставини і та ін. Їх потрібно розпізнавати і обов'язково враховувати в управлінських рішеннях. Суб'єктивні загрози зумовлені умисними або ненавмисними діями людей, різних органів і організацій, зокрема державних і міжнародних підприємств-конкурентів. Тому запобігання їм багато в чому пов'язане з дією на суб'єктів економічних відносин.

За можливістю запобігання виділяють чинники форс-мажорні і нефорс-мажорні. Форс-мажорні вирізняються непереборною дією (війни, катастрофи, надзвичайні лиха, які примушують вирішувати і діяти всупереч наміру). Нефорс-мажорним можна запобігти своєчасними і правильними діями. За вірогідністю настання всі деструктивні чинники (поява зони ризику, виклик, небезпека, загроза) можна поділити на явні (що реально існують), видимі й латентні (приховані, ретельно замасковані, такі, які важко виявити). Вони можуть виявитися раптово. Тому у разі їх виникнення потрібно вжити термінових заходів, докладати додаткових зусиль, використовувати додаткові засоби.

Небезпеки і загрози можна також класифікувати за об'єктами посягання (персонал, майно, інформація, технології, ділове реноме тощо). За природою виникнення можна виокремити небезпеки: політичні, економічні, техногенні, правові, кримінальні, екологічні, конкурентні, контрагентські та ін.

За обсягом втрат або збитків, до яких може призвести деструктивний чинник, небезпеки і загрози можна поділити на зухвалі труднощі, значні й катастрофічні; за ступенем вірогідності – неймовірні, маловірогідні, вірогідні, вельми вірогідні, цілком вірогідні. Деякі науковці розрізняють загрози за ознакою віддаленості їх за часом: безпосередня, близька (до 1 року), далека (понад 1 рік) і в просторі: на території підприємства; на території, прилеглій до підприємства; на території регіону, країни; на зарубіжній території.

Найбільш поширена в науці класифікація небезпек за сферою їх виникнення. За цією ознакою розрізняють внутрішні і зовнішні небезпеки. Зовнішні небезпеки і загрози виникають за межами підприємства, не пов'язані з його виробничою діяльністю. Як правило, це така зміна на-

вколишнього середовища, яка може завдати підприємству збитків. Внутрішні чинники пов'язані з господарською діяльністю підприємства, його персоналу. Вони зумовлені процесами, що виникають у виробництві й під час реалізації продукції і можуть вплинути на результати бізнесу. Найбільш значними з них є: якість планування і ухвалення рішень, дотримання технології, організація праці і робота з персоналом, фінансова політика підприємства, дисципліна та ін. [47, с. 16–17].

Як внутрішніх, так і зовнішніх чинників ризику багато. Це зумовлено передусім тією різноманітністю зв'язків і відносин, в які обов'язково вступає підприємство. При здійсненні матеріальних, фінансових, інформаційних, кадрових та інших зв'язків відбуваються обмін, споживання і переміщення сировини, матеріалів, комплектуючих, машин, устаткування, інвестицій, технологій, грошових коштів та ін. Усі ці зв'язки та відносини виникають у конкретних політичних, соціально-економічних, природно-кліматичних та інших умовах, які склалися як у масштабах усієї країни, так і на рівні певного регіону. Саме конкретна ситуація в тому чи іншому населеному пункті, регіоні, де діє підприємство, може істотно впливати на результати господарської діяльності.

Чинниками, що впливають на результати господарської діяльності, можуть бути: стан підприємницького середовища, наявність місцевих сировинних і енергетичних ресурсів, розвиток транспортних та інших комунікацій, наповнюваність ринку, стан конкурентів, наявність вільних трудових ресурсів, рівень їх професійної підготовленості, рівень соціальної та політичної напруженості, орієнтування населення на продуктивну працю, рівень життя населення, його платоспроможність; криміналізація господарського життя (корумпованість чиновників, рекет, економічна злочинність) та ін. Усі зовнішні чинники, що впливають на економічну безпеку підприємства, можна згрупувати, виділивши: політичні, соціально-економічні, екологічні, науково-технічні, технологічні, юридичні, природно-кліматичні, демографічні, криміналістичні та ін.

Під впливом навколишнього середовища, різних чинників може виникнути багато зовнішніх небезпек і загроз економічній безпеці підприємства. До них належать: несприятливі зміни політичної ситуації; макроекономічні потрясіння (кризи, порушення виробничих зв'язків, інфляція, втрата ринків сировини, матеріалів, енергоносіїв, товарів); зміна законодавства, що впливає на умови господарської діяльності (податкового, відносин власності, договірного тощо); нерозвиненість інфраструктури ри-

нку; протиправні дії кримінальних структур; використання недобросовісної конкуренції; промислово-економічне шпигунство; моральні (психологічні) загрози, залякування, шантаж і фізична, небезпечна для життя дія на працівників та їх сім'ї (убивства, викрадення, побиття); розкрадання матеріальних засобів; протиправні дії конкурентів, їх прагнення оволодіти контрольним пакетом акцій; зараження комп'ютерних програм різними вірусами; протизаконні фінансові операції; надзвичайні ситуації природного і технічного характеру; несанкціонований доступ конкурентів до конфіденційної інформації, складова комерційної таємниці; крадіжки грошових коштів і цінностей; шахрайство; пошкодження будівель, приміщень і та ін.

Аналіз численних зовнішніх небезпек і загроз, напрямів та об'єктів їх дії, можливих наслідків для бізнесу пов'язаний із тривалими дослідженнями. Незважаючи на це, кожне підприємство і передусім менеджери з бізнесу, виходячи з конкретної ситуації, у якій перебуває господарюючий суб'єкт, повинні визначити (спрогнозувати) найбільш значуще (небезпечне) з них і виробити систему заходів щодо їх своєчасного виявлення, ослаблення їх впливу, запобігання їм.

Внутрішні небезпеки і загрози економічній безпеці бізнесу виникають безпосередньо у сфері господарської діяльності підприємства. До основних чинників ризику можна віднести: недостатній рівень дисципліни; протиправні дії працівників; порушення режиму збереження конфіденційної інформації; вибір ненадійних партнерів та інвесторів; відтік кваліфікованих кадрів, неправильна оцінка їх кваліфікації, їх низька компетентність; недостатня патентна захищеність; аварії, пожежі, вибухи; перебої в енерго-, водо-, теплопостачанні; вихід із ладу обчислювальної техніки; смерть провідних фахівців і керівників; залежність деяких керівників від кримінального світу; низький освітній рівень керівників; істотні упущення як у тактичному, так і в стратегічному плануванні, пов'язані насамперед із вибором мети, неправильною оцінкою можливостей підприємства, помилками у прогнозуванні змін зовнішнього середовища.

Виявлення та ідентифікація чинників ризику, небезпек і загроз – одне з найважливіших завдань гарантування економічної безпеки.

Економічні загрози – правова невизначеність економічних відносин; обмеження з боку держави можливостей економічного зростання; корупція; примушування виробників продавати продукцію визначеним споживачам; примушування покупців придбавати товари і послуги у визначе-

них виробників і продавців; заборона реалізувати товар з одного регіону в інший або за кордон; надання окремим фірмам переваг у конкуренції з іншими підприємствами; обмеження доступу на ринок за допомогою монопольної змови фірми-конкурента з іншими фірмами-монополістами; дискримінація з боку фірм-монополістів у наданні послуг, продажу монопольних товарів, а також щодо цін на послуги і товари; шахрайство з боку фірм-конкурентів (у тому числі й у змові з працівниками фірми); привласнення і розтрачання майна; підроблення продукції, істотні порушення договірних відносин партнерами.

Фізичні загрози – крадіжки, вимагання, грабіж, розбій; виведення із ладу обладнання, знищення та пошкодження майна, стихійні лиха, аварії, катастрофи й теракти.

Психологічно-інформаційні загрози – економічне шпигунство; розголошення або неправомірне використання інформації; дискредитація на ринку; соціальні конфлікти навколо або всередині організації, привласнення товарних знаків фірми конкурентом.

Основними загрозами безпеки особи (персоналу) організації є такі:

вбивства звичайні або такі, що супроводжуються насильством, знущанням, тортурами;

викрадення працівників і загрози викрадення членів їх сімей, близьких родичів;

психологічний терор, загрози, залякування, шантаж, здирництво;

грабежі з метою оволодіння грошовими коштами, цінностями, документами, майном;

інші смертельні розправи з використанням отруйних речовин і "ліків", що викликають тривалі й болісні захворювання;

знищення під виглядом нещасного випадку (аварії, катастрофи тощо).

Злочинні посягання стосовно матеріальних цінностей (продукції), приміщень (зокрема житлових), будівель та інших ресурсів виявляються у вигляді:

незаконного ознайомлення з конструкцією, дизайном, виконанням;

підроблення продукції;

крадіжок;

промислового шпигунства;

шахрайства;

знищення різними способами (вибух, підпал, обстріл та ін.).

До зовнішніх загроз і дестабілізуючих чинників можна віднести протиправну діяльність кримінальних структур, конкурентів, фірми і приватних осіб, що займаються промисловим шпигунством або шахрайством; неспроможних ділових партнерів, раніше звільнених за різні провини працівників підприємства; правопорушення з боку корумпованих елементів з числа представників контролюючих і правоохоронних органів.

До внутрішніх загроз і дестабілізуючих чинників належать: дії або бездіяльність (умисні й ненавмисні) працівників підприємства, що суперечать інтересам його комерційної діяльності, наслідком яких можуть бути завдані компанії економічні збитки, витік або втрата інформаційних ресурсів (зокрема відомостей, складових комерційної таємниці і/або конфіденційної інформації), підрив її ділового іміджу в бізнес-колах, виникнення проблем у взаєминах з реальними і потенційними партнерами (аж до втрати важливих контрактів), конфліктних ситуацій з представниками кримінального середовища, конкурентами, контролюючими і правоохоронними органами, виробничий травматизм або загибель персоналу тощо.

Мета протиправних дій стосовно продукції:

відвертий терор;

завдання серйозного морального і матеріального збитку;

порушення на тривалий час нормального функціонування; здирство значних сум грошей або яких-небудь пільг перед лицем терористичної загрози.

До об’єктів, предметів захисту від потенційних загроз і протиправних посягань належать:

персонал (керівні працівники, виробничий персонал, що володіє інформацією, яка становить комерційну таємницю, працівники зовнішніх служб та інший "вразливий" персонал);

грошові кошти (валюта, коштовності, фінансові документи та ін.);

матеріальні засоби (будівлі, споруди, сховища, устаткування, транспорт);

інформаційні ресурси з обмеженим доступом, що становлять службову і комерційну таємницю, та інша конфіденційна інформація на паперових, магнітних, оптичних носіях, інформаційні масиви і бази даних, програмне забезпечення, інформативні фізичні поля різного характеру;

засоби і системи інформатизації (автоматизовані системи і обчислювальні мережі різного рівня й призначення, лінії телеграфного, теле-

фонного, факсимільного, пейджингового, радіо- і космічного зв'язку, технічні засоби передачі інформації, допоміжні засоби і системи);

технічні засоби і системи охорони і захисту матеріальних та інформаційних ресурсів.

У сфері бізнесу постійно існують потенційні та реальні загрози з боку суб'єктів протиправних дій.

Джерелами зовнішніх загроз можуть бути:

кримінальні структури;

промислове шпигунство; фірми-розвідники;

конкуренти (прямі і непрямі);

корумповані представники органів влади, правоохоронних органів, контролюючих органів, засобів масової інформації;

стихійні лиха, аварії й катастрофи тощо. Джерелами внутрішніх загроз можуть виступати:

керівники організації;

менеджери середньої ланки;

працівники фірми;

працівники служби безпеки.

Організована злочинність – співтовариства "злодіїв у законі", що не мають аналогів у світовій кримінальній практиці, банд, угруповань, організованих груп. Основними ознаками організованих злочинних угруповань є:

наявність матеріальної і фінансової бази;

колегіальний орган управління – "рада";

статут організації у вигляді неформальних норм поведінки, традицій, законів, санкцій за їх порушення;

функціонально-ієрархічна система побудови організації;

наявність інформаційних баз корумпованих чиновників, а також об'єктивної інформації про стан справ в органах влади і управління, особливо в правоохоронній системі, банках, фірмах та інших підприємницьких структурах, русі товару, кон'юнктурі ринку, цінах на наркотики і та ін.;

наявність "своїх" людей в органах влади, судовій і правоохоронній системах;

специфічна "мовно-понятійна" система, яка включає жаргон, особливо у письмовій мові.

Випадкові (тимчасові) злочинні групи виникають зазвичай спонтанно або для скоєння одного злочину. Вони нестійкі в часі і не мають суворо регламентованих систем взаємодії і підлеглості.

Злочинці-одинаки – кримінальні елементи, котрі, як правило, діють індивідуально, а якщо мають спільників, то використовують їх або "втемну", або не інформуючи в повному обсязі про свої злочинні наміри. Злочинцями-одинаками можуть бути як особи з кримінальним минулим, так і злочинці, що зважилися на здійснення злочину під впливом несприятливих обставин.

На ринку послуг з'явилося багато фірм, що надають клієнтам такі послуги, як несанкціоноване проникнення в чужі бази даних, прослуховування телефонних розмов, розкрадання документів, що містять комерційну таємницю, і та ін.

Конкуренти – фірми, компанії та інші організації, які:

займаються аналогічною діяльністю;

претендують на використання тих самих приміщень, устаткування, сфери виробництва;

використовують одні й ті самі комунікації;

відчувають потребу у фахівцях, що працюють у банку, фірмі.

Конкуренція зазвичай виражається у таких формах, як суперництво, протиборство. Суперництво припускає цивілізовану боротьбу між компаніями або групами компаній за споживача, постачальника, за вигідні умови кредитування, за голоси виборців. За протиборства перевага віддається таким формам недобросовісної конкуренції, які дають змогу знищити конкурента або завдати йому серйозного збитку. При цьому найбільш популярними прийомами і методами є: дискредитація конкурента і його продукції в очах споживачів, партнерів, кредитних організацій; шкідництво; диверсії (підпали, вибухи); захоплення заручників; шантаж; убивство підприємців. До подібних акцій конкуренти вдаються, використовуючи послуги кримінальних структур або фірм, що займаються промисловим шпигунством [47, с. 17–23].

1.5. Ризики як фактори, що несуть загрози економічній безпеці підприємства, та управління ними

Ризик – це фінансова категорія. Тому на ступінь і величину ризику можна впливати через фінансовий механізм. Основою ризик-менеджменту є цілеспрямований пошук і організація роботи зі зниження ступеня ризику, мистецтво отримання і збільшення доходу в невизначеній господарській ситуації. Кінцева мета ризик-менеджменту відповідає

цільовій функції підприємництва – отримання найбільшого прибутку при оптимальному, прийнятному для підприємця співвідношенні прибутку та ризику.

Ризик-менеджмент є системою управління ризиком і фінансовими стосунками, що виникають у процесі цього управління. Під стратегією управління розуміються напрям і спосіб використання засобів для досягнення поставленої мети. Стратегія дозволяє сконцентрувати зусилля на оптимальних варіантах рішення, відкинувши решту всіх варіантів. Після досягнення поставленої мети стратегія як напрям припиняє своє існування. Нові цілі визначають характер нової стратегії.

Тактика – це конкретні методи і прийоми для досягнення поставленої мети в конкретних умовах. Завданням тактики управління є вибір найбільш оптимального рішення і найбільш прийнятних у цій ситуації методів і прийомів управління.

Інформаційне забезпечення функціонування ризик-менеджменту складається з різного роду і виду інформації: економічної, комерційної, фінансової тощо. Ця інформація включає обізнаність про вірогідність того або іншого страхового випадку, наявність і величину попиту на товари, на капітал, фінансову стійкість і платоспроможність клієнтів, партнерів, конкурентів, тощо. Той, хто володіє інформацією, володіє ринком. Багато видів інформації часто складають предмет комерційної таємниці. Наявність у фінансового менеджера надійної ділової інформації дозволяє йому швидко ухвалювати фінансові і комерційні рішення, впливає на правильність таких рішень, що, природно, веде до зниження втрат і збільшення прибутку [143].

Ризики та відповідні їм втрати відрізняються залежно від специфіки бізнесу. Втрати в комерційному підприємництві можуть мати місце у зв’язку з тим, що відбулося:

1. Несприятлива зміна (підвищення) закупівельної ціни товару в процесі здійснення підприємницького проекту і не блоковане умовами договору про закупівлю приводить до вірогідних втрат (DD), що визначаються за формулою:

$$DD = Про \times Dц, \qquad (1.1)$$

де Про – обсяг закупівель товару у фізичному вимірюванні;

Dц – вірогідне підвищення закупівельної ціни.

2. Непередбачене зниження обсягу закупівлі порівняно з намічени-ми викликає зменшення обсягу реалізації, тобто масштабу всієї операції. Втрата прибутку (доходу) обчислюється як добуток зниження обсягу закупівлі та величини прибутку (доходу), що приходиться на одиницю обсягу реалізації товару.

Слід ураховувати, що зменшення обсягу закупівлі та реалізації може супроводжуватися зниженням витрат, оскільки, окрім так званих умовно-постійних витрат, існують витрати, пропорційні обсягу операції.

3. Втрати товару в процесі обігу (транспортування, зберігання) або втрати якості, споживчої цінності товару, що призводять до зниження його вартості. Рівень такого збитку встановлюється як добуток кількості загубленого товару і закупівельної ціни або добуток зіпсованої кількості товару та зниження відпускної ціни.

4. Збільшення витрат обігу порівняно з наміченими призводить до адекватного зниження доходу, прибутку. Серед можливих причин підвищення витрат можуть бути непередбачені мита, відрахування, штрафи, додаткові витрати.

5. Зниження ціни, за якою реалізується товар, порівняно з проектною викликає втрати у розмірі обсягу реалізації, помноженого на зменшення ціни.

6. Зниження обсягу реалізації, обумовлене непередбачуваним падінням попиту або потреби в товарі, витісненням його конкуруючими товарами, обмеженнями на продаж, здатне викликати втрати доходу і прибутку, що вимірюються як добуток обсягу непроданої продукції на відпускну ціну.

Втрати у виробничому підприємництві зазвичай мають місце за ситуації, коли відбулося:

1. Зниження намічених обсягів виробництва і реалізації продукції внаслідок зменшення продуктивності праці, простою устаткування або недовикористання виробничих потужностей, втрат робочого часу, відсутності необхідної кількості початкових матеріалів, підвищеного відсотка браку веде до недоотримання запланованої виручки. Вірогідні втрати DD в цьому випадку у вартісному виразі визначаються за формулою:

$$DD = DO \times Ц, \qquad (1.2)$$

де DO – вірогідне сумарне зменшення обсягу випуску продукції;

Ц – ціна реалізації одиниці обсягу продукції.

2. Зниження цін, за якими намічається реалізувати продукцію, у зв'язку з недостатньою якістю, несприятливою зміною ринкової кон'юнктури, падінням попиту призводить до вірогідних втрат, що визначаються за формулою:

$$DD = D \times Про, \quad (1.3)$$

де D – вірогідне зменшення ціни одиниці обсягу продукції;

Про – загальний обсяг наміченої до випуску та реалізації продукції.

3. Підвищені матеріальні витрати, обумовлені перевитратою матеріалів, сировини, палива, енергії, ведуть до втрат, що визначаються залежністю:

$$DD = Dm1 \times Ц1 + Dm2 \times Ц2 + ..., \quad (1.4)$$

де DM – вірогідна перевитрата матеріального ресурсу;

Ц – ціна одиниці ресурсу.

4. Інші підвищені витрати, які можуть бути внаслідок високих транспортних витрат, торгових витрат, накладних та інших побічних витрат.

5. Перевитрата наміченої величини фонду оплати праці внаслідок перевищення розрахункової чисельності або через виплату вищої, ніж заплановано, заробітної плати окремим працівникам.

6. Сплата підвищених відрахувань і податків, якщо в процесі здійснення плану ставки відрахувань і податків змінюються у несприятливий для підприємця бік.

7. Не слід випускати з уваги і можливість втрат у вигляді штрафів, природного спаду, а також обумовлених стихійними лихами, хоча врахувати такі втрати розрахунковим чином не є можливим [143].

Можлива й інша класифікація ризиків як джерел загроз економічній безпеці підприємства, а саме – зовнішні та внутрішні.

У групу зовнішніх входять такі ризики:

Ризик невиконання клієнтом своїх зобов'язань. Це ризик того, що клієнт не зможе або не захоче виконати свої зобов'язання перед підприємством. Підприємство може зіткнутися з ситуацією, коли покупець, наприклад, відмовиться від оплати за надану за контрактом продукцію. Навіть при торгівлі на умовах повної передоплати підприємство-постачальник все одно несе витрати, а іноді й прямі втрати, оскільки ви-

мушено шукати іншого покупця. Враховуючи, що продукція, що поставляється, може бути достатньо специфічного застосування, така відмова покупця може привести постачальника до великих фінансових проблем. Такі ризики відносять до так званих передконтрактних ризиків. Одним з ефективних способів їх мінімізації є формування портфеля покупців, коли одна і та ж продукція продається декільком покупцям. При відмові одного з них прийняти товар завжди потрібно мати в запасі іншого, який міг би його купити.

Ризик країни. Це ризик того, що всі або більшість економічних агентів (включаючи уряд) у конкретній державі не зможуть з певної внутрішньої причини виконати свої міжнародні зобов'язання.

Ризик обмеження переказу коштів (трансфертний ризик). Це ризик того, що певна країна виявиться нездібною або не захоче обслуговувати свої міжнародні фінансові зобов'язання унаслідок загального внутрішнього дефіциту іноземної валюти.

Ризик концентрації. Неадекватний розподіл портфеля замовлень між різними покупцями, галузями промисловості, країнами може привести до значних втрат. Переважна орієнтація на одного покупця підвищує ризик концентрації. Не можна забувати про цей ризик при організації банківського обслуговування. Це особливо важливо в нашому нестабільному українському банківському середовищі. Банкрутство банку, в якому підприємство зберігає засоби, може призвести і до банкрутства самого підприємства.

До групи внутрішніх ризиків відносяться такі види:

Ризик неоплати товару, непостачання комплектуючих. Ризик неоплати за поставлений товар або непостачання сплачених комплектуючих – це ризик того, що підприємство не зможе стягнути з боржника загальну суму наданого товарного кредиту або авансу або за рахунок повернення товару і подальші його продажі, а у разі авансу – просто його повернення, або за рахунок ведення інших юридичних дій проти боржника (виставляння претензій, позовів, зокрема в судовому порядку).

Ризик заміщення боржника. Ризик заміщення виникає тоді, коли підприємство вимушене виконувати зобов'язання перед своїм покупцем при невиконанні зобов'язань з боку постачальника. Наприклад, трейдер уклав контракт на постачання партії товару, який має бути поставлений одним з постачальників. При зміні кон'юнктури постачальник відмовляється поставляти товар за контрактом з трейдером. Трейдер вимушений

купити товар на ринку вже, можливо, за вищою ціною і виконати, таким чином, свій контракт перед покупцем. Ризик заміщення може виникнути і при ненадходженні грошових коштів від покупця, які підприємство повинне було використовувати на виконання своїх зобов'язань перед іншими контрагентами.

Ризик завершення операції. Цей ризик виникає в тому випадку, якщо клієнт підприємства або не виконує свої зобов'язання за розрахунком за поставлену продукцію та інше, або виконує їх із запізненням.

Ризик забезпечення операцій. Підприємство може понести втрати при наданні забезпеченого кредиту, якщо йому не вдасться вступити у володіння власністю, запропонованою як забезпечення або стягнути по забезпеченню іншим чином [143].

2. Індикатори та складові економічної безпеки підприємства

2.1. Структура економічної безпеки підприємства та поняття індикаторів економічної безпеки

Індикатори економічної безпеки підприємства – це показники рівня його економічної безпеки, що дають змогу виявити больові точки в його діяльності, визначити основні напрями і найбільш дієві способи підвищення ефективності його роботи.

Поняття економічної безпеки підприємства має внутрішньовиробничі й позавиробничі складові [23, с. 8–9; 47, с. 24–26].

Внутрішньовиробничі складові такі:

1. Фінансова складова: досягнення найбільш ефективного використання корпоративних ресурсів.

2. Інтелектуальна й кадрова складові: збереження і розвиток інтелектуального потенціалу підприємства; ефективне управління персоналом.

3. Техніко-технологічна складова: ступінь відповідності застосовуваних на підприємстві технологій найліпшим світовим аналогам за оптимізації витрат ресурсів.

4. Політико-правова складова: всебічне правове забезпечення діяльності підприємства, дотримання чинного законодавства.

5. Інформаційна складова: ефективне інформаційно-аналітичне забезпечення господарської діяльності підприємства (організації).

6. Екологічна складова: дотримання чинних екологічних норм, мінімізація втрат від забруднення довкілля.

7. Силова складова: забезпечення фізичної безпеки працівників фірми (передовсім керівників) і збереження її майна.

Позавиробничі складові такі:

1. Ринкова складова.

2. Інтерфейсна складова.

2.2. Складові економічної безпеки та управління ними

Фінансова складова як внутрішньовиробнича функціональна складова економічної безпеки вважається головною, оскільки за ринкових умов господарювання фінанси є "двигуном" будь-якої економічної системи.

Фінансово-економічний стан підприємства (організації) характеризується ступенем його (її) прибутковості та оборотності капіталу, фінансової стійкості й динаміки структури джерел фінансування, здатності розраховуватися за борговими зобов’язаннями.

Правильна оцінка фінансових результатів діяльності та фінансово-економічного стану підприємства (організації) за сучасних умов господарювання конче потрібна як для його (її) керівництва і власників, так і для інвесторів, партнерів, кредиторів, державних органів. Фінансово-економічний стан підприємства (організації) цікавить і його (її) конкурентів, але вже в іншому аспекті – негативному; вони заінтересовані в ослабленні позицій конкурентів на ринку.

Про ослаблення фінансової складової економічної безпеки свідчать:

зниження ліквідності підприємства;

підвищення кредиторської та дебіторської заборгованості;

зниження фінансової стійкості тощо.

За цю складову економічної безпеки відповідають фінансова та економічна служби підприємства.

Процесу забезпечення фінансової складової економічної безпеки передбачає виконання таких етапів:

1. Аналіз загроз негативних дій щодо політико-правової складової економічної безпеки.

2. Оцінка поточного рівня забезпечення фінансової складової економічної безпеки.

3. Оцінка ефективності запобігання можливій шкоді від негативних дій щодо фінансової складової економічної безпеки.

4. Планування комплексу заходів із забезпечення фінансової складової економічної безпеки та розробка рекомендацій стосовно його реалізації.

5. Бюджетне планування практичної реалізації пропонованого комплексу заходів.

6. Планування корпоративних ресурсів.

7. Оперативна реалізація запланованих дій у процесі здійснення суб'єктом господарювання своєї фінансово-господарської діяльності.

Спочатку оцінюють загрози економічній безпеці, що мають політико-правовий характер і включають:

внутрішні негативні дії (неефективне фінансове планування та управління активами; малоефективна ринкова стратегія; помилкова цінова й кадрова політика);

зовнішні негативні дії (спекулятивні операції на ринку цінних паперів; цінова та інші форми конкуренції; лобіювання конкурентами недостатньо виважених рішень органів влади);

форс-мажорні обставини (стихійне лихо, страйки, військові конфлікти) та обставини, наближені до форс-мажорних (несприятливі законодавчі акти, ембарго, блокада, зміна курсу валют тощо).

Оцінюючи поточний рівень забезпечення фінансової складової економічної безпеки, аналізують:

фінансову звітність і результати роботи підприємства (організації) – платоспроможність, фінансову незалежність, структуру й використання капіталу та прибутку;

конкурентний стан підприємства (організації) на ринку – частка ринку, якою володіє суб'єкт господарювання; рівень застосовуваних технологій і менеджменту;

ринок цінних паперів підприємства (організації) – оператори та інвестори цінних паперів, курс акцій.

Важливою передумовою забезпечення фінансової складової економічної безпеки є планування (включаючи й бюджетне) комплексу заходів та оперативна реалізація запланованих дій у процесі здійснення тим чи іншим суб'єктом господарювання фінансово-економічної діяльності [23, с. 58; 47, с. 24–28].

Показники, за допомогою яких можна оцінити фінансово-економічний стан (безпеку) підприємства (організації), такі [10; 47; 89]:

1. Прибутковість:

валовий прибуток;

чистий прибуток;

рентабельність активів, власного капіталу, акціонерного капіталу, продукції, одного виробу.

2. Ділова активність:

оборотність активів;

оборотність товарно-матеріальних запасів;

середній термін оплати дебіторської заборгованості;

середній термін оплати кредиторської заборгованості.

3. Фінансова стійкість:

коефіцієнт автономії;

коефіцієнт забезпеченості боргів;

фінансовий важіль (левериджа).

4. Платоспроможність:

коефіцієнт загальної ліквідності;

коефіцієнт термінової ліквідності;

коефіцієнт абсолютної ліквідності.

Належний рівень економічної безпеки значною мірою залежить від інтелекту і професіоналізму кадрів, що працюють на підприємстві. Негативно впливають на інтелектуальну складову:

звільнення провідних висококваліфікованих працівників, що призводить до ослаблення інтелектуального потенціалу;

зниження частки інженерно-технічних працівників і науковців у загальній чисельності працівників;

зниження винахідницької та раціоналізаторської активності;

зниження освітнього рівня працівників.

За інтелектуальну складову економічної безпеки на підприємстві відповідають служба з персоналу і особисто головний інженер.

Склад кадрів безпосередньо впливає на рівень економічної безпеки на підприємстві. Негативний вплив на кадрову складову мають:

1. Внутрішні загрози:

невідповідність кваліфікації працівників вимогам до них;

недостатня кваліфікація працівників;

слабка організація системи управління персоналом;

слабка організація системи навчання;

неефективна система мотивації;

помилки в плануванні ресурсів персоналу;

зниження кількості раціоналізаторських пропозицій та ініціатив;

відхід кваліфікованих працівників;

працівники зорієнтовані на вирішення внутрішніх тактичних завдань;

працівники зорієнтовані на дотримання інтересів підрозділу;

відсутність корпоративної політики або вона "слабка";

неякісні перевірки кандидатів для приймання на роботу.

2. Зовнішні загрози:

умови мотивації у конкурентів кращі (неважко за такого розкладу спрогнозувати перехід фахівців до конкурентів);

настанова конкурентів на переманювання;

тиск на працівників ззовні;

потрапляння працівників у різні види залежності;

інфляційні процеси (не можна не враховувати під час розрахунку заробітної плати і прогнозувати її динаміку).

За цю складову економічної безпеки має відповідати служба з персоналу підприємства.

Щодо критеріїв кадрової безпеки необхідно зробити короткий екскурс у тему про кількісні параметри економічної безпеки компанії.

Головними групами критеріїв безпосередньо в кадровій безпеці є показники:

1) чисельного складу персоналу та його динаміки;

2) кваліфікації й інтелектуального потенціалу;

3) ефективності використання персоналу;

4) якості мотиваційної системи.

Установивши спеціальні критерії і визначивши їх параметри, кадрова служба, крім того, зобов’язана:

1. Забезпечити розроблення поточних і планових значень показників кадрової безпеки для стратегічного і оперативного планування.

2. Здійснювати постійний моніторинг установлених показників у сфері своєї відповідальності.

3. Надавати з різною періодичністю і в певному обсязі дані звітності за станом "своїх" критеріїв.

4. Негайно повідомляти в орган управління і службу безпеки при отримані сигналу щодо негативного відхилення значення показника або про зміну напряму тенденцій планових величин.

5. Брати участь у розробленні й реалізації сценаріїв і заходів щодо стабілізації параметрів діяльності підприємства тощо.

Моніторинг здійснюється з метою виявлення і прогнозування негативних дій щодо інтересів і об'єктів економічної безпеки. Несприятливі явища і процеси можуть бути виражені у:

відхиленні величин установлених контрольних показників від граничних у негативний бік;

збільшенні амплітуди динаміки встановлених показників на величини, більші за допустимі;

виникненні нез'ясовних фінансових, технологічних та інформаційних явищ і процесів;

виникненні форс-мажорних обставин;

нез'ясованій або негативній поведінці окремих працівників і їх груп;

виникненні конфліктних ситуацій між внутрішніми і зовнішніми суб'єктами бізнесу;

підозрілому інтересі з боку зовнішніх суб'єктів до діяльності компанії, підрозділу, об'єкта, його персоналу, керівництва, інформації, матеріальних засобів і грошових коштів;

фактах розкрадань, пошкоджень майна, зникненні грошей і документів, інших неправомірних діях;

спробах несанкціонованого доступу і використання внутрішньої інформації;

виникненні проблем особистої безпеки працівників та ін.

При цьому, зрозуміло, всі посадові особи і працівники зобов'язані негайно повідомляти про такі відхилення в службу безпеки, а іноді – безпосередньо адміністрації. Невжиття відповідних заходів передбачає встановлену відповідальність.

Забезпечення інтелектуальної і кадрової складових економічної безпеки охоплює взаємопов'язані і водночас самостійні напрями діяльності того чи іншого суб'єкта господарювання:

перший зорієнтований на роботу з персоналом фірми, на підвищення ефективності діяльності всіх категорій персоналу;

другий – на збереження й розвиток інтелектуального потенціалу, тобто сукупності прав на інтелектуальну власність або на її використання

(у тому числі патентів і ліцензій) та на поповнення знань і професійного досвіду працівників підприємства (організації).

На першій стадії процесу забезпечення цієї складової економічної безпеки оцінюють загрози негативних дій і можливі наслідки їх. Серед основних негативних впливів на економічну безпеку підприємства виокремлюють недостатню кваліфікацію працівників тих чи тих структурних підрозділів, їх небажання або нездатність приносити максимальну користь своїй фірмі. Вони можуть бути зумовлені низьким рівнем управління персоналом, браком коштів на оплату праці окремих категорій працівників підприємства (організації) чи нераціональними витратами.

Процес планування та управління персоналом спрямований на забезпечення належного рівня економічної безпеки, має охоплювати організацію системи підбору, наймання, навчання і мотивації праці необхідних працівників, зокрема, матеріальні та моральні стимули, престижність професії і волю до творчості, забезпечення соціальними благами [23, с. 73; 47, с. 34–37].

Техніко-технологічна безпека підприємства полягає у рівні відповідності застосовуваних на підприємстві технологій найкращим світовим аналогам за оптимізації витрат. До негативних впливів на цю складову належать:

дії, спрямовані на підрив технологічного потенціалу підприємства;

порушення технологічної дисципліни;

моральне старіння використовуваних технологій.

Зовнішніми загрозами послаблення техніко-технологічної безпеки підприємства можна вважати брак зовнішніх і внутрішніх інвестицій. Труднощі в отриманні довгострокових кредитів від банків не дають змоги поповнювати обігові кошти підприємства і спрямовувати їх на оновлення парку обладнання. Усе це призводить до використання застарілої техніки, технології і до істотної загрози техніко-технологічній безпеці підприємства.

Підвищення цін на енергоносії, відсутність довгострокових контрактів із постачальниками, неспроможність постачальника – це зовнішні загрози економічній безпеці, які є досить високими. Більш як половину необхідних енергоресурсів Україна закуповує за кордоном, тому підвищення цін на енергоносії призводить до зростання собівартості продукції.

Внутрішні загрози техніко-технологічній безпеці підприємства – неефективна організація виробничого процесу, недостатньо кваліфіковані працівники, високий ступінь спрацьованості основного капіталу тощо,

який на підприємствах України становить 60 – 70 %, а в деяких галузях сягає 80 – 85 %. Така негативна тенденція зростає, тому фінансові ресурси підприємства обов'язково потрібно спрямувати на оновлення техніки і технології.

Внутрішні ресурсні загрози техніко-технологічній безпеці підприємства виникають унаслідок неефективного управління оборотними засобами підприємства в усі фази виробничого процесу: підготовка до виробництва, незавершене виробництво і реалізація продукції. Проблеми з матеріальними ресурсами стимулюють впровадження у виробництво нових технологічних процесів, які дають змогу виготовити продукцію з меншими матеріальними витратами, вдосконалити систему розрахунків. За цю складову економічної безпеки має відповідати технологічна служба, (здійснювати контроль за технологічною дисципліною, удосконалювати існуючі й розробляти нові ефективні технології).

Процес забезпечення техніко-технологічної складової економічної безпеки звичайно складається з кількох послідовних етапів.

На першому етапі проводять аналіз ринку технологій у виробництві продукції, аналогічної профілю певного підприємства чи організації-проектувальника (збирання й аналіз інформації про особливості технологічних процесів на підприємствах, котрі виготовляють аналогічну продукцію; аналіз науково-технічної інформації стосовно нових розробок у певній галузі, а також технологій, спроможних здійснити інтервенцію на галузевий технологічний ринок).

На другому етапі аналізують конкретні технологічні процеси і виявляють внутрішні резерви для поліпшення використовуваних технологій.

На третьому етапі здійснюють:

а) аналіз товарних ринків за профілем продукції, що виготовляється підприємством, та ринків товарів-замінників;

б) оцінювання перспектив розвитку ринків продукції підприємства;

в) прогнозування можливої специфіки необхідних технологічних процесів для випуску конкурентоспроможних товарів.

На четвертому етапі переважно розробляють технологічні стратегії розвитку підприємства (виробника продукції), зокрема:

1) виявляють перспективні товари з групи (номенклатури, асортименту), що виготовляється підприємством;

2) планують комплекс технологій для виробництва перспективних товарних позицій;

3) бюджетують технологічний розвиток підприємства на основі оптимізації витрат за програмою технологічного розвитку, за вибору альтернатив, опрацювання власних розробок або за придбання патентів і необхідного устаткування на ринку;

4) розробляють загальний план технологічного розвитку підприємства (з відображенням у ньому вибору: альтернативного варіанта технологічного розвитку; строків та обсягів фінансування; відповідальних виконавців);

5) складають план власних корпоративних ресурсів відповідно до плану технологічного розвитку підприємства.

На п’ятому етапі оперативно реалізують плани технологічного розвитку підприємства в процесі здійснення ним виробничо-господарської діяльності.

Шостий етап є завершальним – аналізують результати практичного виконання заходів щодо забезпечення техніко-технологічної складової економічної безпеки на підставі спеціальної карти розрахунків ефективності таких заходів [23, с. 68; 47, с. 53–55].

Політико-правова безпека підприємства – це захист від надмірного податкового тиску, нестабільного законодавства, неефективної роботи юридичного відділу підприємства. Вона визначає середовище, в якому функціонують підприємства, а також "правила гри для них".

Правова складова полягає у всебічному правовому забезпеченні діяльності підприємства, дотриманні чинного законодавства. Правову небезпеку становлять:

недостатня правова захищеність інтересів підприємства в договірній та іншій діловій документації;

низька кваліфікація працівників юридичної служби відповідного суб’єкта господарювання та помилки у підборі персоналу цієї служби;

порушення юридичних прав підприємства і його працівників; навмисне чи ненавмисне розголошення комерційно важливих відомостей;

порушення норм патентного права.

Протидією цим негативним впливам повинна займатися юридична і патентно-ліцензійна служба, зокрема, вона має здійснювати правове забезпечення діяльності підприємства, юридичне опрацювання договірної документації, ведення судових і арбітражних розглядів, правове навчання персоналу, контроль порушень норм патентного права тощо.

Зовнішньою загрозою політико-правовій безпеці підприємства є часті зміни уряду, нестабільність системи оподаткування, надмірні втру-

чання держави у справи бізнесу тощо. Серйозну загрозу діяльності підприємства становить відсутність правових гарантій у разі насильницького відчуження власності, заблокування рахунків підприємств та ін.

До внутрішніх нормативно-правових загроз підприємства належать шкідливі, непродумані норми внутрішнього розпорядку, посадові положення, інструкції, розпорядження, рішення трудового колективу. Загрозу підприємству становить і відсутність законодавчої бази, яка б давала змогу цивілізовано працювати охоронним службам, усувати неузгодженість діяльності приватних охоронних фірм із державними органами.

Загальний процес забезпечення політико-правової складової економічної безпеки відбувається за типовою схемою, яка охоплює такі елементи (дії) організаційно-економічного спрямування;

1) аналіз загроз негативних впливів;

2) оцінка поточного рівня забезпечення;

3) планування комплексу заходів підвищення цього рівня;

4) здійснення ресурсного планування;

5) планування роботи відповідних функціональних підрозділів підприємства (організації);

6) оперативна реалізація запропонованого комплексу заходів щодо гарантування належного рівня безпеки.

Насамперед детально аналізують загрози внутрішніх і зовнішніх негативних впливів на політико-правову складову економічної безпеки та причини їх виникнення.

Основними причинами виникнення внутрішніх негативних впливів можуть бути:

а) низька кваліфікація працівників юридичної служби відповідного суб’єкта господарювання та помилки у підборі персоналу цієї служби;

б) недостатнє фінансування юридичного забезпечення підприємницької або іншої діяльності;

в) небажання чи нездатність підприємства (організації) активно впливати на зовнішнє політико-правове середовище його (її) діяльності.

Останнє звичайно виявляється у слабкому правовому опрацюванні договірних відносин певного суб’єкта господарювання з іншими, невмінні захищати інтереси підприємства (організації) у конфліктних ситуаціях, неефективному плануванні юридичного забезпечення бізнесової діяльності.

Причини виникнення зовнішніх негативних впливів здебільшого мають подвійний характер:

1) політичний:

зіткнення інтересів суспільних груп (верств) населення з економічних, національних, релігійних та інших мотивів;

військові конфлікти (дії);

економічна й політична блокада, ембарго;

фінансові та політичні кризи світового (міжнародного) характеру;

2) законодавчо-правовий:

здійснення власних політичних та інших цілей партіями (суспільними рухами), що перебувають при владі;

зміна положень чинного законодавства з питань власності, господарського і трудового права, оподаткування тощо.

Оцінка поточного рівня забезпечення політико-правової безпеки підприємства (організації) проводиться за кількома напрямами:

1) рівень організації та якості робіт із забезпечення цієї складової загального рівня економічної безпеки;

2) бюджетно-ресурсне забезпечення робіт;

3) ефективність діяльності відповідних підрозділів суб'єктів господарювання.

Загальний процес охорони правової складової економічної безпеки відбувається за типовою схемою, яка охоплює такі елементи (дії) організаційно-економічного спрямування:

аналіз загроз негативних впливів;

оцінка поточного рівня забезпечення;

планування комплексу заходів щодо підвищення цього рівня;

ресурсне планування;

планування роботи відповідних функціональних підрозділів підприємства;

оперативна реалізація запропонованого комплексу заходів щодо організації належного рівня безпеки [47, с. 58–60].

Інформаційна складова полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства. Відповідні служби виконують при цьому певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової економічної безпеки. До таких функцій належать:

1) збирання всіх видів інформації про діяльність того чи того суб'єкта господарювання;

2) аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів і методів;

3) прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів;

4) оцінка рівня економічної безпеки за всіма складовими та в цілому, розроблення рекомендацій для підвищення цього рівня на конкретному суб'єкті господарювання;

5) інші види діяльності з розроблення інформаційної складової економічної безпеки.

На підприємство постійно надходять потоки інформації, що різняться джерелами їх формування. Виокремлюють інформацію:

відкриту офіційну;

вірогідну нетаємну, одержану через неформальні контакти працівників фірми з носіями такої інформації;

вірогідну таємну, отриману через неформальні контакти працівників фірми з носіями такої інформації.

Дослідження показують, що 90 – 95 % усієї необхідної інформації можна отримати легально, вивчаючи виступи працівників підприємства на конференціях, семінарах; відкриті публікації підприємства і його окремих працівників; експонати різних виставок, ярмарків, презентацій; дані товарних і фондових бірж, оголошення про наявні вакансії, конкурси на заміщення посади тощо. Тому керівник підприємства повинен запровадити правові норми захисту таємниць, а також систему контролю за збереженням комерційної таємниці.

Оперативна реалізація заходів з розроблення та охорони інформаційної складової економічної безпеки здійснюється послідовним виконанням певного комплексу таких робіт:

а) збирання різних видів необхідної інформації;

б) оброблення та систематизація добутої інформації;

в) аналіз цієї інформації;

г) захист інформаційного середовища підприємства, що традиційно охоплює:

заходи захисту суб'єкта господарювання від промислового шпигунства з боку конкурентів чи інших юридичних і фізичних осіб;

технічний захист приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу заінтересованих юридичних і фізичних осіб до закритої інформації;

збирання інформації про потенційних ініціаторів промислового шпигунства та проведення необхідних запобіжних дій з метою припинення таких спроб;

зовнішня інформаційна діяльність.

Головною метою будь-якої системи інформаційної безпеки є гарантування стійкого функціонування об'єкта, запобігання загрозам його безпеки, захист законних інтересів замовника від протиправних посягань, запобігання розкраданню грошових коштів; розголошуванню, втратам, витоку, спотворенню і знищенню службової інформації; забезпечення нормальної виробничої діяльності всіх підрозділів об'єкта. Система інформаційної безпеки має також сприяти підвищенню якості послуг, що надаються, і гарантій безпеки майнових прав та інтересів клієнтів.

Досягти поставлених цілей можна при вирішенні таких основних завдань:

віднесення інформації до категорії обмеженого доступу (службова таємниця);

прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів причин і умов, що сприяють фінансовим, матеріальним і моральним збиткам, порушенню нормального функціонування і розвитку об'єкта;

створення умов функціонування з найменшою вірогідністю реалізації загроз безпеці інформаційних ресурсів і зумовлення різних видів збитку;

створення механізму і умов оперативного реагування на загрози інформаційній безпеці та прояви негативних тенденцій у функціонуванні, ефективне припинення посягань на ресурси на основі правових, організаційних і технічних заходів, засобів гарантування безпеки;

створення умов для максимально можливого відшкодування і локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, ослаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей [23, с. 79; 47, с. 61–64].

Безпека підприємства в екологічній сфері – це захист від руйнівного впливу природних, техногенних чинників і наслідків господарської діяльності підприємства. Повені, землетруси, смерчі, зсуви ґрунту, лавини можуть завдати величезної шкоди майну підприємства, здоров'ю працівників. На практиці передбачити природні катастрофи неможливо, однак потрібно вжити всіх заходів, щоб наслідки стихійних лих були мінімальними для підприємства. Техногенні катастрофи виникають унаслідок ви-

користання фізично зношених основних засобів, непланованого вимкнення електроенергії або через низьку кваліфікацію і безвідповідальність працівників. Екологічні збитки можуть істотно впливати на фінансовий стан фірми. Наприклад, такі події, як судовий позов за порушення екологічного законодавства, аварія з екологічними наслідками на підприємстві, спричинюють збитки, які належать до категорії фінансово-екологічних і вимірюються у грошовій формі. Екологічні збитки внаслідок втрати здоров'я працівниками фірми, скорочення обсягів виробництва та реалізації продукції впливають на фінансовий стан фірми дещо повільніше. Такі екологічні збитки, як страждання людей унаслідок втрати здоров'я, не можуть бути виміряні у грошовій формі. Компенсацію за них визначають суб'єктивно. Екологічні збитки фірми можуть бути непокритими або покритими частково. Це вагоме джерело небезпеки для організації.

У результаті господарської діяльності саме підприємство може стати джерелом небезпеки для навколишнього середовища. До внутрішніх чинників, які погіршують його екологічну безпеку, належать: помилки, допущені на стадії проектування нових виробів, шкідливих для здоров'я людей, а також на стадії розроблення і впровадження нових технологій; штрафи за забруднення довкілля та незаконно створені звалища тощо.

Екологічна складова полягає у дотриманні чинних екологічних норм, мінімізації втрат від забруднення навколишнього природного середовища.

Проблему гарантування екологічної безпеки суспільства від суб'єктів господарювання, що здійснюють виробничо-комерційну діяльність, можна вирішити тільки розробленням і ретельним дотриманням національних (міжнародних) норм гранично допустимої концентрації шкідливих речовин, які потрапляють у навколишнє середовище, а також дотриманням екологічних параметрів продукції, що виготовляється. Підприємства-продуценти добровільно не будуть цього робити, бо такі заходи потребують додаткових витрат на очисні споруди та на відповідні ефективні екологічно чисті технології. Єдиним чинником, що спонукає підприємства до належної екологізації виробництва, є застосування відчутних штрафів за порушення національного екологічного законодавства.

Алгоритм процесу забезпечення екологічної складової економічної безпеки передбачає такі послідовні дії:

1) розрахунок карти ефективності здійснюваних заходів для забезпечення екологічної складової економічної безпеки за звітними даними про фінансово-господарську діяльність підприємства (організації);

2) аналіз виконаних розрахунків і розроблення рекомендацій для підвищення ефективності здійснюваних заходів;

3) розроблення альтернативних сценаріїв реалізації запланованих заходів;

4) вибір пріоритетного сценарію на основі порівняння розрахунків ефективності запланованих;

5) подання вибраного планового сценарію у складі загального плану гарантування економічної безпеки в підрозділи, які здійснюють функціональне планування фінансово-господарської діяльності підприємства (організації);

6) практичне здійснення запланованих заходів у процесі діяльності відповідного суб'єкта господарювання [23, с. 78; 47, с. 71–73].

Силова безпека підприємства полягає у захисті фізичної особи від загроз її життю, здоров'ю та матеріальному благополуччю, а також захист майна підприємства від кримінальних посягань. Силова складова полягає у забезпеченні фізичної безпеки працівників фірми (насамперед, керівників) і збереженні її майна. До основних негативних впливів на цю складову належать фізичні й моральні впливи на конкретних особистостей (особливо на керівництво та провідних спеціалістів) з метою заподіяти шкоду їх здоров'ю та репутації, що становить загрозу нормальній діяльності їх підприємства.

Негативні впливи, що завдають шкоди майну підприємства, несуть загрозу зниження вартості його активів і втрати економічної незалежності (дезінформація, знищення інформації).

Причинами цих негативних явищ є:

нездатність підприємств-конкурентів досягти переваг коректними методами ринкового характеру, тобто за рахунок підвищення якості власної продукції, зниження поточних витрат на виробництво (діяльність), удосконалення маркетингових досліджень ринку тощо;

кримінальні мотиви одержання злочинними юридичними (фізичними) особами доходів через шантаж, шахрайство або крадіжки;

некомерційні мотиви посягань на життя та здоров'я керівників і працівників підприємства (організації), а також на майно фірми.

Протидією цим негативним впливам повинна займатися служба охорони. Її обов'язок – забезпечувати фізичний захист керівництва підприємства, організовувати пропускний режим, здійснювати охорону приміщень, ліній зв'язку й устаткування.

На практиці за силову безпеку підприємства відповідає служба охорони, яка здійснює фізичний захист керівників підприємства, організовує пропускний режим, охороняє будинки, приміщення, лінії зв'язку та обладнання, захищає інформацію від несанкціонованого доступу, забезпечує режим секретності документів і матеріалів.

Рівень силової складової економічної безпеки підприємства можна також визначити за оцінкою ймовірності реалізації загроз для цілісності майна та фізичної безпеки працівників підприємства.

Розглянемо принципову схему організації силової складової економічної безпеки. Аналіз загроз негативних впливів за цією силовою складовою до причин їх виникнення передбачає:

1. Аналіз рівня організації силової складової економічної безпеки за напрямами, ресурсами, виконавцями, взаємодією та ефективністю витрат.

2. Прогнозування можливих негативних впливів та очікуваної шкоди від них.

3. Розроблення рекомендованого комплексу заходів для запобігання можливим негативним впливам.

4. Планування бюджету на використання рекомендованого комплексу заходів і розрахунок очікуваної ефективності від його реалізації.

5. Планування підбору і спеціального навчання відповідного персоналу.

6. Оперативне планування реалізації пропонованих заходів за ресурсами та виконавцями.

До негативних дій щодо силової складової економічної безпеки-належать:

1) фізичні й моральні впливи особистого спрямування (проти конкретної особистості);

2) негативні дії, спрямовані на те, щоб завдати шкоди майну, зокрема, загрози зменшення активів підприємства (організації) і втрати ним (нею) фінансової незалежності;

3) негативний вплив на інформаційне середовище суб'єкта господарювання (так зване промислове шпигунство) [47, с. 75–78].

Ринкова складова економічної безпеки підприємства – це захист від неефективно обраної моделі поведінки на ринку, помилок у товарній збутовій політиці, політиці ціноутворення, виготовлення неконкурентоспроможної продукції. Ця складова економічної безпеки характеризує ступінь

відповідності внутрішніх можливостей розвитку підприємства зовнішнім можливостям, які генеруються ринковим середовищем. Про ослаблення ринкової безпеки свідчать:

зменшення частки ринку, яку займає підприємство;

ослаблення конкурентних позицій і спроможності протидіяти конкурентному тиску;

зниження адаптаційних можливостей підприємства до змін ситуації на ринку, відставання від вимог ринку і та ін.

За ринкову складову безпеки на підприємстві має відповідати служба маркетингу. Ця складова відображає рівень відповідності внутрішніх виробничих можливостей підприємства зовнішнім, які формуються в ринковому середовищі, тобто наскільки науково-дослідна робота, виробнича і збутова діяльність відповідають запитам ринку і конкретним потребам споживачів.

Значущість ринкової безпеки підприємства полягає у тому, що вона відповідає за доведення виготовленої продукції до конкретного споживача. Відомо, що всі зусилля з виробництва будуть зведені нанівець, якщо продукція не буде продана.

Неузгоджена робота маркетологів, дизайнерів, конструкторів, економістів, фінансистів, низька якість виготовленої продукції, невчасне реагування на зміну кон'юнктури ринку, неефективна збутова мережа, низький рівень культури підприємства – це чинники внутрішнього середовища, які створюють загрозу ринковій безпеці підприємства.

Зовнішній чинник – це неконтрольоване підприємством середовище, яке складається з покупців, посередників, конкурентів, фінансових установ, рекламних агентств, митних і податкових організацій.

На ринкову безпеку впливають: нечесні дії конкурентів, рівень платоспроможності покупців, часті зміни податків, курсу валют, політична ситуація в країні і світі.

Чим більше уваги підприємство приділяє вивченню навколишнього середовища, стежить за ним, аналізує всі зміни, тим швидше можна передбачити небезпеку, вигідніше використати внутрішні можливості, прибутковіше вести бізнес [47, с. 79–80].

Інтерфейсна складова характеризує надійність взаємодії з економічними контрагентами. Економічній безпеці підприємства становлять загрозу можливі непередбачені зміни умов взаємодії (навіть до розриву відносин) з економічними контрагентами: постачальниками, торговими і збутовими по-

середниками, інвесторами, споживачами і та ін. Відповідальність за цю складову безпеки несе також служба маркетингу [47, с. 81].

2.3. Оцінка безпеки економічного простору функціонування підприємства

Займаючи свій сегмент загального економічного простору, кожна окрема фірма, незалежно від обсягів, місця й мети її діяльності, постійно знаходиться в ситуації стійкої невизначеності, непередбачуваності можливих змін як внутрішніх, так і зовнішніх умов господарювання. Ухвалюючи ризикове рішення в умовах жорсткої конкуренції та прагнучи запобігання або захисту від існуючих або прогнозованих загроз і небезпек, фірма забезпечує безпеку свого економічного простору.

Аналізуючи безпеку економічного простору функціонування підприємства, в першу чергу, увагу доцільно приділити таким складовим аналізу [103]:

блок ринкових факторів (робоча сила, засоби виробництва, капітал, технології);

блок неринкових факторів;

блок соціально-політичних факторів;

блок факторів впливу економічного простору.

Кожен із зазначених блоків може бути оцінений за допомогою певної сукупності показників. Основні фактори, індикатори, що впливають на ефективність господарської діяльності підприємницької фірми, представлені у табл. 2.1.

Таблиця 2.1

Індикатори безпеки економічного простору підприємства

№ п/п	Назва індикатора	Порогове значення індикатора	Напрям зміни індикатора, що позитивно впливає на рівень безпеки
1	2	3	4
1. Блок ринкових факторів			
1.1. Робоча сила			
1.1.1	Відношення кількості робітників з повною середньою та вищою освітою до загальної кількості робітників підприємства, %	75	плюс

Продовження табл. 2.1

1	2	3	4
1.1.2	Відношення робітників старше 50 років до загальної кількості робітників підприємства, %	20	мінус
1.1.3	Відтік кваліфікованих кадрів до загальної кількості працюючих, %	10	мінус
1.1.4	Рівень захворюваності працюючих до середнього в регіоні знаходження підприємства	1	мінус
1.2. Засоби виробництва			
1.2.1	Індекс виробництва, %	100	плюс
1.2.2	Мінімальний рівень завантаження потужностей, достатній для рентабельної роботи підприємства, %	70	плюс
1.2.3	Знос основних засобів, %	60	мінус
1.2.4	Продуктивність праці, тис. грн/осіб	200	плюс
1.2.5	Частка енергоносіїв у собівартості продукції, %	5	мінус
1.2.6	Рівень рентабельності, %	30	плюс
1.3. Капітал			
1.3.1	Співвідношення фактичного та необхідного обсягів інвестицій для підтримки існуючого потенціалу підприємства	1	плюс
1.3.2	Співвідношення кредиторської та дебіторської заборгованості	1	мінус
1.3.3	Відношення грошових зобов’язань до виручки	0,5	мінус
1.3.4	Частка в усіх витратах на виробництво витрат на імпортні комплектуючі та сировину, що потребують валютного заміщення, %	25	мінус
1.3.5	Коефіцієнт абсолютної ліквідності	0,2	плюс
1.3.6	Індекс кредитоспроможності	2,675	плюс
1.4. Технології			
1.4.1	Частка інноваційної продукції в загальному випуску продукції, %	10	плюс
1.4.2	Частка науково-дослідних робіт у загальному обсязі НДДКР, %	20	плюс
1.4.3	Відношення балансової вартості інновацій до середньорічної вартості основних фондів	20	плюс
1.4.4	Кількість отриманих підприємством патентів і ліцензій до їх середньої кількості в регіоні розміщення підприємства	1	плюс

Закінчення табл. 2.1

1	2	3	4
2. Блок неринкових факторів			
2.1	Рівень тіньової економіки в регіоні розміщення підприємства до середнього в країні	1	мінус
2.2	Наявність у підприємства пільг	так / ні	плюс / мінус
2.3	Частка виграних судових справ до загальної кількості тих, що відбулися, %	75	плюс
2.4	Відношення витрат на охорону власності до прибутку, %	15	плюс
2.5	Індекс антропогенного навантаження	1	мінус
3. Блок соціально-політичних факторів			
3.1	Співвідношення середньої зарплати на підприємстві та середньої в економіці країни	1	плюс
3.2	Забезпеченість робітників житлом до середнього в регіоні знаходження підприємства	1	плюс
3.3	Демократизм регіону знаходження підприємства	3,3	мінус
3.4	Рівень заборгованості з заробітної плати	0	мінус
3.5	Рівень злочинності в регіоні знаходження підприємства до середнього в країні	1	мінус
4. Фактори впливу економічного простору			
4.1	Частка основної продукції на ринку профільної продукції, %	35	плюс
4.2	Частка продукції, що має стійкий збут, в загальному обсязі продукції, %	50	плюс
4.3	Адаптивність підприємства до потреб ринку	1	плюс
4.4	Співвідношення обсягів продукції, що випускається підприємством як складовою інтегрованої структури бізнесу (ІСБ) та ІСБ в цілому, %	50	плюс

Отже, безпека економічного простору підприємства визначається якісним станом основних факторів виробництва – робочої сили, засобів виробництва та капіталу в грошовій формі, в сукупності зі здатністю підприємства забезпечити їх найбільш ефективне використання й адаптуватися до умов, що змінюються, та меж його економічного простору з метою отримання максимального прибутку.

3. Система економічної безпеки підприємства

3.1. Поняття та основні складові системи економічної безпеки підприємства

Система економічної безпеки кожного підприємства є індивідуальною, її повнота і дієвість залежать від чинної в державі законодавчої бази, від обсягу матеріально-технічних і фінансових ресурсів, виділених керівниками підприємств, від розуміння кожним з працівників важливості гарантування безпеки бізнесу, а також від досвіду роботи керівників служб безпеки підприємств.

Надійний захист економічної безпеки підприємства можливий лише за комплексного і системного підходу до її організації. Тому в економіці існує таке поняття, як система економічної безпеки підприємства. Ця система забезпечує можливість оцінити перспективи зростання підприємства, розробити тактику і стратегію його розвитку.

Основними елементами системи економічної безпеки підприємства є [47, с. 85]:

1) захист комерційної таємниці та конфіденційності інформації;

2) комп'ютерна безпека;

3) внутрішня безпека;

4) безпека будинків і споруд;

5) фізична безпека;

6) технічна безпека;

7) безпека зв'язку;

8) безпека господарсько-договірної діяльності;

9) безпека перевезень вантажів та осіб;

10) безпека рекламних, культурних, масових заходів, ділових зустрічей та переговорів;

11) протипожежна безпека;

12) екологічна безпека;

13) радіаційно-хімічна безпека;

14) конкурентна розвідка;

15) інформаційно-аналітична робота;

16) експертна перевірка механізму системи забезпечення.

Організація системи безпеки будь-якого комерційного підприємства повинна мати такі чотири рівні [47, с. 85]:

1. Адміністративний – управлінські рішення, необхідні для забезпечення безперебійного функціонування об’єкта.

2. Оперативний – заходи забезпечення безпеки господарюючого суб’єкта специфічними засобами і методами.

3. Технічний – використання сучасних технологій у сфері забезпечення всіх видів безпеки.

4. Режимно-пропускний – система фізичної безпеки, зокрема охорона фінансових, інтелектуальних і матеріально-технічних цінностей підприємства. При цьому захист території охоплює такі основні компоненти:

механічну систему захисту;

пристрій сповіщення про спроби вторгнення;

оптичну (телевізійну) систему пізнання порушників;

оборонну систему (звукова і світлова сигналізація);

центральний пост управління охорони;

персонал (патрулі, постові, чергові, мобільна група швидкого реагування, оператори).

При цьому не слід забувати, що ефективна охорона власності об’єкта можлива лише за достатньої автономії діяльності охорони. При дотриманні охороною єдиних правил режиму підприємства адміністрація не повинна чинити на службу режиму будь-який тиск у вигляді скасування чи зниження рівня чинних правил обмеження доступу на об’єкт.

Головне завдання системи управління економічною безпекою підприємства – передбачення і випередження можливих загроз, що призводять до кризового стану, а також проведення антикризового управління, яке спрямоване на виведення підприємства з кризового стану; мінімізація зовнішніх і внутрішніх загроз економічному стану суб’єкта підприємництва, зокрема його фінансовим, матеріальним, інформаційним, кадровим ресурсам, на основі розробленого комплексу заходів економіко-правового і організаційного характеру. Слід мати на увазі, що найбільше значення у справі забезпечення економічної безпеки підприємництва мають первинні економіко-правові та організаційні заходи, що забезпечують фундамент, основу системи безпеки, на відміну від вторинних – технічних, фізичних тощо [47, с. 86].

У процесі досягнення поставленої мети фірма вирішує конкретні завдання, які об’єднують усі напрями забезпечення безпеки.

Завдання, вирішувані системою гарантування безпеки такі [47, с. 87]:

прогнозування можливих загроз економічній безпеці;

організація діяльності із запобігання можливим загрозам (превентивні заходи);

виявлення, аналіз і оцінювання виниклих реальних загроз економічній безпеці;

ухвалення рішень і організація діяльності з реагування на виниклі загрози;

постійне вдосконалення системи забезпечення економічної безпеки підприємництва.

Головною умовою формування системи економічної безпеки підприємства є визначення сфер, у яких діють чинники небезпек і загроз. До таких сфер належать: безпека в техногенній, науково-технічній, екологічній, інформаційній, психологічній сферах, фізична та пожежна безпека.

Надійність і ефективність системи безпеки підприємства визначають за одним критерієм – відсутністю чи наявністю завданих йому матеріальних збитків і моральної шкоди. Зміст цього критерію характеризується такими показниками:

1) запобігання витоку конфіденційних відомостей;

2) запобігання протиправним діям з боку персоналу підприємства, його відвідувачів, клієнтів або припинення таких дій;

3) збереження майна й інтелектуальної власності підприємства;

4) запобігання надзвичайним ситуаціям;

5) припинення насильницьких злочинів щодо окремих (спеціально виділених) працівників підприємства і груп їх;

6) своєчасне виявлення і припинення спроб несанкціонованого проникнення на об’єкти підприємства, що охороняються.

Політика безпеки підприємства – це орієнтири для дій і ухвалення рішень, які полегшують досягнення цілей. Для встановлення цих загальних орієнтирів необхідно сформулювати цілі забезпечення безпеки підприємства.

Складовими політики безпеки є:

1. Завдання та цілі (виявлення, прогнозування небезпек і загроз та запобігання їм; забезпечення захищеності діяльності підприємства; створення власної служби безпеки).

2. Функції (прогнозування, виявлення, послаблення небезпек і загроз і запобігання їм; забезпечення захищеності діяльності підприємства, його персоналу і майна).

3. Принципи (комплектність, або системність; пріоритет запобіжних заходів; безперервність; законність; плановість; економність; взаємодія; поєднання гласності і конфіденційності; компетентність).

4. Стратегія (необхідність раптово реагувати на виниклі загрози; орієнтація на прогнозування, попереднє виявлення небезпек і загроз; спрямованість на відшкодування завданих збитків).

Цілями політики безпеки можуть бути:

зміцнення дисципліни праці і підвищення її продуктивності;

захист законних прав та інтересів підприємства; зміцнення інтелектуального потенціалу підприємства;

збереження і примноження власності;

підвищення конкурентоспроможності вироблюваної продукції;

максимально повне інформаційне забезпечення діяльності підприємства і підвищення його ефективності;

орієнтація на стандарти й лідерство в розробленні та освоєнні нової технології і продукції, що випускається;

виконання виробничих програм;

сприяння управлінським структурам у досягненні цілей підприємства;

запобігання залежності від випадкових і недобросовісних ділових партнерів [47, с. 89–90].

З урахуванням викладеного можна визначити такі загальні орієнтири дій і ухвалення рішень, які полегшують досягнення цих цілей:

збереження і нарощування ресурсного потенціалу;

проведення комплексу превентивних заходів щодо підвищення рівня захищеності власності й персоналу підприємства;

залучення до діяльності із забезпечення безпеки підприємства всіх його працівників;

професіоналізм і спеціалізація персоналу підприємства;

пріоритетність несилових методів запобігання загрозам і їх нейтралізації.

Дії суб’єктів, що створюють економічну безпеку підприємництва, мають певну стратегію і тактику.

Стратегічне управління у будь-якій організації і, зокрема, у сфері безпеки зазвичай здійснюється у такій послідовності:

розроблення і обґрунтування стратегії фірми;

складання стратегічного плану;

складання планів гарантування безпеки, фінансових планів, планів будівництва, маркетингу та ін.;

експертна оцінка стратегії і планів;

визначення основних видів стратегічного менеджменту, на які робить ставку організація, і виявлення можливих загроз та ризиків;

реалізація стратегії;

коригування стратегії і планів;

аналіз і оцінка результатів у ході і після реалізації стратегії.

Суть розроблення і реалізації стратегії полягає у тому, щоб вибрати потрібний напрям розвитку організації з численних альтернативних напрямів, потім забезпечити умови й безпеку виробничо-господарської діяльності, бізнесу і спрямувати діяльність організації так, щоб забезпечити прибуток та імідж фірми. Тоді таке стратегічне управління можна визначити як системне [47, с. 91].

Менеджери безпеки, по-перше, беруть безпосередню участь у розробленні програм для кожного виду стратегічного управління; по-друге, забезпечують безпеку реалізації цих програм наявними в службі безпеки спеціальними силами й засобами.

Тактика гарантування безпеки передбачає застосування конкретних процедур і виконання конкретних дій з метою забезпечення економічної безпеки суб’єкта підприємництва. Такими діями, залежно від характеру загроз і тяжкості наслідків їх реалізації, можуть бути, наприклад:

розширення юридичної служби фірми;

вжиття додаткових заходів щодо збереження комерційної таємниці;

створення підрозділу комп’ютерної безпеки;

висловлення претензій контрагентові-порушникові;

звернення з позовом до судових органів;

звернення до правоохоронних органів.

Серед існуючих засобів гарантування безпеки можна виділити [47, с. 103]:

1) технічні – охоронно-пожежні системи, відео-, радіоапаратура, засоби виявлення вибухових приладів, бронежилети, огородження тощо;

2) організаційні – спеціалізовані організаційні структурні формування, що забезпечують безпеку підприємства;

3) інформаційні – передусім друкована і відеопродукція з питань збереження конфіденційної інформації. Крім того, важлива інформація

для прийняття рішень з питань економічної безпеки зберігається на комп'ютерах;

4) фінансові – без достатніх грошових коштів неможливе функціонування системи економічної безпеки підприємства, треба тільки використовувати їх цілеспрямовано і з високою віддачею;

5) правові – підприємство має у своїй діяльності не тільки керуватися законами та підзаконними актами, що видані вищими органами влади, а й розробляти власні (локальні) правові акти з питань гарантування економічної безпеки підприємства;

6) кадрові – підприємство має бути забезпечене кадрами, що займаються питаннями економічної безпеки;

7) інтелектуальні – кваліфіковані спеціалісти, наукові працівники, що дає змогу модернізувати систему безпеки підприємства.

Одночасне використання всіх цих засобів неможливе. Їх вводять поетапно: перший етап – виділення коштів; другий – формування кадрових і організаційних засобів; третій – розроблення системи правових засобів; четвертий – залучення технічних, інформаційних та інтелектуальних засобів.

Переведеним із статичного у динамічний стан зазначеним засобам відповідають методи забезпечення економічної безпеки підприємства:

технічні – спостереження, контроль, ідентифікація;

інформаційні – складання характеристик на працівників, аналітичні матеріали конфіденційного характеру тощо;

фінансові – матеріальне стимулювання працівників, що мають досягнення у забезпеченні економічної безпеки підприємства;

правові – судовий захист законних прав та інтересів, сприяння діям правоохоронних органів;

кадрові – підбір, навчання кадрів, що забезпечують безпеку підприємства;

інтелектуальні – патентування, ноу-хау тощо [47, с. 104].

Механізм реалізації безпеки – це системне застосування функцій, заходів, засобів та принципів безпеки. Система безпеки виконує дві основні функції: запобіжно-профілактичну й оперативно-інформаційну.

Запобіжно-профілактична функція реалізується через виконання загальних заходів безпеки, основними з яких є:

здійснення організаційно-правового впливу на діяльність персоналу і клієнтів організації через розроблення і впровадження нормативів безпеки;

підбір, перевірка і контроль роботи персоналу, розроблення ефективної кадрової політики та програм стимулювання праці;

охорона організації: об'єктів, грошей, матеріальних цінностей, комунікацій, обладнання, вантажів, персоналу;

атестація приміщень, спеціальне обладнання окремих із них, облік носіїв інформації обмеженого доступу, захист засобів зв'язку, організація службового і спеціального діловодства;

захист інформаційних ресурсів обмеженого доступу;

удосконалення технологій виробництва, введення в них елементів захисту;

формування позитивного іміджу організації;

планування і забезпечення діяльності організації в кризових ситуаціях;

забезпечення безпеки споруд і будівель установ, їх комунікаційних систем;

створення систем сповіщення персоналу;

розроблення заходів відповідальності за порушення встановлених правил безпеки діяльності.

Оперативно-інформаційна функція реалізується через виконання спеціальних заходів безпеки, основними з яких є:

організація і ведення конкурентної розвідки, формування інформаційних ресурсів;

інформаційно-аналітичні дослідження клієнтів, партнерів і конкурентів, інформаційно-аналітичне забезпечення прийняття рішень керівництвом організації;

взаємодія із правоохоронними органами з питань запобігання протиправним посяганням на власність, персонал та імідж організації і припинення їх;

розроблення і проведення заходів щодо протидії недобросовісній конкуренції, у тому числі промисловому шпигунству;

проведення службових розслідувань за фактами протиправних дій персоналу організації та порушення ними встановлених правил роботи;

проведення заходів щодо дезінформації конкурентів; проведення заходів впливу на недобросовісних клієнтів, боржників і зловмисників щодо відшкодування організації втрат, яких вона зазнала з їх вини [47, с. 104–105].

Під час формування і здійснення заходів та використання засобів безпеки потрібно керуватися вихідними положеннями, тобто принципами забезпечення економічної безпеки, основними з яких є:

1. Економічна доцільність і мінімізація можливого збитку і витрат на забезпечення безпеки (критерій "ефективність – вартість").

2. Своєчасність – запобіжний характер заходів гарантування безпеки. Передбачає постановку завдань з комплексної безпеки на ранніх стадіях розроблення системи безпеки на основі аналізу і прогнозування обстановки, загроз безпеки, а також розроблення ефективних заходів запобігання посяганням на законні інтереси.

3. Комплексність:

гарантування безпеки персоналу, матеріальних і фінансових ресурсів від можливих загроз всіма доступними законними засобами і методами;

гарантування безпеки інформаційних ресурсів протягом усього їхнього життєвого циклу, на всіх технологічних етапах їх оброблення (перетворення) і використання, у всіх режимах функціонування;

здатність системи до розвитку і вдосконалення відповідно до зміни умов функціонування фірми.

Особливу увагу треба приділяти принципу комплексності. Для безпеки у всьому різноманітті структурних елементів фірми, за безлічі загроз і способів несанкціонованого доступу, потрібно застосовувати всі види і форми захисту та протидії в повному обсязі. Неприпустимо застосовувати окремі форми або технічні засоби.

Отже, під комплексною безпекою слід розуміти повне охоплення об’єктів захисту всією сукупністю форм протидії і захисту (охорона, режим, кадри, документи і та ін.) на основі правових, організаційних та інженерно-технічних заходів.

4. Законність. Припускає розроблення системи безпеки на основі законодавства у сфері підприємницької діяльності, інформації і її захисту, приватної охоронної діяльності, а також інших нормативних документів з безпеки, затверджених органами державного управління в межах їх компетенції, із застосуванням усіх дозволених методів виявлення і припинення правопорушень.

5. Обґрунтованість. Пропоновані заходи і засоби захисту мають бути реалізовані на сучасному рівні розвитку науки і техніки, бути обґрунтованими з огляду на заданий рівень безпеки і відповідати встановленим вимогам і нормам.

6. Безперервність. Вважається, що зловмисники тільки й шукають можливість, як би обійти захисні заходи, вдаючись для цього до легальних і нелегальних методів.

7. Активність. Захищати інтереси фірми треба з достатнім ступенем наполегливості, широко використовуючи маневр силами і засобами забезпечення безпеки та нестандартні заходи захисту.

8. Спеціалізація. Передбачає використання для розроблення і впровадження заходів і засобів захисту спеціалізованих організацій, що найбільш підготовлені до конкретного виду діяльності із гарантування безпеки, мають досвід практичної роботи і державну ліцензію на право надання послуг у цій галузі. Експлуатацією технічних засобів і реалізацією заходів безпеки мають займатись професійно підготовлені працівники служби безпеки, її функціональні та обслуговуючі підрозділи.

9. Взаємодія і координація. Припускають здійснення заходів безпеки на основі чіткої взаємодії всіх зацікавлених підрозділів і служб, сторонніх спеціалізованих організацій у цій сфері, координацію їх зусиль для досягнення поставленої мети, а також інтеграцію діяльності з органами державного управління і правоохоронними органами.

10. Удосконалення – поліпшення заходів і засобів захисту на основі власного досвіду, появи нових технічних засобів з урахуванням змін у методах і засобах розвідки й промислового шпигунства, нормативних вимог накопиченого вітчизняного і зарубіжного досвіду.

11. Централізація управління – самостійне функціонування системи безпеки з єдиними організаційними, функціональними і методичними принципами, з централізованим управлінням діяльністю системи управління.

12. Достатність – застосовування таких засобів і заходів активного і пасивного захисту, які б були достатніми для протидії загрозам чи небезпекам.

13. Гнучкість – застосовування моделі економічної безпеки залежно від характеру і рівня розвитку загрози чи небезпеки. Це надає мобільності діям у сфері безпеки і підвищує їх ефективність [47, с. 106–107].

Система економічної безпеки, залежно від ситуації та її розвитку, може функціонувати в трьох режимах: повсякденному, підвищеної готовності і надзвичайного стану [47, с. 107].

Повсякденний режим – це звичайний робочий режим, коли всі суб’єкти системи безпеки, крім кризової групи, виконують свої функції, реалізують заходи запобігання виникненню загроз, їх виявлення та розроб-

лення відповідних типових планів дій на випадок реалізації тих чи інших загроз. Залежно від ситуації, що складається, розрізняють такі види планів:

план дій у разі загрози вибуху;

план дій при захопленні заручників або викраденні працівників організації;

план дій при вимаганні;

план дій у разі нападу на приміщення організації;

план дій під час нападу на інкасаторів.

Типові кризові плани є документами конфіденційного характеру, доступ до яких має вузьке коло осіб. Складають подібні плани у двох-трьох примірниках. Один зберігається в керівника організації, другий – у начальника служби безпеки, третій може бути у заступника керівника, який виконує його обов'язки.

Розробляючи такі плани, слід зважати на те, що це не перелік заходів, а послідовна лінія поведінки організації в конкретній кризовій ситуації, спрямована на гарантування безпеки.

Режим підвищеної готовності – це функціонування системи безпеки у разі виявлення конкретних потенційних загроз.

На доповнення до дій, що виконуються у повсякденному режимі, здійснюють ще такі:

уточнюють і вдосконалюють типові плани дій з урахуванням виду загрози, її інтенсивності та масштабності;

підвищують готовність сил безпеки, які можуть бути задіяиі для припинення дії загрози;

можливий початок роботи кризової групи.

Режим надзвичайного (кризового) стану – це функціонування системи безпеки за наявності реальних загроз, їх дії. У цьому разі:

оперативне управління організацією переходить до кризової групи;

рада з безпеки розпочинає працювати в постійному режимі;

забезпечується повна готовність системи безпеки, особливо служби безпеки, функціональних і лінійних керівників та персоналу організації до безпосереднього припинення дії загрози;

залучаються зовнішні сили безпеки (державна служба охорони, органи внутрішніх справ) та сили підтримки (структури міністерства надзвичайних ситуацій тощо).

Слід зазначити, що застосування кожного із засобів окремо не дає необхідного ефекту, він можливий тільки на комплексній основі. Разом із тим одночасне впровадження всіх згаданих засобів в принципі неможливе.

3.2. Теоретичні положення з формування системи управління економічною безпекою підприємства

Складність підприємства як системи, що функціонує в умовах ринкової економіки, означає наявність у нього відповідної внутрішньої структури, що складається з елементів, їх властивостей і зв'язків, які забезпечують у результаті своєї взаємодії виконання комплексу функцій системи й досягнення її цілей на підставі збирання, аналізу, накопичення та розподілу знань.

Система управління – це система, завданням якої є вироблення й реалізація управлінського впливу, або рішень, для формування необхідної поведінки керованої системи (або об'єкта управління) в умовах складнопрогнозованих впливів навколишнього середовища для досягнення сформульованих цілей. Зі зростанням темпів науково-технічного прогресу, розвитку інформаційних технологій і невизначеності зовнішнього середовища на перший план виходять питання своєчасного розпізнавання загроз для існування підприємств, стійкості, можливостей розвитку й наслідків. Вони стають критеріями оцінки ефективності системи управління. Внутрішня будова системи управління економічною безпекою підприємства розглядається як відповідь на вплив зовнішнього середовища й організаційно-економічних характеристик самого підприємства. Обирається така структура управління, що забезпечує максимальне досягнення цілей.

Побудову системи управління економічною безпекою підприємства варто здійснювати при дотриманні певної системи принципів, сформульованих на базі чинних законів розвитку. Загальна схема такої побудови представлена на рис. 3.1.

Закон становить об'єктивно існуючий стійкий істотний взаємозв'язок явищ об'єктивної дійсності. Неврахування у діяльності підприємства законів неминуче приведе до кризової ситуації. Навпаки, їх точне врахування при вмілому керівництві може знизити рівень можливих негативних наслідків та порушення економічної безпеки підприємства.

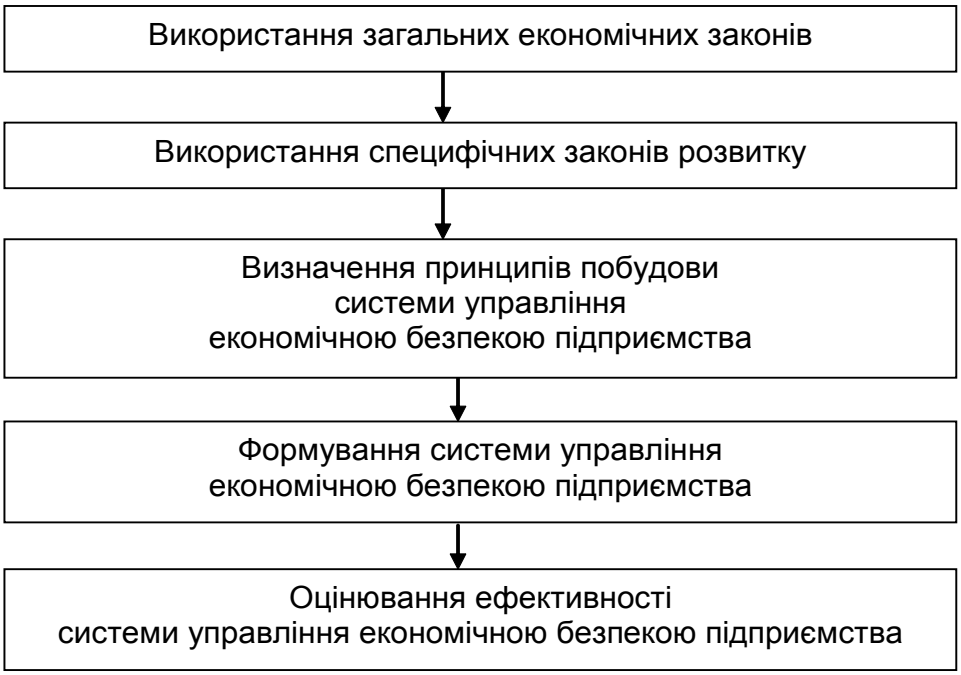


Рис. 3.1. **Загальна схема побудови системи управління економічною безпекою підприємства**

Як основні загальні економічні закони варто виділити такі:

1. Закон попиту (фіксує зворотну залежність між ціною товару й кількістю його придбання населенням або цільовими групами).

2. Закон відповідності попиту та пропозиції (зводиться до рівності пропозиції та попиту на задоволення актуальної потреби, що регулюється ринковим механізмом).

3. Закон спадаючої віддачі (свідчить, що, починаючи з певного моменту, додаткове включення одиниць змінного ресурсу при фіксованій величині іншого ресурсу дає зменшуваний граничний продукт у розрахунку на кожну наступну одиницю першого).

4. Закон економії часу (в економічній теорії розглядається як економія минулої й живої праці на одиницю продукції або неухильне зниження собівартості продукції на одиницю споживчої вартості).

5. Закон необмеженого зростання потреб (зводиться до того, що в процесі розвитку суспільства змінюються, зростають і його потреби, попит на які задовольняється продуктами, що випускаються організаціями з використанням певних технологій і технологічних процесів).

Побудова раціональної системи управління економічною безпекою й забезпечення її ефективного функціонування можливо лише при точному врахуванні та використанні чинних законів організаційного розвит-

ку, що і є однією з найважливіших завдань менеджменту. При побудові системи управління економічною безпекою підприємства як специфічні закони розвитку необхідно враховувати такі:

1. Закон онтогенезу полягає в тому, що будь-яка сутність (живий організм, підприємство, продукт, потреба, попит на задоволення потреби та ін.) проходить свій життєвий цикл, тобто в процесі своєї життєдіяльності минає відносно постійну черговість етапів, що характеризуються переліком конкретних, відносно стабільних показників.

2. Закон композиції відображає ієрархічність у цільовій орієнтації системи, коли цілі більш високого рівня підкоряють собі цільові настанови нижніх рівнів ієрархії. Дія цього закону формує в організації: проблему виявлення головної, загальної мети; проблему визначення цілей нижнього рівня, що підтримують загальну цільову настанову; проблему узгодження багатьох системних цілей між собою, тобто підвищення ефективності цільового функціонування системи.

3. Закон пропорційності вимагає домірності, погодженості характеристик елементів, що утворюють систему, у тому числі соціально-економічну. Невиконання цієї вимоги спричиняє недовикористання наявних ресурсів організації, зниження її ефективності й втрату конкурентоспроможності.

4. Закон найменших свідчить, що "структурна стабільність" системи визначається найменшою стабільністю її компонентів.

5. Закон синергії свідчить, що при формуванні елементами єдиного цілого (системи) останнє забезпечує збільшення загального ефекту до величини більшої, ніж сума ефектів цих елементів, що діють незалежно; визначає виникнення в цілісному сполученні елементів ефекту системності, коли ефективність функціонування цілого виявляється вище сумарної ефективності функціонування елементів. У виробничій системі цей закон проявляється в раціоналізації складу елементів системи, їх максимального погодженого використання при досягненні встановлених цілей.

6. Закон необхідного й достатнього інформаційного забезпечення зводиться до виявлення стійкого зв’язку між обсягом інформації й ефективністю вироблення й ухвалення управлінського рішення. Так, у міру зростання обсягу інформації зростає визначеність ситуації, число варіантів рішення скорочується, зменшується час прийому рішення, ефективність зростає. Надлишковий обсяг інформації спричиняє зростання часу на її переробку, при цьому зростання ефективності ухвалення рішення

спадає, тому що розглянуті варіанти перебувають поблизу оптимуму. Таким чином, організація інформаційного забезпечення системи управління є однією з важливих завдань при її формуванні.

7. Закон необхідної розмаїтості передбачає обмеженість кількості елементів у раціонально організованій системі як знизу, так і зверху. Мінімальний за розмаїтістю склад системи визначається можливістю виконання нею основної функції, максимальний – ефективністю функціонування.

8. Закон емерджентності зводиться до придбання системою нових властивостей, що були відсутні у її елементів; зводиться до того, що при формуванні елементами єдиного цілого (системи) останнє набуває нових властивостей, відсутніх у самостійних елементів, що його утворили.

9. Закон наростання організаційної ентропії в процесі життєдіяльності, під якою розуміється енергетичний рівень організації, рівень її підприємницького духу, заповзятливості її керівників, рівень опору організації дезорганізуючим факторам, що перешкоджають її розвитку.

Отже, узагальнюючи представлені закони щодо побудови системи управління економічною безпекою підприємства, слід зазначити, що важливими умовами в даному випадку є необхідність врахування цілеспрямованості системи та її інформаційної забезпеченості.

Принципи побудови систем управління – це загальні закономірності й стійкі вимоги, при дотриманні яких формується система управління, що забезпечує ефективний розвиток підприємства в умовах дії загроз.

Принципи побудови системи управління достатньо повно розглянуто у багатьох наукових працях [9; 10; 39; 47; 93; 98; 145]. Загалом виділяються такі основні принципи.

1. Об’єктивності й детальної розробки цілей і стратегії організації. Цей принцип передбачає необхідність зв’язку системи управління підприємства з його цільовими настановами. При побудові системи управління повинні виключатися дублювання, дифузія цілей, обов’язкове закріплення мети за конкретним підрозділом. Основна роль системи управління зводиться до зосередження всіх зусиль для досягнення загальних цілей з найменшими протиріччями. При формуванні системи управління визначається єдина мета, що досягається спільними зусиллями через діяльність всіх структур і підрозділів підприємства.

2. Урахування відносного значення управлінських функцій (принцип рівноваги). При цьому виділяються основні й другорядні функції, які необхідні в сукупності, але розрізняються за ступенем значущості. При форму-

ванні системи управління цей факт повинен враховуватися для визначення управлінського рівня й підрозділу, що реалізує ту або іншу функцію.

3. Спеціалізації. Визначає дроблення робіт на кожному з рівнів управління, що забезпечує можливість і необхідність функціональної координації. На першому етапі формування системи управління спеціалізація практикується через групування аналогічних і близьких по суті робіт, при виконанні яких потрібна певна кваліфікація, тобто відбувається горизонтальний поділ праці. У той же час відбувається вертикальний поділ праці, що відокремлює роботу з координування дій від самих дій. Діяльність кожної управлінської одиниці в системі управління повинна здійснюватися відповідно до напряму роботи вищої одиниці. У той же час ця діяльність повинна відповідати цілям і стратегії всієї організації.

4. Координації (кооперації). Це принци досить тісно пов'язаний з попереднім, оскільки формування системи управління на основі спеціалізації вимагає координації діяльності різних управлінських одиниць. Вимоги принципів спеціалізації й координації найчастіше перебувають у протиріччі один з одним. Вирішення цієї проблеми є нелегким і залежить від конкретних умов організації.

5. Організаційного контролю (самоконтролю) покликаний виявляти прорахунки й спрощення в діяльності управлінської структури або працівника, допущені ними при виконанні попередньої частини роботи. При цьому мається на увазі в основному самоконтроль.

6. Зниження управлінських видатків. Оскільки формування системи управління призводить до додаткових управлінських видатків, то одним із завдань господарської діяльності організації є зниження управлінських видатків. При цьому мова йде про раціоналізацію системи управління.

Виділяються також принципи, що ґрунтуються на підвищенні значущості автоматизації управлінських процесів.

1. Принцип нових завдань. Суть принципу зводиться до необхідності при автоматизації системи управління не просто копіювати старі сформовані структури, процеси, процедури, а формувати нові з врахуванням величезних можливостей, що надаються комп'ютером.

2. Принцип комплексного або системного підходу при розробленні системи управління. Рекомендується вирішувати всі класи організаційних завдань на єдиній інформаційній базі й у взаємному зв'язуванні один з одним.

3. Принцип першого керівника. Принцип враховує опір суб'єктів – об'єктів управління при реалізації практично будь-яких нововведень в організаційній побудові. Тому участь перших осіб підприємства при формуванні (реструктуруванні) системи управління вкрай важливий.

4. Принцип безперервного розвитку системи (онтогенезу). Будь-яка система існує, поки вона розвивається. Організаційні системи в процесі розвитку розширюють коло розв'язуваних завдань, поглиблюють системність такого рішення, підвищують синергізм системи управління.

5. Принцип автоматизації документообігу та єдиної інформаційної бази. З метою підвищення точності, об'єктивності, погодженості управлінських рішень вони повинні вироблятися на єдиній інформаційній базі. Вихідна інформація, у свою чергу, формується, поповнюється на основі автоматизованого збору й переробки вихідних даних. При цьому варто дотримуватися правила про однократне введення даних і багаторазове їх використанні.

6. Принцип модульності й типізації. Зводиться до виділення відносно самостійних частин системи управління (модулів), розроблення системи автоматизованих процесів, що протікають у них, і потім широкому використання таких модулів у будь-яких підсистемах, де їх застосування обґрунтовано.

7. Принцип погодженості пропускних здібностей окремих частин системи. З огляду на те, що при автоматизації процесів управління застосовуються технічні засоби (персональні комп'ютери, кабельні мережі, оргтехніка), процес управління стає усе більше схожий на виробничий. В організації виробничих процесів принцип "вузького місця" є тривіальним і обов'язково повинен враховуватися. Він зводиться до того, що продуктивність виробничого ланцюга визначається продуктивністю її найменш продуктивної ланки. Тому для раціонального використання можливостей всіх елементів системи при її побудові варто погоджувати їх продуктивності.

У процесі побудови та функціонування системи управління економічною безпекою підприємства доцільно використовувати такі принципи (рис. 3.2).

1. Принцип ієрархічності полягає в побудові багаторівневої організаційної структури управління з раціональним розподілом функцій, що виконуються, завдань і відповідних їм владних повноважень.

2. Принцип координації ґрунтується на цільовій спрямованості діяльності організації та її складових. Принцип координації – це визначення

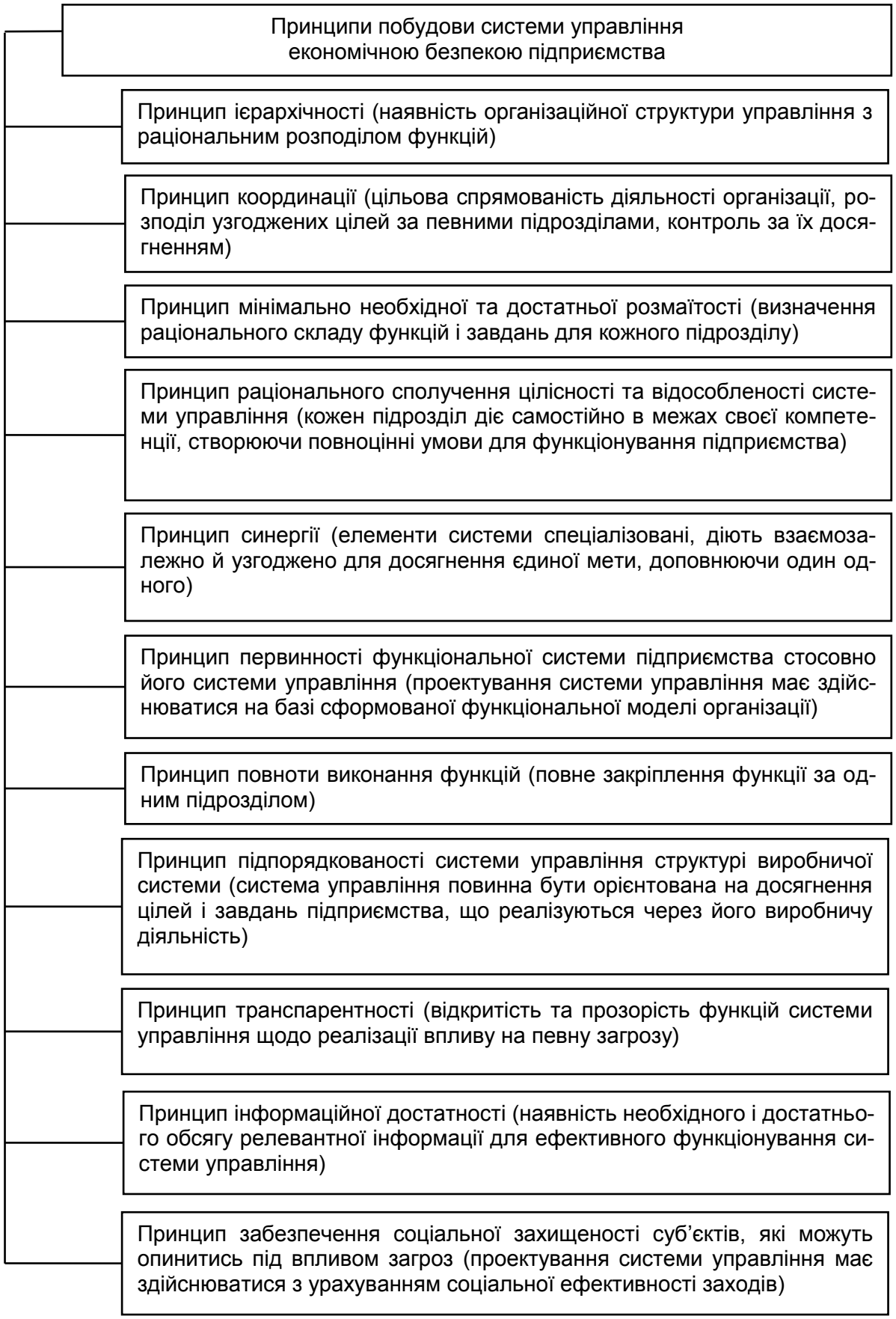


Рис. 3.2. **Принципи формування системи управління економічною безпекою підприємства**

й розподіл погоджених цілей за підрозділами та посадовими особами і чіткий контроль за їх досягненням, оскільки досягнення цілей нижчого рівня забезпечує досягнення цілей більш високого рівня й цільових настанов організації в цілому.

3. Принцип мінімально необхідної й достатньої розмаїтості. Полягає в необхідності визначення раціонального складу функцій і завдань певного обсягу, що закріплюється за підрозділом, посадовою особою в рамках організаційної структури управління. Вузька спеціалізація (одна або мале число взаємозалежних функцій, завдань, закріплених за управлінським підрозділом або посадовою особою), підвищуючи професіоналізм у даній області, звужує кругозір фахівця, позбавляє його масштабного підходу до вирішення організаційних завдань. Широка спеціалізація, навпаки, часто не дозволяє фахівцю досягти високих результатів у реалізації конкретних функцій і завдань. Таким чином, при побудові системи управління необхідно знайти раціональне сполучення складу й обсягу функцій, що виконуються, і розв'язуваних завдань.

4. Принцип раціонального сполучення цілісності й відособленості системи управління. Цілісною визнається система, у якій кожний елемент зв'язаний з усіма іншими елементами й зміни, внесені в один з елементів, викликають необхідність внесення змін в усі інші елементи. Відособленою вважається система, у якій елементи не зв'язані між собою й зміна кожного з них не вимагає зміни інших елементів. У рамках цього дослідження принцип реалізує системний підхід до формування системи управління, коли кожний підрозділ або посадова особа діє в рамках своєї компетенції самостійно (відособленість елемента системи), але його дії у взаємозв'язку з реалізацією інших функцій, доповнюючи одна одну, створюють повноцінні умови для цілеспрямованого функціонування підприємства (цілісність системи управління). Оптимальним варто вважати таке сполучення цілісності й відособленості системи управління економічною безпекою підприємства, коли реалізується принцип Парето, що зводиться до того, що будь-яка зміна в будь-якому елементі системи управління призведе до зниження ефективності її функціонування. Таким чином, самостійність у діях підрозділів обмежена й може оцінюватися за допомогою контролю динаміки показників ефективності організації в цілому. У наслідок об'єктивного характеру розвитку системи управління необхідно з певною періодичністю досліджувати повноту виконання цього принципу.

5. Принцип синергії. Будь-який набір елементів може вважатися системою тільки тоді, коли елементи спеціалізовані, діють взаємозалежно й узгоджено щодо досягнення єдиної для них мети (або системи цілей), а їх функціонування органічно доповнює один одного. Тобто принцип синергії в побудові системи управління економічною безпекою підприємства зводиться до такого – техніка, технології, структури й та ін., застосовувані в процесі управління, повинні, органічно доповнюючи один одного, виключати дублювання й при використанні єдиної інформаційної бази забезпечувати найбільшу ефективність діяльності організації, тобто при мінімальній кількості використовуваних ресурсів забезпечувати максимальний результат.

6. Принцип первинності функціональної системи підприємства стосовно його системи управління. Цілі організації досягаються через функціонування її виробництва. Таке функціонування можливо при успішному виконанні повного комплексу взаємозалежних функцій, що утворюють функціональну модель організації. Отже, проектування системи управління економічною безпекою повинне здійснюватися на базі сформованої функціональної моделі організації, кожний елемент якої досліджений і є повна інформація про його характеристики (періодичність виконання, обсяг виконання (трудомісткість), черговість у технологічному процесі управління, процедури реалізації й та ін.).

7. Принцип повноти виконання функцій. Функція становить повний комплекс взаємозалежних, однорідних за характером робіт, розв’язуваних завдань. Виконання функції передбачає використання специфічних методів і інструментів менеджменту. Дроблення функції за декількома підрозділами підприємства, як правило, пов’язане з необґрунтованими витратами на узгодження, дублювання та ін. Таким чином, раціональним варто визнати повне закріплення функції за одним підрозділом (посадовою особою).

8. Принцип підпорядкованості системи управління економічної безпекою підприємства структурі виробничої системи. Система управління повинна бути орієнтована на досягнення цілей і завдань підприємства. Цілі підприємства досягаються через його виробничу діяльність. Отже, система управління економічною безпекою повинна бути підлегла виробництву.

9. Принцип транспарентності передбачає, що система управління повинна враховувати необхідність дотримання вимоги відкритості мети,

завдань та функцій, що виконуються нею як для внутрішнього, так і для зовнішнього середовищ.

10. Принцип інформаційної достатності полягає в тому, що інформаційне забезпечення має бути достатнім для ефективного функціонування системи управління. З точки зору зовнішньої необхідності визначає важливість урахування всіх факторів ринкового середовища та відповідних загроз, а внутрішня необхідність визначає важливість формалізації того, що необхідно знати, а саме підґрунтя кожного управлінського процесу та його вплив на інші процеси. Тобто поєднання зовнішньої та внутрішньої необхідності визначає певні критерії, згідно з якими здійснюється функціонування системи управління економічною безпекою. Отже, принцип інформаційної достатності визначає, з одного боку, критерії збору та отримання інформації щодо зовнішнього середовища, а з іншого – критерії формування інформаційного масиву про внутрішній стан підприємства. Принцип інформаційної достатності не має сталого кількісного визначення. Оскільки у кожному випадку досягнення конкретної мети потребує своєї достатньої системи інформаційного забезпечення.

Принцип соціальної захищеності суб’єктів, які можуть відчути на собі вплив певної загрози через реалізацію певних організаційно-економічних перетворень, пов’язаний, в першу чергу, з можливістю виникнення їх неприйняття з боку безпосередніх виконавців, в зв’язку з чим важливого значення набуває забезпечення достатнього рівня соціальної ефективності заходів, що впроваджуються системою управління.

Отже, основними вимогами до системи управління економічною безпекою підприємства є: інформаційна забезпеченість процесу управління; припустимі тривалість циклу управління й рівень перешкод у ньому; захищеність контуру управління від зовнішніх перешкод; обмежена припустимою величиною ймовірність порушення циклу управління у всьому діапазоні умов функціонування системи; здатність системи до виконання своїх функцій у всьому діапазоні зовнішніх умов; забезпечення запасу стійкості до малих збурювань зовнішнього й внутрішнього середовищ; припустима вартість системи, включаючи видатки на створення і функціонування. З урахуванням зазначених вимог у складі системи управління економічною безпекою підприємства необхідно виділити такі підсистеми: формування цілей, інформаційну (інформаційно-комунікаційну), аналітичну, виконавчу й контролюючу (рис. 3.3).

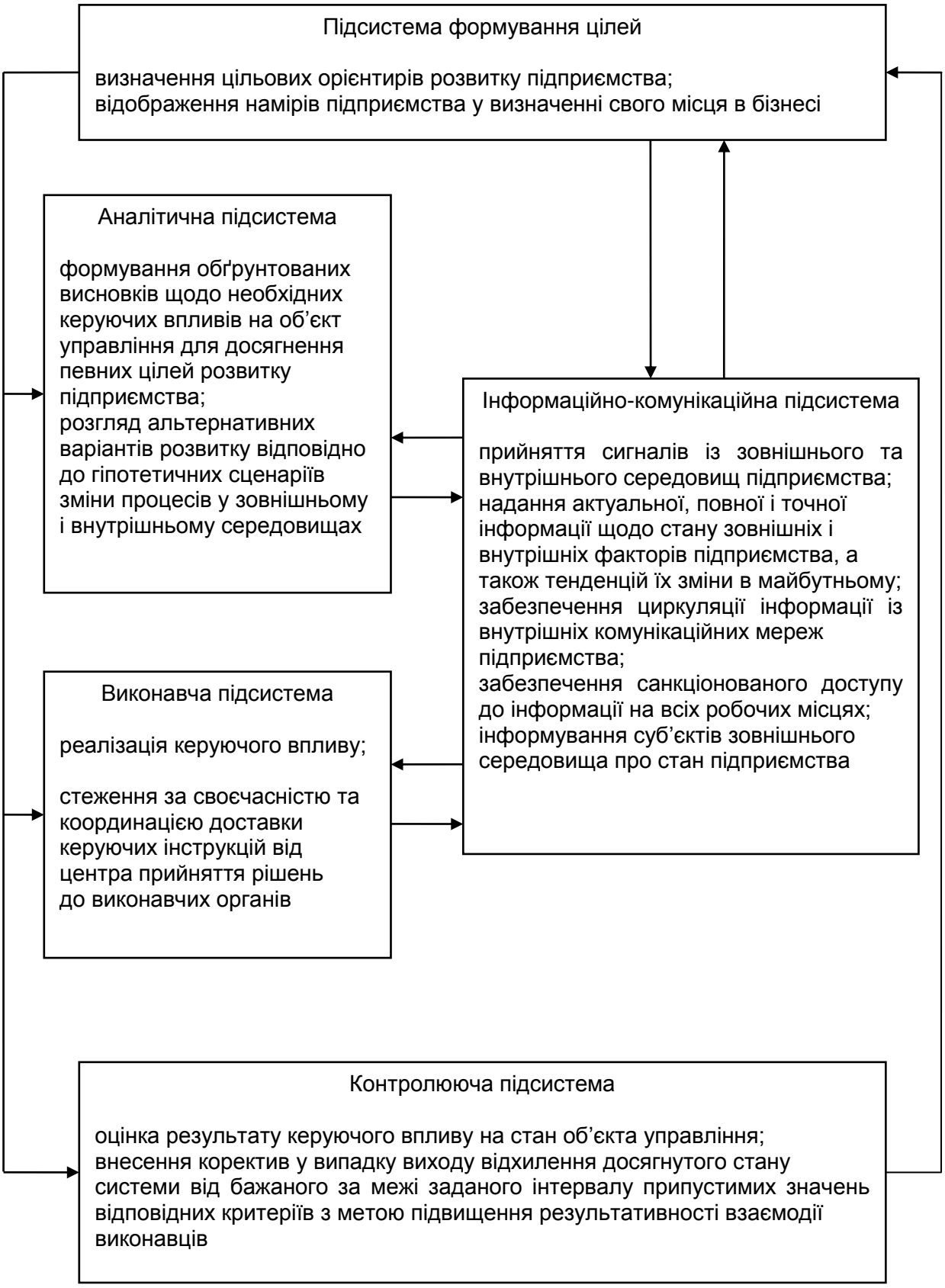


Рис. 3.3. **Структура системи управління економічною безпекою підприємства**

Функціонування підсистеми формування цілей передбачає визначення цільових орієнтирів розвитку підприємства в умовах дії загроз. Необхідність цієї підсистеми обґрунтовується тим, що цілі відображають наміри підприємства у визначенні свого місця в бізнесі й пов'язані з вирішенням проблеми підвищення конкурентоспроможності підприємства, забезпечення його стійкої позиції на ринку й довгострокового успіху. Тобто певного рівня економічної безпеки.

Інформаційна (інформаційно-комунікаційна) підсистема повинна: приймати сигнали із зовнішнього й внутрішнього середовищ підприємства; надавати актуальну, повну й точну інформацію про стан зовнішніх і внутрішніх факторів підприємства, а також про тенденції їх зміни в майбутньому; забезпечувати циркуляцію інформації з внутрішніх комунікаційних мереж підприємства; забезпечувати санкціонований доступ до інформації на всіх робочих місцях; інформувати суб'єктів зовнішнього середовища про стан підприємства. Необхідність інформаційної підсистеми в сучасних умовах господарювання обумовлена зростанням темпів науково-технічного й економічного розвитку, збільшенням інформаційного навантаження на систему управління економічною безпекою, глобалізацією економічних процесів.

Аналітична підсистема передбачає наявність фахівців, інструментарію й методів, за допомогою яких на підставі інформації, що надходить, вони могли б зробити в припустимий термін обґрунтований висновок про необхідні керуючі впливи на об'єкт управління для досягнення певного рівня економічної безпеки підприємства. Роль даної підсистеми досить велика, тому що управління підприємством здійснюється в умовах високого ступеня невизначеності зовнішнього середовища, що приводить до необхідності розгляду керівництвом великої кількості альтернативних варіантів розвитку відповідно до гіпотетичних сценаріїв зміни процесів у зовнішньому та внутрішньому середовищах. Для підвищення ефективності аналітичної підсистеми варто втримувати складність структури підприємства в певних межах, обумовлених динамізмом його зовнішнього й внутрішнього середовищ. Це передбачає наявність обмеження на величину, а також структурну й функціональну складність підприємства. Структура повинна бути за можливості більш простою, мати короткі тракти інформаційного забезпечення, розробки й реалізації керуючих впливів, що у мінімальному ступені спотворюють реакцію системи.

Особливе значення в рамках аналітичної підсистеми має також наявність кваліфікованого персоналу, що розділяє цілі підприємства.

Виконавча підсистема повинна дозволяти швидко й точно реалізовувати керуючий вплив. При цьому необхідно стежити за своєчасністю й координацією доставки керуючих інструкцій від центра прийняття рішень до виконавчих органів, перевіряючи точність їх розуміння персоналом. При реалізації складних керуючих впливів, що включають велику кількість виконавців, необхідна додаткова організація механізмів синхронізації й координації дій. Одним з важливих факторів, що підвищують ефективність виконавчої підсистеми, є наявність достатньо високого рівня мотивації працівників підприємства. що відповідають за підтримку певного рівня його економічної безпеки.

Інформаційний обмін супроводжує всі етапи взаємодії персоналу підприємства за вертикальними та горизонтальними зв'язками. Призначення комунікаційного процесу полягає в забезпеченні адекватного сприйняття інформації всіма учасниками процесу управління економічною безпекою на підприємстві, а також різними групами за його межами. У табл. 3.1 представлені групи впливу й завдання, які керівництво підприємства повинне вирішувати в процесі взаємодії з цими групами для забезпечення власної економічної безпеки. При цьому інформаційний обмін має здійснюватись відповідно до ресурсів знань, характерних для кожної групи впливу.

Таблиця 3.1

Групи впливу й завдання цільового впливу підприємства в процесі комунікацій з ними для забезпечення власної економічної безпеки

Групи впливу	Характерні ресурси знань	Завдання цільового впливу підприємства
1	2	3
Персонал підприємства	Кваліфікація, професійні знання, досвід, власні потреби	Забезпечення вимого техніки безпеки, виконавської дисципліни; створення сприятливих умови праці; удосконалення системи мотивації й стимулювання персоналу; підвищення продуктивності праці; підвищення кваліфікації персоналу
Акціонери	Альтернативні джерела вкладення коштів	Оптимізація дивідендів і інших доходів власників; участь акціонерів у розподілі прибутку; інформування акціонерів про діяльність підприємства

Продовження табл. 3.1

1	2	3
Профспілкова організація	Соціальна відповідальність бізнесу	Розробка трудового договору, збалансованого за позиціями трудового колективу й адміністрації; участь в управлінні підприємством; політика соціального партнерства; удосконалення організаційної культури
Споживачі	Потреби, власні уявлення про якісну продукцію	Максимальне врахування запитів споживачів у товарах і послугах; удосконалення зв'язків із союзами споживачів; досягнення високого рівня якості товарів; зміцнення зв'язків зі споживачами
Комерційні посередники, оптові покупці	Цінова і товарна політика, комерційні умови	Підвищення ефективності спільної цінової й товарної політики, стимулювання збуту; спільне проведення рекламних кампаній; передача прав користування символікою підприємства
Постачальники	Цінова політика, умови поставок, комерційні умови	Досягнення взаємовигідних угод на поставки; удосконалення системи постачальницької логістики; підвищення ефективності спільної цінової політики й умов поставки
Банки, фондові біржі	Умови кредитування та розміщення коштів	Досягнення сприятливих умов кредитних угод; ефективне розміщення вільних коштів з урахуванням ліквідності, рентабельності й допустимості ризику
Маркетингова інфраструктура ринку	Умови функціонування та співпраці з консультаційними фірмами	Установлення ділових відносин з консультаційними фірмами, інформаційними центрами й іншими маркетинговими посередниками; проведення зовнішнього аудита маркетингу із залученням зовнішніх консультантів
Конкуренти	Стан внутрішнього середовища, політика щодо споживачів, положення на ринку	Активний захист позицій підприємства при строгому дотриманні норм сумлінної конкуренції; безперервне вдосконалення товарів і послуг, а також перед- і післяпродажного супроводу своїх товарів
Засоби масової інформації (ЗМІ)	Джерела збору інформації, досвід подання інформації та створення іміджу підприємства	Підтримка регулярних і ефективних контактів для формування позитивного образу підприємства, досягнення позитивної реакції громадськості на господарську, суспільну й іншу діяльність підприємства; ефективне використання ЗМІ для реклами власної продукції
Громадські організації	Права споживачів, стан екології, етика бізнесу	Турбота про дотримання прав споживачів; екологічна безпека; підтримка соціально значимих програм і організацій; дотримання етичних норм бізнесу

Закінчення табл. 3.1

1	2	3
Органи влади	Законодавча база, суспільні цілі	Строге дотримання законів та інших актів органів влади; своєчасне одержання інформації про зміни в законодавстві; досягнення законної підтримки бізнесу підприємства з боку органів влади; участь у суспільно значимих програмах; створення робочих місць

Контролююча підсистема необхідна для оцінки результату керуючого впливу на стан об'єкта управління й внесення коректив у випадку виходу відхилення досягнутого стану системи від бажаного за межі заданого інтервалу припустимих значень відповідних критеріїв економічної безпеки з метою підвищення результативності взаємодії виконавців. Важливою умовою ефективності контролюючої підсистеми є її незалежність від виконавчої з позиції виключення їх скоординованих дій у приватних інтересах, що суперечать інтересам і цілям системи управління економічною безпекою підприємства.

В сучасних умовах господарювання рівень інформаційного забезпечення, його якість, а також повнота, релевантність й оперативність інформації має велике значення для прийняття своєчасних управлінських рішень щодо мінімізації негативного впливу певних загроз діяльності підприємства.

Представлена в табл. 3.1 інформація свідчить про те, наскільки складна й різноманітна система комунікацій підприємства. При цьому варто враховувати, що в конкретних ситуаціях можуть виникати нові контактні аудиторії, специфіку яких також необхідно враховувати для забезпечення ефективності контактів з ними та відповідного рівня економічної безпеки підприємства.

3.3. Концепція безпеки підприємства

Концепція – це система поглядів, ідей, цільових настанов, пронизаних єдиним, визначальним задумом, провідною думкою щодо постановки і шляхів вирішення виявлених проблем. До будь-якої концепції ставляться такі вимоги:

1. Конструктивність. Ця вимога може бути визнана реалізованою, якщо в концепції дістане відображення:

початковий стан об’єкта, на перетворення якого спрямована концепція;

стан об’єкта, досягнутий у результаті реалізації концепції;

заходи досягнення сформульованих у концепції цілей; засоби, необхідні і достатні для досягнення поставлених цілей;

джерела ресурсного забезпечення, використовувані в процесі реалізації концепції;

механізм реалізації концепції, тобто способи (методи) використання виділених засобів і ресурсів.

2. Вписуваність. Мається на увазі те, що потрібно здійснити перетворення якогось об’єкта на систему концепції взаємозв’язаних об’єктів, одним із компонентів якої цей об’єкт є.

3. Відкритість. Розроблена концепція повинна давати змогу в її рамках реагувати на зміну умов реалізації концепції і вносити корективи в реалізацію у разі потреби в них.

Зазначені вимоги диктують як обов’язкову умову введення до логічної структури концепції таких позицій:

1) виявлення об’єкта і предмета, визначення їх суті, місця серед множини інших;

2) чітке формулювання ролі і завдання реалізації концепції;

3) виділення умов, необхідних і достатніх для реалізації концепції, та зіставлення їх з існуючими;

4) визначення заходів і шляхів реалізації, що забезпечують перетворення об’єкта реалізації концепції;

5) формулювання критеріїв успішності заходів щодо розроблення концепції.

Концепція безпеки підприємства є офіційно затвердженим документом, у якому відображена система поглядів, вимог та умов організації заходів безпеки персоналу і власності підприємства. Структура концепції може мати такий вигляд:

I. Опис проблемної ситуації у сфері безпеки підприємства.

1. Перелік потенційних і реальних загроз безпеки, їх класифікація і ранжування.

2. Причини і чинники зародження загроз.

3. Негативні наслідки загроз для підприємства.

II. Механізм гарантування безпеки.

1. Визначення об’єкта і предмета безпеки підприємства.

2. Формулювання політики і стратегії безпеки.

3. Принципи гарантування безпеки.

4. Цілі гарантування безпеки.

5. Завдання гарантування безпеки.

6. Критерії і показники безпеки підприємства.

7. Створення оргструктури управління системою безпеки підприємства.

III. Заходи щодо реалізації заходів безпеки.

1. Формування підсистем загальної системи безпеки підприємства.

2. Визначення суб'єктів безпеки підприємства і їх ролі.

3. Розрахунок засобів і визначення способів гарантування безпеки.

4. Контроль і оцінка процесу реалізації концепції.

Необхідно зважати на те, що якнайповніше уявлення про систему безпеки підприємства можна отримати після вивчення офіційно прийнятих документів з концепції безпеки підприємства, комплексної програми гарантування безпеки підприємства і планів його підрозділів з реалізації цієї програми [47, с. 109–110].

3.4. Оцінка ефективності функціонування системи управління економічною безпекою підприємства

Функціонування системи управління економічною безпекою підприємства передбачає виконання певних завдань, функцій, досягнення певної мети. У зв'язку з цим особливу увагу слід приділити проблемі оцінки ефективності системи управління економічною безпекою.

Оцінювання ефективності системи управління можливо здійснювати за допомогою традиційних витратних показників шляхом співставлення економічного ефекту та витрат, пов'язаних з досягненням цього ефекту. Як ефект може виступати додатково отриманий прибуток за рахунок удосконалення системи управління.

Не зважаючи на різноманітність можливих підходів щодо оцінювання ефективності системи управління економічною безпекою підприємства, недостатньо дослідженими є питання оцінювання ефективності, пов'язані з використанням інформаційних ресурсів з урахуванням певних затримок з їх передачі, що можуть бути викликані різноманітними причинами.

Отже, зі зростанням швидкості змін у зовнішньому і внутрішньому середовищах підприємства при незмінних параметрах системи управ-

ління зростає запізнення її реакції на відповідні події. Це запізнення (затримка) складається з таких складових:

затримки первинної інформації Т1 у процесі нагромадження досить повного масиву інформації про стан зовнішнього й внутрішнього середовищ підприємства, а також різних перевірок найбільш важливих її фрагментів з метою забезпечення вірогідності й достатньої точності інформації. Інформаційний масив, що збирається, містить фрагменти, що відносяться до різних процесів у зовнішньому і внутрішньому середовищах, які відрізняються своїми швидкостями, а також інтенсивністю впливу на систему управління;

затримки Т2 при передачі інформації з місця подій до центрів її обробки й прийняття управлінських рішень. У центр прийняття рішень інформація надходить після її попередньої обробки, що вимагає певного часу й тому вносить свій внесок у старіння інформації про стан зовнішнього й внутрішнього середовищ. Порушення адекватності реакції системи управління на певні події також є наслідком затримки, пов’язаної з фізичною передачею інформації з ліній зв’язку;

затримки Т3, пов’язані з постановкою завдання управління в центрі ухвалення рішення, перевіркою несуперечності вхідних даних і їх уточнення на основі інформації з місця подій, вибором методу рішення завдання, аналізом можливих наслідків для кожного з розглянутих альтернативних варіантів, що завершується вибором оптимального варіанта управлінського рішення, у результаті чого формується набір інструкцій для виконавчих органів з розрахованою реакцією системи управління на події в зовнішньому і внутрішньому середовищах;

затримки керуючої інформації Т4, при її передачі за каналами зв’язку до виконавчих органів, а також при її дешифруванні виконавчими органами;

затримки Т5 при приведенні виконавчих органів у стан готовності до виконання керуючих інструкцій;

затримки Т6, пов’язані з контролем результатів реакції системи управління на певні зміни в зовнішньому і внутрішньому середовищах підприємства.

Загальна затримка Те реакції системи управління економічною безпекою на події в зовнішньому і внутрішньому середовищах дорівнює сумі часткових:

$$Te = T1 + T2 + T3 + T4 + T5 + T6. \quad (3.1)$$

Отже, ефективність системи управління економічною безпекою забезпечується також результативністю інформаційного обміну. В зв'язку з цим пропонується вирішальне правило для додаткового оцінювання ефективності системи управління на основі визначення змін показника Те з урахуванням його фактичного (Теф) та базового значень (Теб) (табл. 3.2).

Таблиця 3.2

Вирішальне правило для додаткового оцінювання ефективності системи управління економічною безпекою підприємства

Система управління ефективна	Система управління неефективна
Теф – Теб ≤ 0	Теф – Теб > 0

Відповідно до табл. 3.2, якщо фактичне запізнення реакції системи на певні події зменшилось порівняно з базовим, за умови, що якісні, а також традиційні витратні показники не змінюються або несуттєво змінюються, то система є ефективною і навпаки.

Для підвищення ефективності інформаційного обміну на підприємстві в процесі управління його економічною безпекою доцільна реалізація таких заходів:

налагодження регулярних каналів збору інформації, що дозволяють вести моніторинг обстановки;

організація на регулярній основі конкурентної розвідки, що дозволяє: прогнозувати й оцінювати зміни на ринках і тим самим допомагає визначати перспективні для підприємства ринкові ніші; вивчати й оцінювати конкурентів, а також реальна зміна їх економічного становища в результаті тих або інших успіхів і невдач; прогнозувати дії конкурентів і партнерів; виявляти нових або потенційних конкурентів у регіональному, національному й світовому масштабі; оцінювати поява нових технологій, здатних змінити стан підприємства; оцінювати поява нових продуктів і їх потенційний вплив на ринок; проводити моніторинг ризиків підприємства; підбирати й перевіряти кандидатів на відповідальні пости на підприємстві; сприяти розширенню кругозору керівництва щодо нових перспектив-

них методів управління, здатних підвищити економічну ефективність підприємства й та ін.;

наближення експертів, що керують збором інформації, до місця, де протікають процеси, що цікавлять підприємство, для того, щоб вони могли на місці направляти процес збору й здійснювати контроль інформації, що збирається, реалізуючи зворотний зв'язок в інформаційному процесі;

формування інтерактивної структури управління на підприємстві, що характеризується такими особливостями: відносною незалежністю кожного елемента структури; переважним розташуванням елементів структури на горизонтальному рівні; рекомендаційним характером взаємодії вищого рівня з нижчим; взаємодією між елементами структури в режимі реального часу; відсутністю залежності ступеня складності структури й шляхів проходження сигналу від географічної далекості елементів структури й та ін.;

створення комунікаційних мереж, що становлять з'єднання регулярними інформаційними потоками індивідів, що беруть участь у комунікаційному обміні і складаються не тільки з вертикальних (з'єднують керівників з їх підлеглими) і горизонтальних (з'єднують членів організації, що мають у ній однаковий статус) зв'язків, але й діагональних (з'єднують керівників з підлеглими інших підрозділів), що дозволить точніше формалізувати процедури спілкування, визначаючи коло проблем, що лежать в основі комунікацій, знизити надмірність повідомлень;

забезпечення персоналу набором методик і відповідним інструментарієм для збору й оцінки інформації, що надходить, на предмет її релевантності, актуальності, повноти й точності;

підвищення рівня кваліфікації персоналу, що займається збором і оцінкою інформації;

використання сучасних методів мотивації й стимулювання персоналу, що бере участь у зборі й оцінці інформації.

Період ефективного функціонування інформаційного, методичного, технічного забезпечення системи управління економічною безпекою підприємства має обмежений характер, і з часом система вимагає перегляду. У зв'язку з цим система управління повинна бути сприйнятлива до впровадження управлінських інновацій, які дозволяють адаптуватися до змін факторів зовнішнього середовища.

4. Особливості діяльності служби безпеки підприємства

4.1. Служба безпеки як підсистема підприємства

Завдання гарантування безпеки підприємства є одним із основних, пріоритетних завдань, що стоять перед усіма структурними ланками і всіма працівниками підприємства, так само як і завдання збільшення прибутку, підвищення власного добробуту. Ефективний захист економічних інтересів фірми може бути забезпечений лише у разі об'єднання зусиль її персоналу: адміністрації, інженерно-технічних працівників, службовців, робітників.

Служба безпеки фірми – це самостійний структурний підрозділ. Вона вирішує завдання безпосереднього забезпечення за хисту життєво важливих інтересів фірми в умовах комерційного і підприємницького ризику, конкурентної боротьби. На всіх великих і середніх підприємствах (в організаціях) зазвичай створюються автономні служби безпеки, а безпеку функціонування невеликих фірм можуть гарантувати територіальні (районні або міські) служби за договорами найму одного чи кількох охоронців. Такі служби охорони зазвичай створюються при місцевих органах внутрішніх справ або при державній службі безпеки [47, с. 113].

Система діяльності підприємства організаційно складається з таких частин, як:

організаційно-управлінська діяльність;

фінансова;

комерційна або інша основна діяльність підприємства;

кадрова;

із гарантування власної безпеки.

Кожна структурна ланка має свої функціональні обов'язки і вирішує своє конкретне завдання. Водночас кожна структурна ланка і кожен співробітник працюють для досягнення загальної мети: підвищення добробуту підприємства, збільшення його прибутку. Від того, як буде реалізована ця мета, залежатиме їх особисте благополуччя, їх особистий прибуток.

Служба безпеки як відділ підприємства вирішує завдання:

організації захисту економічних інтересів на підприємстві;

гарантування безпеки спеціальними засобами і методами.

Виконуючи організаційну функцію, служба безпеки працює у взаємодії з дирекцією і відділами (функціональними ланками) підприємства.

Служба безпеки спільно з дирекцією забезпечує:

ухвалення правильних управлінських рішень (забезпечує керівництво інформацією, веде аналітичну роботу);

управління системою безпеки (консультує керівництво з питань захисту економічних інтересів);

створення режиму збереження комерційної таємниці (розробляє правила, що забезпечують його дотримання);

надання допомоги і здійснення контролю за діяльністю всіх функціональних ланок підприємства.

Служба безпеки спільно з відділами забезпечує:

здійснення комерційних операцій (бере участь у підготовці контрактів, перевіряє надійність партнерів, відстежує виконання взятих ними зобов'язань);

підбір, перевірку і підготовку персоналу;

навчання персоналу прийомів поведінки і правил спілкування, формування загальної і особистої зацікавленості, створення на підприємстві обстановки пильності.

Служба безпеки самостійно працює спеціальними засобами і методами:

у середовищі працівників підприємства;

у середовищі партнерів і конкурентів підприємства.

Отже, в підприємницькій діяльності гарантування безпеки – цілісне явище, що має свою чітку структуру й систему. Перед нею стоїть конкретна мета, якої досягають вирішенням управлінських і специфічних завдань.

Діяльність із гарантування безпеки на підприємстві спрямована на конкретні об'єкти і здійснюється особливими засобами і методами. Вона тісно пов'язана з діяльністю всіх функціональних ланок підприємства і має здійснюватися комплексно. Будучи підсистемою організації, ця діяльність має здійснюватися з позицій сучасного менеджменту – науки, практики і мистецтва управління виробництвом, послугами, збутом, персоналом відповідно до умов ринкової економіки, демократичних і економічних свобод.

Організація як самокерована система, з одного боку, є елементом загального ринкового організму, з другого – самостійною спільністю із специфічним внутрішнім середовищем, здатним в умовах конкуренції до ефективної діяльності і розвитку. Тому системний підхід тут особливо важливий. Саме система здатна швидко реагувати на зміни, їх відпра-

цювання, аналіз, вибір альтернативних рішень щодо виниклих нестандартних ситуативних проблем або завдань [47, с. 114–115].

Основною метою підсистеми безпеки фірми є запобігання: збитку в її діяльності за рахунок розголошення, просочування інформації та несанкціонованого доступу до джерел конфіденційної інформації; розкраданню фінансових і матеріально-технічних коштів, знищенняю майна і цінностей; порушенню роботи технічних засобів забезпечен ня виробничої діяльності, зокрема засобів інформатизації, а також запобігання збитку персоналу організації.

Завданнями підсистеми безпеки фірми є:

своєчасне виявлення й усунення загроз персоналу і ресурсам; причин і умов виникнення фінансового, матеріального і мо рального збитку інтересам фірми, порушення її нормального функціонування і розвитку;

віднесення інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації, належного захисту від неправомірного використан ня), а інших ресурсів – до різних рівнів уразливості (небезпеки) і до категорії тих, що підлягають збереженню;

створення механізму і умов оперативного реагування на загрози безпеки і прояви негативних тенденцій у функціонуванні фірми;

ефективне припинення посягань на ресурси і загроз персоналу на основі комплексного підходу до безпеки;

створення умов для максимально можливого відшкодування й локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, для ослаблення негативного впливу наслідків порушення безпеки на досягнення стратегічної мети [47, с. 115–116].

Організаційна структура підсистеми безпеки організації може бути різною залежно від виду підприємства (банк, фірма), його розмірів, форм власності тощо. Створювати її слід усвідомлено й раціонально, максимально використовуючи досвід фахівців у сфері безпеки бізнесу.

Структура, чисельність і склад служби безпеки визначаються реальними потребами фірми і ступенем конфіденційності її інформації. Залежно від розмірів і потужності організації її безпека і захист інформації можуть бути гарантовані по-різному: від абонементного обслуговування силами приватних охоронних і детективних структур до розгортання повномасштабної власної служби і системи безпеки з розвиненою структурою і штатною чисельністю.

У своїй діяльності служба безпеки керується:

інструкцією з організації режиму і охорони;

інструкцією щодо захисту комерційної таємниці; переліком відомостей, що становлять комерційну таємницю;

інструкцією щодо роботи з конфіденційною інформацією для керівників, фахівців і технічного персоналу;

інструкцією щодо організації зберігання справ, що містять конфіденційну інформацію, в архіві;

інструкцією щодо інженерно-технічного захисту інформації;

інструкцією про порядок роботи з іноземними представниками і представництвами та ін.

Служба безпеки фірми завжди має бути готовою до подолання критичної (кризової) ситуації, що може виникнути через зіткнення інтересів бізнесу та злочинного світу. Для управління безпекою багато які фірми створюють так звані кризові групи, у складі яких працюють керівник фірми, юрист, фінансист і керівник служби безпеки. Головна мета діяльності кризової групи – протидіяти зовнішнім загрозам для безпеки фірми.

Служба безпеки будь-якої фірми постійно виконує певний комплекс завдань. Головними з них для будь-якої фірми є такі [47, с. 116–118]:

1) гарантування безпеки виробничо-господарської діяльності та захисту відомостей, що вважаються комерційною таємницею фірми (підприємства, організації);

2) організація роботи з правового та інженерно-технічного захисту комерційної таємниці фірми;

3) запобігання необґрунтованому допуску й доступу до відомостей та робіт, які становлять комерційну таємницю;

4) організація спеціального діловодства, яке унеможливлює несанкціоноване одержання відомостей, віднесених до комерційної таємниці відповідної фірми;

5) виявлення і локалізація можливих каналів витоку конфі денційної інформації в процесі звичайної діяльності та в ек стремальних ситуаціях;

6) забезпечення режиму безпеки за здійснення всіх видів діяльності, зокрема зустрічі, переговори й наради у рамках ділової співпраці фірми з іншими партнерами;

7) забезпечення охорони приміщень, устаткування, офісів, продукції і технічних засобів, необхідних для виробничої або іншої діяльності;

8) забезпечення особистої безпеки керівництва та провідних менеджерів і спеціалістів фірми;

9) оцінка маркетингових ситуацій та неправомірних дій конкурентів і зловмисників.

Перелік конкретних завдань щодо гарантування безпеки фірми залежно від специфіки її діяльності може бути більшим або меншим, але завжди достатнім та обґрунтованим.

Сукупність конкретних завдань, що стоять перед службою безпеки фірми, зумовлює певний набір виконуваних нею функцій:

організація і забезпечення пропускного та внутрішньооб'єктного ре-у жиму в приміщеннях; порядок несення служби; контроль дотримання вимог режиму персоналом фірми і партнерами (відвідувачами);

участь у розробці основоположних документів (статуту, правил внутрішнього розпорядку, договорів тощо) з метою відображення в них вимог забезпечення безпеки й захисту комерційної таємниці;

розробка та здійснення заходів із забезпечення роботи з документами, у що містять відомості, які є комерційною таємницею, контроль виконання вимог матеріалів інструктивного характеру;

виявлення і перекриття можливих каналів витоку конфіденційної інформації, облік та аналіз порушень режиму безпеки працівниками фірми, клієнтами та конкурентами;

організація та проведення службових розслідувань за фактами розголошення або втрати документів, інших порушень безпеки фірми;

розробка, оновлення і поповнення переліку відомостей, що становлять комерційну таємницю, та інших нормативних актів, які регламентують порядок забезпечення безпеки й захист інформації;

забезпечення суворого виконання вимог нормативних документів з питань захисту комерційної таємниці;

організація та регулярне проведення навчання працівників фірми і служби безпеки за всіма напрямами захисту комерційної таємниці;

ведення обліку сейфів і металевих шаф, у яких дозволене постійне чи тимчасове зберігання конфіденційних документів, а також облік та охорона спеціальних приміщень і технічних засобів у них;

підтримка контактів із правоохоронними органами та службами безпеки сусідніх підприємств (організацій) в інтересах вивчення криміногенної обстановки в районі (зоні) [47, с. 117].

4.2. Структура та особливості управління діяльністю служби безпеки підприємства

Очолює службу безпеки начальник служби на посаді заступника керівника фірми з безпеки.

Органами управління безпекою великого підприємства є:

дирекція фірми – вищий орган управління;

правління служби безпеки – виконавчий орган.

До складу правління зазвичай входять начальник служби безпеки, заступник начальника служби безпеки, секретар-інспектор.

Начальник служби безпеки є безпосереднім керівником персоналу служби безпеки. Він підпорядковується директорові підприємства або одному із його заступників відповідно до штатного розпису. Начальник служби безпеки здійснює керівництво діяльністю служби безпеки, вирішує всі організаційні питання, пов'язані з діяльністю служби безпеки, крім тих, що стосуються виключної компетенції дирекції підприємства.

Начальника служби безпеки призначає дирекція підприємства з осіб, що мають вищу освіту. Директор фірми укладає з ним трудовий договір, у якому обумовлено всі посадові обов'язки та умови праці.

Начальник служби безпеки без додаткового доручення діє від імені служби безпеки у всій своїй діяльності, має право підпису всіх правових і бухгалтерських документів служби безпеки, визначає посадові оклади її працівників, вирішує питання щодо надання чи позбавлення премій, інших видів заохочення та мотивування, укладає трудові до говори із працівниками служби безпеки тощо.

На час відпустки чи відрядження начальник служби безпеки делегує свої права заступникові.

Начальник служби безпеки відповідає за:

надання охоронних і пошукових послуг з метою безпеки фірми і суворого дотримання чинного законодавства України;

забезпечення збереженості спеціальних засобів, зброї, боєприпасів, що придбані підприємством;

якість професійної підготовки осіб зі складу служби безпеки.

Начальнику служби безпеки не дозволяється суміщати охоронну діяльність із державною службою чи виборною оплачуваною посадою в громадських об'єднаннях, а також надавати послуги особисто чи через своїх підлеглих, що пов'язані із забезпеченням безпеки інших підприємств.

Підбираючи начальника служби безпеки, ставлять насамперед два питання, що стосуються його професіоналізму і лояльності. Відповідно до виконуваних ним функцій він має знати не просто дані про підприємство, а всі проблемні аспекти його роботи, весь негатив, а деколи й дуже багато про особисте життя керівництва фірми. Тому підбір особи на таку посаду має бути дуже чітким і обдуманим.

При підборі кандидата на посаду начальника служби безпеки слід чітко визначити пріоритети його роботи. Такими пріоритетами можуть бути загрози з боку конкурентів, боротьба з шахрайством персоналу, протидія кримінальним угрупованням чи нейтралізація дії силових структур. Залежно від цього і потрібно шукати спеціаліста. Якщо головна проблема – силові структури, кращим буде працівник з керівної посади в цих структурах з відповідними налагодженими зв'язками. Якщо кримінал, то працівник має досвід роботи з ним і досвід створення відповідних систем безпеки. Якщо конкуренти, важливим є досвід збору інформації та аналізу економіки підприємства.

У найзагальнішому вигляді процес управління складається з трьох стадій, кожна з яких охоплює послідовно здійснювані етапи або операції:

I стадія: збирання, оброблення, узагальнення та аналіз інформації;

II стадія: вироблення і ухвалення управлінського рішення;

III стадія: організація виконання управлінського рішення.

Така структура процесу управління не є загально прийнятою, яку слід копіювати в управлінні діяльністю служби безпеки.

Відповідно до специфіки діяльності служби безпеки та її зовнішнього оточення слід (у межах зазначеної структури) виробляти свій підхід до процесу управління. Наведемо варіант структури процесу управління:

I. Оцінка обстановки.

1. Преамбула.

2. Формулювання обмежень і критеріїв ухвалення рішення.

3. Формування набору альтернативних вирішень проблеми.

4. Оцінка альтернатив.

II. Оцінка конкуруючих сил на ринку послуг (виробництві) – злочинних елементів (груп) у регіоні (зоні) дислокації фірми.

III. Оцінка своїх сил.

5. Технічне забезпечення захисту фірми.

6. Фізичне забезпечення захисту.

7. Якісна характеристика працівників служби безпеки.

IV. Оцінка фірм, що співпрацюють і взаємодіють на ринку послуг.

V. Організація взаємодії постів і порядок їх посилення за різних режимів діяльності.

VI. Організація зв'язку між постами для забезпечення взаємодії.

VII. Організація взаємодії з органами МВС.

VIII. Дія сил і засобів служби безпеки при порушенні режимів за хисту.

IX. Забезпечення охорони провідних фахівців фірми, їх сімей і власності.

Таким чином, раціональне впровадження в практику основних елементів системи, механізму і процесу управління дає змогу керівництву служби безпеки значно підвищити ефективність управлінської дії на результати її діяльності.

Багатогранність сфери гарантування безпеки фірми, зокрема захист її комерційної таємниці, вимагає створення спеціальної служби для реалізації всіх захисних заходів.

Структура, чисельність і склад служби безпеки фірми визначаються реальними фінансовими можливостями, масштабом комерційної діяльності, ступенем конфіденційності інформації. Залежно від цих чинників служба безпеки може налічувати від 2 – 3 осіб, що працюють за сумісництвом, до чисельності працівників повномасштабної служби з розвиненою структурою [47, с. 124–127].

4.3. Організація праці та функції менеджера з економічної безпеки

Основною складовою економічної безпеки підприємства є фінансова складова. У зв'язку з цим процес управління економічною безпекою можливо звести до управління ризиками, що можуть призвести до певних втрат прибутку. Отже, в цьому випадку система управління може розглядатись як ризик-менеджмент, що включає процес вироблення мети ризику і ризикових вкладень капіталу, визначення вірогідності настання події, виявлення ступеня й величини ризику, аналіз навколишнього оточення, вибір стратегії управління ризиком, визначення необхідних для даної стратегії прийомів управління ризиком і способів його зниження, здійснення цілеспрямованої дії на ризик. Вказані процеси в сукупності складають етапи організації ризик-менеджменту як підґрунтя діяльності менеджера з питань економічної безпеки, зокрема в фінансовій сфері.

Фінансовий менеджер, що займається питаннями ризику, повинен мати два права: право вибору рішення і право відповідальності за нього. Рішення повинне ухвалюватися менеджером одноособово. У ризик-менеджменті через його специфіку недоцільне колективне ухвалення рішення, за яке ніхто не несе ніякої відповідальності. Крім того, колективне рішення через психологічні особливості окремих людей є більш суб'єктивним, ніж рішення, що приймається окремим фахівцем.

Система управління економічною безпекою підприємства є достатньо динамічною. Ефективність її функціонування багато в чому залежить від швидкості реакції на зміни умов ринку, економічної ситуації, фінансового стану об'єкта управління.

У фінансовій сфері органом управління економічною безпекою може бути фінансовий менеджер, менеджер з ризику або відповідний апарат управління: сектор страхових операцій, сектор венчурних інвестицій, тощо. Ці сектори або відділи є структурними підрозділами фінансової служби компанії, а отже, і системи управління економічною безпекою підприємства в цілому.

Відділ ризикових вкладень капіталу може здійснювати такі функції:

проводити венчурні і портфельні інвестиції;

розробляти програму ризикової інвестиційної діяльності;

збирати, обробляти, аналізувати і зберігати інформацію про навколишнє оточення та його загрози;

визначати ступінь і вартість ризиків, стратегію і прийоми управління ризиком;

розробляти програму ризикових рішень й організовувати її виконання, включаючи контроль і аналіз результатів;

здійснювати страхову діяльність, укладати договори страхування і перестраховки;

розробляти умови страхування і перестраховки;

вести відповідну бухгалтерію, статистичну і оперативну звітність за ризиковими вкладеннями капіталу та дією відповідних загроз.

До функцій фінансового менеджера в системі управління економічною безпекою можна віднести такі:

прогнозування;

організація;

регулювання;

координація;

стимулювання;

контроль.

Прогнозування є розробкою на перспективу змін фінансового стану об’єкта. Прогнозування – це передбачення певної події. Особливістю прогнозування є також альтернативність в побудові фінансових показників, що визначає різні варіанти розвитку фінансового стану об’єкта управління на основі тенденцій, що намітилися. Управління на основі передбачення цих змін вимагає вироблення у менеджера певного чуття ринкового механізму й інтуїції, а також застосування гнучких, екстрених рішень.

Організація в управління економічною безпекою є об’єднанням людей, що спільно реалізують, наприклад, програму ризикового вкладення капіталу на основі певних правил.

Регулювання – дія на об’єкт управління з метою усунення відхилень в певних критеріях економічної безпеки, що виникли. Головним чином це поточні заходи.

Координація – забезпечення узгодженості роботи всіх ланок системи управління економічною безпекою.

Стимулювання в управлінні економічною безпекою представляє спонуку фахівців до зацікавленості в результаті своєї праці.

Контроль є перевіркою організації роботи щодо зниженню ступеня дії відповідних зовнішніх і внутрішніх загроз. За допомогою контролю забезпечується інформація про ступінь виконання наміченої програми дій, зокрема прибутковість ризикових вкладень капіталу, співвідношення прибутку та ризику.

Як форма підприємницької діяльності, управління економічною безпекою підприємства є творчою діяльністю [143].

5. Недобросовісна конкуренція та захист комерційної таємниці

5.1. Сутність комерційної таємниці підприємства

На думку західних теоретиків-економістів, успішний розвиток підприємництва значною мірою залежить від політико-економічного середовища (командно-адміністративного або ринково-конкурентного), в якому відбувається ринкова діяльність. Проте не менш важливим чинником, що формує економічне середовище, є криміногенна ситуація, які утруднює

або зводить нанівець дії підприємця. Наявність умов, за яких виникає реальна загроза завдання шкоди (збитків) суб'єкту господарювання, визначає першочерговим оперативне рішення проблеми гарантуванні економічної безпеки.

У ринкових умовах підприємницька діяльність у нашій країні здійснюється в ситуації наростаючої невизначеності та мінливості економічного середовища. Отже, виникає неясність і невпевненість в отриманні очікуваного кінцевого результату, тому зростає ризик непередбачених втрат. Особливо це спостерігається на початку освоєння підприємництва.

В умовах командно-адміністративної економіки всі звикли до того, що економічна обстановка формується "зверху", в наказовому порядку, у вигляді набору правил і норм. Плани, програми, ухвали інструкції, державні ціни, фонди, ліміти, наряди, тарифи формували ту економічну систему і те господарське середовище, в яких змушені були діяти підприємства і люди.

Звичайно, жорстка система централізованих настанов і розпоряджень сковувала ініціативу, пригнічувала зацікавленість і творчий пошук. Але вона забезпечувала явну або удавану чіткість, нав'язаний "порядок".

В ринковій економіці інформація стає товаром і має підпадати законам товарно-грошових відносин. Кожен власник має право відстоювати свої інтереси, узгоджені з інтересами інших власників і суспільства.

Багато питань підприємницької діяльності регулюються і забезпечуються цивільним, адміністративним, трудовим, авторським, кримінальним та іншими видами законодавства, і говорити нині про те, що за допомогою тільки правового регулювання і охорони можна вирішити всі проблеми, пов'язані із гарантуванням безпеки підприємництва, не тільки передчасно, а й, як свідчить практика, не реально в найближчому майбутньому.

Ринок – це передусім економічна свобода. Над підприємцем можуть стояти тільки закон і встановлювані ним обмеження. Державне регулювання в умовах ринку полягає переважно у встановленні норм здійснення підприємницької діяльності і податкової системи. Решта визначається виробником і споживачем, а деякою мірою складається випадково.

За економічну свободу доводиться платити. Адже свобода одного підприємця водночас супроводжується і свободою інших підприємців, які вільні купувати чи не купувати його продукцію, пропонувати за неї свої ціни, продавати йому свою продукцію за певними цінами, диктувати свої умови операцій. При цьому природно, що ті, з ким до водиться вступати

в господарські відносини, насамперед добиваються своєї вигоди, а вигода одних може стати збитком для інших. До того ж, підприємець-конкурент взагалі схильний витісняти свого опонента з ринку.

У нових ринково-конкурентних умовах виникає багато проблем, пов'язаних із гарантуванням безпеки не тільки фізичних і юридичних осіб, їх майнової власності, а й підприємницької (комерційної) інформації як виду інтелектуальної власності. Для захисту підприємницьких інформаційних потоків від різних посягань застосовують як правові, так і спеціальні заходи, а за потреби – їх комплекс.

Сукупність відомостей, які використовують у підприємницькій діяльності, можна умовно згрупувати за такими напрямами:

а) підприємницька (комерційна) інформаційна система (відомості про стан економічної системи; чинники, які позитивно чи негативно впливають на сферу господарювання і комерції, в якій діє підприємець);

б) правова інформаційна система (відомості про чинне законодавство, що регулює й охороняє діяльність підприємницьких (комерційних) структур);

в) спеціально-оперативна інформаційна система (відомості про способи, сили і засоби гарантування безпеки підприємницької інформації від доступу третіх осіб) [47, с. 302–303].

Підприємницька діяльність у всіх сферах нерозривно пов'язані отриманням і використанням різних видів інформації. Причому нині інформація є особливим товаром, що має конкурентну вартість. Для підприємця часто найбільш цінною є інформація, яку він використав для досягнення мети фірми і розголошування якої може позбавити його можливості вирішувати ці завдання, тобто створює загрозу безпеці підприємницької діяльності. Звичайно, не вся інформація може, в разі її розголошування, створювати таку загрозу, проте існує певна інформація, яка потребує захисту.

Інформація, яку використовують у підприємницькій діяльності вельми різноманітна. Її можна поділити на два види: промислова і комерційна. До промислової належать: інформація про технологію і спосіб виробництва, технічні відкриття і винаходи, ноу-хау; конструкторська документація, програмне забезпечення тощо. Комерційна інформація – це відомості про фінансово-економічне становище підприємства (бухгалтерська звітність), кредити банківські операції, про укладені договори, контрагентів, структуру капіталів і плани інвестицій, стратегічні плани марке-

тингу, аналіз конкурентоспроможності власної продукції, клієнтів, плани виробничого розвитку, ділове листування та ін. [47, с. 304].

Відповідно до Закону України "Про інформацію", громадяни, юридичні особи, що володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, отриманою власним коштом або такою, котра є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної і встановлюють для неї систему (способи) захисту. Для цього, крім наказу про комерційну таємницю, підприємства можуть складати посадові інструкції із зазначенням порядку і системи обміну інформацією між працівниками підприємства і зовнішніми користувачами, деталізований графік документообігу із призначенням осіб, відповідальних за витік інформації, вносити спеціальні розділи в трудові угоди та контракти тощо.

У наведеному далі переліку відомості, що становлять комерційну таємницю, згруповано за тематичним принципом. Пропонований поділ на групи має рекомендаційний характер і може бути змінений залежно від специфіки відомостей, що становлять комерційну таємницю конкретного підприємства (організації). Відомості, введені в цей перелік, є комерційною таємницею тільки з урахуванням особливостей конкретного підприємства.

1. Відомості про фінансову діяльність:

прибуток, кредити, товарообіг;

фінансові звіти і прогнози;

комерційні задуми;

фонд заробітної плати;

вартість основних і оборотних фондів;

кредитні умови платежу;

банківські рахунки; планові звітні калькуляції.

2. Інформація про ринок:

ціни, знижки, умови договорів, специфікація продукції;

обсяг, історія, тенденції виробництва і прогноз для конкретного продукту;

ринкова політика і плани;

маркетинг і стратегія цін;

відносини зі споживачами і репутація;

чисельність і розміщення торгових агентів;

канали і методи збуту;

політика збуту;

програма реклами.

3. Відомості про виробництво і продукцію:

технічний рівень, техніко-економічні характеристики проектованих виробів;

плановані терміни створення проектованих виробів;

застосовування і перспективні технології, технологічні процеси, прийоми і устаткування;

дані про модифікацію і модернізацію раніше відомих технологій, процесів, устаткування;

виробничі потужності;

стан основних і оборотних фондів;

організація виробництва;

розміщення і розмір виробничих приміщень і складів;

перспективні плани розвитку виробництва;

технічні специфікації існуючої і перспективної продукції;

схеми і креслення окремих вузлів, готових виробів, нових розробок;

стан програмного і комп'ютерного забезпечення;

оцінка якості та ефективності;

номенклатура виробів; спосіб упаковування;

доставка.

4. Відомості про наукові розробки:

нові технологічні методи, нові технічні, технологічні і фізичні принципи, заплановані для використання в продукції підприємства;

програми НДР;

нові алгоритми;

оригінальні програми.

5. Відомості про систему матеріально-технічного забезпечення:

склад торгових клієнтів, представників і посередників;

потреби в сировині, матеріалах, комплектувальних вузлах і деталях, джерела задоволення цих потреб;

транспортні й енергетичні потреби.

6. Відомості про персонал підприємства:

чисельність персоналу підприємства;

визначення осіб, що приймають рішення, та їхня філософія.

7. Відомості про принципи керівництва підприємством:

застосовувані і перспективні методи керівництва виробництвом;

факти ведення переговорів, предмет і цілі нарад і засідань органів керування;

плани підприємства щодо розширення виробництва; умови продажу і злиття фірм.

8. Інші відомості:

важливі елементи систем безпеки, кодів і процедур доступу до інформаційних мереж і центрів;

принципи організації захисту комерційної таємниці [47, с. 305–306].

Інформація фірми, що становить комерційну таємницю, за важливістю може належати до чотирьох рівнів:

1. Життєво важлива – незамінна інформація, наявність якої стратегічно необхідна для функціонування підприємства. Витік цієї інформації ставить під загрозу самофункціонування організації (підприємства).

2. Важлива – інформація, процес ліквідації наслідків витоку якої складний або пов'язаний з великими витратами.

3. Корисна – інформація, витік якої завдає матеріальної шкоди підприємству, однак воно може ефективно функціонувати й у разі витоку цієї інформації.

4. Неістотна – інформація, витік якої не завдає матеріального збитку підприємству і не впливає на його функціонування [47, с. 306–307].

Інформація, що належить до перших трьох рівнів, є комерційною таємницею.

Уся ця інформація має різну цінність для підприємця, і розголошування її може призвести (або не призвести) до загроз економічній безпеці різного ступеня важкості. Тому інформацію доцільно поділяти на три групи:

а) інформація для відкритого користування будь-яким споживачем у будь-якій формі;

б) інформація обмеженого доступу – тільки для органів, що мають відповідні законодавчо встановлені права (міліція, податкова поліція, прокуратура);

в) інформація тільки для працівників (або керівників) фірми.

Інформація, що належить до другої і третьої груп, є конфіденційною і має обмеження у розповсюдженні.

Отже, конфіденційна інформація – це документована (тобто зафіксована на матеріальному носієві і з реквізитами, що дають змогу іденти-

фікувати її) інформація, доступ до якої обмежується відповідно до законодавства України. Частина цієї комерційної інформації становить особливий блок, і її можна віднести до комерційної таємниці.

Комерційна таємниця підприємства – це інформація, що не є державним секретом і пов'язана з виробництвом, технологічною інформацією, управлінням, фінансами та ін. Розголошування (передача, витік) її може завдати збитку інтересам фірми. Така загальна характеристика категорії "комерційна таємниця" підприємства є законодавчо правильною [47, с. 307].

Узагальнення різних поглядів вітчизняних і зарубіжних авторів дає змогу дати розширене трактування цієї складної категорії. У найбільш загальному вигляді вона охоплює інформацію про:

торговельні відносини фірм;

організацію і розміри обороту засобів;

стан ринку збуту;

банківські операції;

постачальників і споживачів;

сутність патентів;

структуру капіталів;

плани інвестицій;

укладені контракти;

формування ціни на товар;

розмір прибутку і обсяг виробництва.

До виробничої таємниці належить інформація про:

способи виробництва і технології;

організацію праці;

технічні відкриття і винаходи;

мета і характер дослідницьких робіт.

Доцільно також у загальному обсязі комерційної інформації виділити два основні блоки. Такий підхід передбачає, що до категорії науково-технічної і технологічної інформації належать відомості про конструкцію машин і устаткування, використовувані матеріали, методи і способи виробництва, дизайн, програмне забезпечення та ін.

До категорії ділової належить інформація про:

фінанси підприємства (фінансова звітність, стан розрахунків з клієнтами, заборгованість, кредити, платоспроможність, прибуток, собівартість продукції та ін.);

стратегічні й тактичні плани розвитку виробництва, зокрема з використанням нових технологій, винаходів, ноу-хау;

плани та обсяги реалізації продукції (плани маркетингу, характер і обсяг торговельних операцій, рівень цін, складські запаси);

аналіз конкурентоспроможності своєї продукції, ефективності експорту й імпорту, передбачуваний час виходу на ринок; плани рекламної діяльності;

списки торгових та інших клієнтів, конкурентів, відомості про взаємини з ними, їх фінансове становище, умови контрактів та ін.;

методи і організацію управління;

власну оцінку характеру і репутації персоналу та підприємства;

систему організації праці [47, с. 308–309].

На практиці керівники та підприємці не завжди цілком чітко уявляють собі, що означає поняття "комерційна таємниця", як її слід охороняти і як результати подібної роботи можуть впливати на економічний стан підприємства.

За оцінками експертів, втрата лише чверті інформації, що належить до комерційної таємниці, забезпечує вагомі переваги конкурентам і протягом кількох місяців призводить до банкрутства половини фірм, що припустилися витоку інформації. Є всі підстави вважати, що в процесі розвитку ринкових відносин із властивими їм конкуренцією і господарським розрахунком підходи до охорони комерційної таємниці радикально зміняться.

У ринковій економіці інформація є товаром і її отримання, зберігання, передача та використання мають відповідати законам товарно-грошових відносин. Кожен власник має право охороняти свої інтереси і захищати необхідну інформацію, отримуючи при цьому певну свободу підприємництва. Право на таємницю означає обмеження державного втручання в економічне життя підприємства і захист його інтересів під час взаємодії з іншими суб’єктами ринкових відносин. На відміну від державних і військових таємниць, комерційна таємниця є власністю конкретного підприємства. Її головне призначення – забезпечувати підприємству економічні переваги в конкурентній боротьбі.

За нинішніх ринкових конкурентних відносин просочування інтелектуальної інформації може негативно позначитися на становищі підприємства в боротьбі за споживача. Саме тому тепер доцільно юридично точно визначати категорію і правовий статус комерційної таємниці, розробляти механізм відповідальності за її розголошування. Інтереси окре-

мих підприємств мають бути підпорядковані інтересам країни. Паралельно із розвитком приватизації і становленням підприємництва в нашій країні потрібно створити систему, що забезпечує продаж інформації підприємства за кордон без збитку для держави в цілому. У промислово розвинених країнах аналоги таких систем є. Вони передбачають різні ефективні методи економічної дії на приватних підприємців, котрі на збиток національним інтересам країни дозволяють собі порушувати заборони держави на експорт науково-технічної продукції.

Економічна безпека підприємств порушується насамперед тоді, коли його співробітники працюють за сумісництвом в інших місцях, використовуючи при цьому документацію (методики, креслення, програми та ін., створену на основному підприємстві, але юридично не закріплену в його власності. Адже саме ця інтелектуальна продукція (знання й технологія) часто становить найбільш цінний капітал підприємства. Будь-який суб'єкт господарських відносин, що використовує цю інформацію, зобов'язаний укладати з підприємством договір і віддавати йому частину прибутку, отриманого від використання досягнень. Проте нинішній економічний і правовий стан опрацьовування цього питання не дає змоги підприємству – власникові інформації заявити і реалізувати свої претензії.

Для вирішення цієї проблеми доцільно законодавчо обмежити (а іноді й повністю заборонити) безкоштовне використання досвіду окремих підприємств. Водночас потрібно регламентувати порядок купівлі-продажу пріоритетних розробок з урахуванням їх реальної ринкової вартості. Підприємці мають підготуватися до переходу внутрішнього ринку на патентно-ліцензійну систему охорони промислової власності. На підприємствах доцільно зміцнити відповідні підрозділи патентно-ліцензійних відділів, ввести досвідчених фахівців у маркетингові служби, організувати власними зусиллями ефективну систему захисту інформації.

Фахівці науково-технічних, виробничих, економічних та інших служб підприємства повинні навчитися правильно й конкретно (у вартісній формі) оцінювати передбачувані та реальні втрати фірми внаслідок просочування інформації, віднесеної до категорії комерційної таємниці.

У найбільш загальному вигляді втрати підприємства від недотримання умов конфіденційності призводять до того, що [47, с. 311]:

знижуються можливості продажу ліцензій на власні наукові розробки, втрачається пріоритет в освоєних галузях науково-технічного прогре-

су, зростають витрати на переорієнтацію діяльності дослідницьких підрозділів;

виникають (створюються конкурентами) труднощі в закупівлі сировини, технології, устаткування та інших компонентів, необхідних для нормальної виробничої діяльності;

обмежується співпраця підприємства з діловими партнерами, знижується вірогідність укладання вигідних контрактів, виникають проблеми у виконанні договірних зобов'язань;

зростають витрати підприємства на створення нової ринкової стратегії, зміну структури маркетингових досліджень та ін;

виникає реальна загроза застосування економічних санкцій щодо винних у розголошуванні комерційної таємниці.

Точний вартісний розрахунок сукупного розміру всіх втрат досить складний, трудомісткий, а іноді просто неможливий через брак достовірних початкових даних. Тому в більшості випадків достатньо укрупненої експертної оцінки втрат підприємства, зумовлених недотриманням вимог захисту інформації.

Компенсація перелічених вище втрат підприємства часто вимагає значних додаткових витрат, що знижує ефективність виробництва загалом і можливість успіху в конкурентній боротьбі. Саме тому питанням захисту комерційної таємниці нині приділяється дедалі більше уваги.

5.2. Обґрунтування переліку інформації, що становить комерційну таємницю

Конфіденційну інформацію поділяють на інформацію обмеженого доступу і на секретну. До першої належать відомості, розголошування яких заподіює збитку тактичним інтересам, таким як зрив конкретного контракту, зниження відсотка прибутків від операції, ускладнення угод, виконання окремої угоди. Розголошування секретної інформації завдає збитку інтересам фірми, може поставити під загрозу саме її існування надалі. Її становлять відомості, ознайомлення з якими дає змогу конкурентам підірвати репутацію фірми в очах партнерів, заподіяти їй фінансового збитку, призвести до конфлікту з державними органами, поставити у залежність від кримінальних структур.

Вітчизняні підприємства переймають практику іноземних підприємств, яка передбачає чотири способи визначення поняття "комерційна таємниця" [47, с. 314, 316]:

1. Тотальний. Суть цього методу дуже проста. Ознайомившись із переліком Закону України "Про комерційну таємницю", в якому зазначено, що не може бути комерційною таємницею, потрібно просто методом виключення все, що залишилося, визнати комерційною таємницею підприємства. Таким чином, таємницею буде вся інформація підприємства. Цей спосіб найбільш простий і найменш ефективний. Справді, дуже легко оголосити всю інформацію, що підлягає захисту, секретом. Проте відкритим залишається питання щодо її захисту.

2. Плагіаторський. Теж достатньо легкий спосіб. Треба просто з'ясувати, яку саме інформацію партнери вважають комерційною таємницею, і так само вчинити на підприємстві. Природно, що повного списку ніхто з конкурентів не надасть, але підказати, які саме сфери діяльності підлягають засекречуванню, конкуренти зможуть надати. Можливо також просто ознайомитись із спеціальними матеріалами і літературою, що досліджує ці теми. Зазвичай як допоміжну інформацію там подано перелік інформації, яка може бути віднесена до комерційної таємниці. Проблема тільки в тому, що все, що вдасться дізнатися у такий спосіб, буде швидше рекомендацією, з якої потрібно створити необхідний продукт. У комерційній таємниці є достатньо універсальних положень, які підходять абсолютно для всіх. У кожній ситуації потрібна індивідуальна робота, що враховує всі нюанси й особливості. Те, що одні вважають таємним, може бути відкритим в інших випадках і навпаки.

3. Аналітичний. Цей спосіб дещо складніший за перелічені, але і набагато ефективніший. Спосіб полягає у "рольових іграх", його використовують психологи, слідчі, маркетологи та ін. Необхідно уявити, яка саме інформація про конкурентів була б особливо корисною, і розглянути ситуацію щодо власного підприємства. Отримані таким чином результати після певного опрацювання і слід визнати комерційною таємницею. Природно, що такі "сеанси перевтілення" слід проводити регулярно, адже підприємство розвивається. Результат такої роботи, якщо вона проведена зі всією серйозністю, може бути дуже ефективним.

4. Експертний. Якщо в описах попередніх способів були ситуації, коли бізнесмен намагається самостійно вирішити свої проблеми, то в цьому разі потрібно звернутися за допомогою до фахівців. Природно,

професіонал, що займається захистом комерційної таємниці, здатний зробити це набагато краще за будь-яку непідготовлену особу. Люди, чиєю професією є захист і безпека, мають відмінну підготовку, підкріплену практичним досвідом. І для них не становитиме особливих труднощів виконати свою роботу.

Якнайкращим рішенням є створення власної служби безпеки, що складається хоча б з кількох працівників, які займаються безпосередньо питаннями захисту. На жаль, мати службу безпеки може не кожне підприємство. Тоді до вирішення питання залучають фахівця-консультанта. Доцільно не просто одноразово залучати такого спеціаліста для надання послуг, а регулярно звертатися до нього по допомогу.

У будь-якому разі до інформації, що становить комерційну таємницю, належать:

кредитні договори з банками;

договори купівлі і продажу, починаючи від певної суми;

відомості про перспективні ринки збуту, джерела коштів або сировини, товари, вигідних партнерів;

будь-яка інформація, надана партнерами, якщо за її розголошування передбачені штрафні санкції.

Для безпосереднього визначення переліку відомостей, що становлять комерційну таємницю, на підприємстві можна створити спеціальну комісію, яка займатиметься групуванням і уточненням інформації з цього переліку. Чисельність членів такої комісії – не більше 4 – 5 осіб. Створюють її з найбільш кваліфікованих і компетентних фахівців основних підрозділів та представників служби безпеки підприємства, ознайомлених як із діяльністю підприємства в цілому, так і з роботою окремих підрозділів. До складу комісії бажано вводити [47, с. 317–318]:

фахівця, який володіє фінансовими питаннями, кон’юнктурою ринку та інформацією про діяльність конкуруючих фірм (як правило, це фінансовий менеджер);

фахівця, який досконало знає систему організації роботи підприємства, її особливості;

фахівця з питань зв’язків з іншими підприємствами, а також з укладення контрактів і договорів;

фахівця, який володіє всіма відомостями про продукцію, що випускається, її технологічний цикл і виробництво, про проходження усіх видів

інформації (усної, документальної, у вигляді зразків, вузлів, блоків, готової продукції).

У разі якщо підприємство є великим або виготовлена ним продукція досить різнорідна, можна створити кілька таких груп: одну – головну для координації та узагальнення результатів роботи, інші – залежно від потреби – за кожною окремою виробничою ділянкою.

Проте підприємство може складатися лише з кількох осіб, особливо на початкових етапах розвитку. Тоді такої мети справді здатен досягти один керівник за умови, що він володіє всією необхідною інформацією. Однак, щоб уникнути суб'єктивних помилок, краще розглядати ці питання щонайменше удвох.

Як уже зазначалося, у групі мають бути провідні фахівці, які володіють повним обсягом даних, що можуть бути віднесені до комерційної таємниці. Однак це не означає, що варто обов'язково ознайомлювати всіх залучених експертів з конкретною інформацією, яка може становити комерційну таємницю, якщо раніше вони її не знали.

Достатньо, коли хоча б один із них був детально обізнаний з окремим питанням, що розглядається, а інші мали про нього загальне уявлення. Такий підхід зробить роботу групи більш раціональною і зможе на першому етапі усунути можливі передумови для необґрунтованого поширення комерційної таємниці.

Отже, перед групою експертів потрібно поставити комплекс завдань у такій послідовності [47, с. 318]:

а) виділити всі види діяльності підприємства, що приносять прибуток на даний момент;

б) за наявними даними про ринок збуту оцінити, чи перевищує рівень прибутку з певного виду діяльності аналогічні показники на інших підприємствах;

в) визначити ймовірну перспективу рентабельності цієї діяльності.

Якщо з економічного погляду зазначений вид діяльності відповідає цілям підприємства і нині, і в перспективі, а прибуток вищий, ніж у конкуруючих фірм, то експерти мають визначити, що саме в цьому виді діяльності дає змогу отримувати прибуток. Відповідь на це питання і буде комерційною таємницею підприємства. Так, для відомостей наукового характеру це зазвичай:

ідеї, винаходи, відкриття;

окремі формули;

нові технічні проекти;

нові методи організації праці та виробництва;

програмне забезпечення;

результати наукових досліджень.

Для відомостей технологічного характеру:

конструкторська документація, креслення, схеми, записи;

описи технологічних процесів;

ноу-хау;

точні знання конструкційних характеристик виробів та оптимальних параметрів розроблюваних технологічних процесів (розміри, обсяги, конфігурація, зміст компонентів у відсотках, температура, тиск, час тощо);

відомості про матеріали, з яких виготовлені окремі деталі, умови експериментів, обладнання та устаткування, на якому вони проводилися;

окремі нові або унікальні вимірювальні комплекси, прилади, верстати й устаткування, що використовуються на підприємстві.

Для відомостей ділового характеру:

дані про укладені або заплановані контракти;

дані про постачальників і клієнтів;

огляди ринку, маркетингові дослідження;

інформація про конфіденційні переговори;

калькуляція витрат виробництва підприємства, структури цін, рівня прибутку;

плани розвитку підприємства та його інвестицій [47, с. 318–319].

Якщо у виділенні вузлових відомостей виникають проблеми, то можна розглянути вид діяльності щодо окремих технологічних етапів, логічного алгоритму дій. У будь-якому разі корисними будуть аналогічні приклади організації захисту таємниць західними фірмами.

Для уникнення незаконного та несанкціонованого розповсюдження комерційної таємниці на досліджуваному підприємстві, так само як і на інших підприємствах, потрібно під час приймання на роботу ретельно вивчати обставини індивідуального ставлення людини до потреби збереження комерційної таємниці, обставини минулої роботи людини тощо.

Отже, вивчення проблеми правового захисту комерційної таємниці дає змогу зробити висновок про необхідність подальшої законодавчої, науково-дослідної роботи та постійного розроблення практичних рекомендацій щодо вдосконалення системи організації захисту такої інформації.

5.3. Недобросовісна конкуренція та методи викрадення таємниць підприємства

Перехід від планового господарювання до ринкового, виникнення численних приватних підприємств, зниження ролі державного регулювання в різних сферах економічного життя – все це призводить до різкого посилення конкуренції між виробниками товарів та послуг. Історичний досвід показує, що загалом конкуренція сприяє розвитку продуктивних сил і прогресу суспільних відносин, проте лише тоді, коли вона має цивілізовані форми. Саме в цьому разі перевагу отримує той суперник, чия стратегія спрямована на підвищення якості пропонованих товарів і послуг, зниження цін на них, надання додаткових пільг споживачам.

Водночас протиборство між конкурентами може відбуватися з використанням нецивілізованих, недобросовісних і навіть незаконних засобів і методів. У такому разі вперед вириває не той, хто краще працює, хто більше піклується про споживача, а зухвалий злочинець. На жаль, нині в Україні, зокрема, великого поширення набули саме нецивілізовані форми конкурентної боротьби. Сприятливі умови для них створюють специфічні умови пострадянського економічного простору: загальна низька культура підприємницької діяльності, незавершеність процесу формування ринкових відносин, відсутність або неефективність багатьох законодавчих і нормативних актів, економічна нестабільність (інфляція, безробіття, неплатежі), відсутність розгалуженої системи державних органів і суспільних організацій для боротьби з нецивілізованою, недобросовісною і незаконною конкуренцією.

Основний принцип конкуренції зі знаком "мінус" полягає в прагненні зміцнити своє становище за рахунок ослаблення позицій конкурентів (аж до їх повного витіснення) або обману споживачів, або поєднанням того й іншого. Нецивілізована конкуренція відбувається у формі економічного шпигунства, корупції, брехливої реклами, компрометації окремих працівників і фірм в цілому, фальсифікації та підробки продукції конкурентів, маніпулювання з діловою звітністю для отримання різних фінансових вигод і, нарешті, за допомогою прямого обману, грабежу, завдання матеріального збитку, психологічного й фізичного придушення (аж до вбивства).

Конфіденційна інформація існує, як правило, в матеріальній формі. Це зразки продукції або товарів, різні документи, креслення, плани, схе-

ми, аналітичні огляди, моделі, каталоги, довідники, фотографії і слайди, магнітні та оптичні носії інформації.

Нерозуміння вітчизняними бізнесменами значення заходів захисту конфіденційної інформації є однією з причин небажання західних партнерів мати з ними справи. Вони приїздять, дивляться на те, як вирішуються проблеми охорони офісів, комерційних таємниць, посміхаються, підписують протоколи про наміри – і не роблять жодного кроку далі. Вони розуміють, що все вкладене ними буде або розграбовано, або використано з мінімальною ефективністю. А головне – вкрадуть їхні комерційні таємниці. Тим часом у Західній Європі і США втрата 20 % конфіденційної інформації призводить до розорення фірми протягом одного місяця [47, с. 320–321].

Відповідно до міжнародних правових норм розрізняють три види недобросовісної конкуренції [47, с. 322]:

1) коли комерційну діяльність однієї фірми прагнуть видати споживачеві за діяльність іншої;

2) дискредитація комерційної діяльності за допомогою розповсюдження помилкової інформації;

3) неправомірне використання в комерційній діяльності позначень, що вводять споживача в оману. Існуючі на Заході законодавчі акти щодо товарних знаків, фірмових найменувань, недобросовісної конкуренції визначають конкретну відповідальність за такі дії:

підкуп покупців конкурентів;

з'ясування комерційних таємниць конкурента за допомогою шпигунства або підкупу його службовців;

установлення дискримінаційних комерційних умов;

таємна змова на торгах і неофіційне створення таємних картелів;

бойкот торгівлі іншої фірми для протидії конкуренції або запобігання їй;

продаж своїх товарів за свідомо заниженою ціною з наміром протидіяти конкуренції або придушити її (демпінг);

навмисне копіювання товарів, послуг, реклами або інших видів комерційної діяльності конкурента і та ін.

Відомі три форми недобросовісної конкуренції [47, с. 323]:

1. Економічне придушення, яке передбачає різні засоби і способи обмеження ділової практики, компрометацію фірм-конкурентів, їх керівників, шантаж персоналу, зрив операцій, паралізацію діяльності фірм шляхом використання ЗМІ і мафіозних зв'язків у державних органах.

2. Промислове або комерційне шпигунство, яке має на меті протиправне заволодіння комерційними засобами конкурента для отримання власних вигод.

Якщо інформація про конкурентів, що надходить легальними каналами, не дає повної і точної відповіді на запитання, яке цікавить адміністрацію підприємства, то, незважаючи на те, що більшість серйозних підприємців вважають, що застосовувати шпигунство неетично, багато компаній все-таки вдаються до послуг комерційних шпигунів. Шпигуни конкуруючих компаній часто використовують такі засоби, як пряму пропозицію, підкуп, крадіжки та інші прийоми. Такі підходи полегшуються тим, що нова техніка підслуховування, яка з'явилася на ринку, робить промислове і комерційне шпигунство набагато ефективнішим.

Зазначимо, що сума, яку зазвичай недобросовісні конкуренти пропонують за видачу цінної інформації, набагато перевищує посадовий оклад працівника фірми. Таким чином, підписка про нерозголошення таємниці зовсім не є гарантією повного її збереження.

3. Пряме фізичне придушення, що є злочинним посяганням на життя і здоров'я персоналу підприємства. Основні методи фізичного придушення конкурента:

організація пограбувань і розбійних нападів на офіси, виробничі та складські приміщення, розкрадання вантажів тощо;

знищення матеріальних цінностей і нерухомості конкурента шляхом підпалів, вибухів і та ін.;

фізичне усунення керівників, захоплення заручників.

Найактивніше в Україні виявляються криміналізація і недобросовісна конкуренція у фінансовій сфері. Більшість експертів вважають, що це особливо відчутно в національній кредитно-фінансовій сфері.

Щодо викрадення таємниць підприємства, передбачається відповідальність за два самостійні склади злочинів [47, с. 324]:

1) незаконне збирання з метою використання відомостей, що становлять комерційну таємницю;

2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це завдало великої матеріальної шкоди суб'єкту підприємницької діяльності.

Способи вчинення незаконного добування можуть бути різними, зокрема [47, с. 325]:

вилучення, в тому числі викрадення, матеріальних носіїв інформації, яка становить комерційну таємницю (документів, що містять відповідні відомості, або предметів матеріального світу, певні ознаки яких можуть бути досліджені з метою встановлення необхідної інформації);

незаконне дослідження носіїв опосередкованої інформації (технічних демаскуючих ознак, що містяться у власних або відображених фізичних полях об'єктів, які захищаються, а також у їхніх слідах у навколишньому середовищі);

незаконне ознайомлення з такими документами або предметами в будь-який спосіб;

порушення таємниці повідомлень;

організація витоку мовної інформації;

одержання інформації від осіб, які нею володіють, за плату (в цьому разі йдеться про осіб, які не мають права розпоряджатися відповідною інформацією);

шляхом застосування погроз або насильства.

Зазначені дії (як і інші злочинні дії в інформаційній сфері) також можуть бути вчинені фізичним (безпосередні дії людини, що завдають шкоди інтересам, які охороняються законом, та правам суб'єктів інформаційних правовідносин, що спрямовані на організацію витоку інформації) чи технічним (організація витоку інформації технічними каналами) способами.

Фізичний спосіб скоєння в більшості випадків спрямований не на інформацію безпосередньо, а на її матеріальні носії (викрадення), тоді як злочини, що вчинені технічним способом, здебільшого не зачіпають цілісності та належності матеріальних носіїв. У сучасних умовах набуває розповсюдження технічний спосіб незаконного збирання інформації шляхом використання інформаційних мереж як глобальних, так і локальних. Для прикладу таких злочинів можливо навести викрадення баз даних з інформацією про клієнтів через підключення до банківських інформаційних мереж.

Досить різноманітними є також засоби вчинення злочину технічними каналами. Для досягнення мети підприємницького шпигунства шляхом отримання інформації за допомогою технічних засобів застосовуються: акустичні засоби (спрямовані або вмонтовані мікрофони, вібродатчики), лазерні засоби отримання мовної інформації, засоби отримання інформації з дротів та комунікацій, засоби перехоплення побічних ви-

промінювань, закладені пристрої, комп'ютерна техніка, в тому числі її інформативні частини. Засоби вчинення підприємницького шпигунства у формі незаконного збирання відомостей, що становлять комерційну таємницю, так само, як і інші ознаки об'єктивної сторони підприємницького шпигунства (місце, час та обставини вчинення), не мають значення для кваліфікації злочину, але можуть бути враховані судом під час призначення покарання винній особі.

Наступною формою об'єктивної сторони підприємницького шпигунства є незаконне використання відомостей, що становлять комерційну таємницю. Це означає впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять комерційну таємницю.

5.4. Економічне шпигунство та його особливості

Шпигунство в даному контексті розглядається як спосіб добування інформації, що становить комерційну таємницю. Термін "шпигунство" (економічне, промислове, комерційне, науково-технічне) означає активні дії, спрямовані на збирання або розкрадання цінної інформації, закритої для доступу сторонніх осіб.

Відповідно до західної теорії, промислове шпигунство – це добування законним і незаконним шляхом у конкуруючих фірм (монополій, а також партій, фізичних або юридичних осіб, правоохоронних органів і та ін.) відомостей чи інформації з галузі наукових досліджень, виробництва продукції із застосуванням найбільш перспективної технології, а також персональних даних з метою їх використання в конкурентній боротьбі або навіть у корисливих цілях.

Економічне шпигунство – ширше поняття, яке охоплює і такі його підвиди, як промислове, виробниче, науково-технічне, комерційне шпигунство. Якщо таємницею володіє одна особа, це викликає інтерес до неї іншої особи, для задоволення якого чиняться дії, спрямовані на отримання нею певної матеріальної або іншої вигоди. Особа, що бере участь у подібній діяльності, має загальновідому назву "шпигун". У підприємництві конкурентна боротьба неможлива без отримання інформації. Прагнення отримати відомості в умовах закритого до них доступу законним шляхом неминуче породжує недобросовісну конкуренцію, тобто

об’єктивну потребу шпигувати за конкурентом. Без володіння інформацією про дії конкурента, передбачуваний попит на продукцію, перспективні наукові розробки важко, а деколи і неможливо бути конкурентоздатним. Виникають дві тісно пов’язаних обставини:

а) підприємець змушений виступати як захисник своїх таємниць (цінної інформації);

б) підприємець змушений з метою конкуренції здобувати (красти, купувати) чужі секрети, що захищаються. Те, що не захищається, особливої цінності не має.

У зарубіжній літературі про промислове шпигунство наголошується, що ця діяльність зовсім не вважається злочинною і не є підставою для кримінальної відповідальності. Якщо в процесі розкрадання секретної інформації підприємству, установі або працівникам завдано збитку, то кримінальному покаранню винна особа підлягає саме за останнє діяння, а не за сам факт розкрадання цінних відомостей. Загалом такий підхід є правильним, оскільки сам підприємець не зацікавлений у тому, що коли він здійснюватиме розкрадання інформаційних матеріалів (а займатися цим він змушений через ринкову діяльність), то перебуватиме під загрозою застосування до нього кримінального покарання. Здебільшого значно легше звернути увагу на охорону своїх таємниць, ніж вдаватися до кримінально-правового захисту.

Розглянемо детальніше ознаки промислового шпигунства. До них належать:

суб’єкт (хто може займатися певним видом діяльності);

предмет (на що посягає промислове та інше шпигунство);

спосіб, засіб дії, за допомогою яких здійснюється оволодіння закритими відомостями;

адресат (хто виступає замовником).

Суб’єктами промислового (комерційного) шпигунства можуть бути громадяни України, іноземні громадяни, особи без громадянства, що належать і не належать до працівників промислових підприємств, установ, фірм. Виконавцем шпигунства можуть виступати безпосередньо підприємець, працівники власної служби безпеки, приватних детектив них розшукових фірм або окремі особи, що працюють у приватному порядку. Пошук промислової, комерційної інформації і оволодіння нею здійснюють в одних випадках за завданням замовника, а в інших – за власною ініціативою для подальшої її продажу зацікавленим особам.

Аналіз зарубіжної практики свідчить, що в приватних службах безпеки, які спеціалізуються на розкраданні чужих таємниць, є значна за чисельністю клієнтура замовників і покупців. Наприклад, у Великій Британії одне з приватних розшукових агентств, разом із розслідуванням фактів про промислове шпигунство, гарантуванням безпеки підприємств і фірм, займається також добуванням (розкраданням) інформації про конкурентні приватні підприємства. Подібні фірми не прагнуть особливо конспірувати, приховувати свою діяльність. їх координати є у спеціальних довідниках. Нині в країнах ринкової економіки діють сотні й тисячі агентств та десятки тисяч промислових шпигунів.

Такі агентства починають утворюватися і діяти також на території України. Проте різкого зростання кількості таких служб слід очікувати тільки в умовах ринково-конкурентної економіки, що сформувалася аналогічно до західних країн.

З цілком зрозумілих причин видати секрети можуть і працівники фірми. Якщо особам, що не працюють на підприємстві, потрібно долати фізичні й технічні перешкоди для проникнення до таємниць, то працівники фірми можуть і не докладати подібних зусиль. Таємною інформацією вони вже володіють або мають можливість зібрати її. Мотивацією таких дій можуть бути користь, помста тощо. Тому при формуванні колективу працівників необхідно враховувати, кому з них можна довіряти свої таємниці, а кому не варто. Вирішують це питання самі підприємці.

Наступною ознакою шпигунства є предмет посягання, тобто інформація, яка є цінною для її володаря і закрита для сторонніх осіб. Носії такої інформації найрізноманітніші: документи, креслення, схеми, патенти, дискети, касети, в яких містяться дані наукових досліджень, бухгалтерські матеріали, контракти, плани й рішення керівництва фірм. Предметом промислового шпигунства може бути інформація не тільки фірм, а й державних підприємств і установ.

Певні труднощі виникають при визначенні промислової таємниці підприємств, фірм, компаній зі змішаним капіталом. Наприклад, приватний і державний капітал; державний та іноземний приватний капітал; вітчизняний та іноземний приватний капітал. Неминуче зіткнення інтересів вітчизняного й іноземного власника як між собою, так і з державою. В останньому випадку необхідно враховувати наявність державної (військової) таємниці, службової таємниці, інших відомостей, визначених кримінальним законодавством, а також промислову таємницю. Відомості,

що становлять державні секрети, перелічені у спеціальних нормативних актах, затверджених урядом держави. На їх підставі видаються відомчі акти, що визначають види таємниць, які підлягають охороні. Промислова ж таємниця може бути введена в переліки державних таємниць, а може і не належати до них. Посягання на секрети державних підприємств і установ переслідується кримінальним законом, тоді як підприємницькі секрети кримінальним законом не захищені.

Наступною ознакою промислового шпигунства є спосіб його здійснення. Дії із заволодіння інформацією чиняться таємно від оточення, шляхом її розкрадання, збирання, купівлі, видачі. Не є винятком і знищення, спотворення або саботаж щодо використання інформації. Мета цього – не дати власникові можливості використовувати її для отримання вигоди, бути конкурентоспроможним.

До засобів отримання таємниць належать різні технічні системи. Якщо в Україні основними власниками розвідувальних технічних засобів є спеціальні державні органи (служби), то на Заході вони перебувають у користуванні приватних осіб. Це дає змогу підприємцям широко використовувати засоби електронної розвідки для отримання необхідної інформації, зняття її з телефонних переговорів, комп'ютерів, приміщень, де ведуться секретні переговори, і та ін. Застосування цих та інших засобів залежить від інформації, яку має намір отримати суб'єкт. Один вид інформації може бути викрадений, інший – прослуханий, третій – сфотографований (або зроблені зарисовки), четвертий – записаний на магнітофон, п'ятий – знятий кінокамерою і т. д. Іноді використовують комплекс спеціальних заходів для її отримання. Залежно від виду отримання інформації вживають відповідних заходів захисту.

Адресатами (замовниками) отримання промислової (комерційної) інформації виступають підприємці малого і великого бізнесу, керівники державних підприємств, а також уряди іноземних держав. Захист таємниць промислових і комерційних фірм і проникнення в них є двома сторонами однієї медалі. До них однаковою мірою виявляють цікавість як приватні особи, так і працівники державних служб.

Різноманітними є форми та методи економічного шпигунства.

Підкуп – найпростіший і найефективніший спосіб отримання конфіденційної інформації. Зрозуміло, він потребує деякої попередньої роботи для з'ясування ступеня обізнаності тих або інших працівників фірми в її справах. Підкуп зазвичай здійснюється через посередників, тому необ-

хідною умовою є збирання інформації про них: треба точно знати, кому дати гроші, скільки, коли, через кого і за що. Проте всі такі витрати перекриваються однією важливою обставиною – працівникові фірми не потрібно долати фізичні й технічні перешкоди для проникнення в її секрети.

Ще одним способом економічного шпигунства є "вливання своїх людей" до складу персоналу фірми-конкурента. Для впровадження є два шляхи: перший – коли агент виступає під власним прізвищем і працює за професією; другий – коли він працевлаштується за підробленими документами. Впровадження власної агентури до конкурентів складніше за звичайний підкуп або шантаж, але, на відміну від завербованих інформаторів, свій агент є набагато надійнішим та ефективнішим як джерело конфіденційної інформації.

Залежно від ступеня цінності інформатора будуються відносини між сторонами, що співпрацюють. Чим він важливіший, тим більше потрібно дотримуватися заходів конспірації. Зокрема, зустрічі з ним маскуються під побутові контакти, відбуваються на конспіративних квартирах або в громадських місцях, через тайники і навіть за допомогою технічних засобів. Спілкування з менш цінними людьми може бути звичайним. При цьому сторони особливо не піклуються про свою безпеку. Отже, вибіркове приховане спостереження за власними працівниками може дати керівникові фірми (через його оперативних співробітників) вельми цікаві відомості для роздумів.

Викрадення інформації можливе багатьма способами:

розкрадання носіїв інформації (дискет, магнітних, оптичних дисків, перфокарт);

копіювання програмної інформації з носіїв;

читання залишених без нагляду роздруків програм;

читання інформації з екрана сторонньою особою (під час відображення її законним користувачем або за його відсутності);

підключення спеціальних апаратних засобів, що забезпечують доступ до інформації;

використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань (відомо, що за допомогою спрямованої антени таке перехоплення можливе стосовно ПК в металевому корпусі на відстані до 200 м, а в пластмасовому – до 1 км);

несанкціонований доступ програм до інформації, або розшифровування програмної зашифрованої інформації. Останній спосіб називається

"електронним грабежем", а людей, що використовують його, називають "хакерами". Цей вид злочинів найбільш поширений там, де є комп'ютерні мережі в масштабі фірми, організації, населеного пункту або регіону.

Спостереження теж дає цінну конфіденційну інформацію, особливо якщо воно пов'язане з копіюванням документації, креслень, зразків продукції і та ін. Загалом процес спостереження складний, оскільки потребує значних витрат сил, часу і коштів. Тому його ведуть здебільшого вибірково: у визначеному місці, в певний час спеціально підготовлені люди і за допомогою технічних засобів.

Фотографування застосовують в економічному шпигунстві досить широко за допомогою сучасної апаратури за денного освітлення і вночі, на надблизькій відстані і на віддалі до кількох кілометрів, у видимому світлі і в інфрачервоному діапазоні (в останньому випадку можна виявити виправлення, підробки, а також прочитати текст на обгорілих документах).

Велику небезпеку в економічному шпигунстві становлять люди, які володіють фотографічною зоровою пам'яттю. Їм достатньо одного погляду, щоб охопити значний зміст, запам'ятати і відтворити його практично без спотворень. Особливо легко це вдається фахівцям у розвідувальній галузі діяльності, яким достатньо лише натяку, щоб зрозуміти основний зміст тексту (креслення, розробки).

Прослуховування і підслуховування за значущістю перебувають на останньому місці серед основних форм і методів отримання конфіденційної інформації. Це зрозуміло, бо інформацію збирають випадково, безсистемно, близько 90 – 95 % відсотків її становлять вислови, що не викликають ніякого інтересу у конкурентів. Крім того, потрібно багато часу для аналізу цієї інформації. Проте цей метод дуже широко використовують через його простоту.

Підслуховування телефонних переговорів найбільш поширене. Його здійснюють:

за рахунок мікрофонного ефекту телефонного апарата;

контактним підключення до лінії зв'язку;

безконтактним підключенням до телефонної лінії;

за допомогою телефонних радіозакладок;

за рахунок так званого високочастотного "нав'язування".

Слід зазначити, що підслуховувати можна не тільки стаціонарні телефонні лінії, а й переговори по радіотелефону, зокрема в системах сті-

льникового зв’язку. Все залежить від того, який спосіб прослуховування використовують, за допомогою якої апаратури.

Загалом кількість моделей технічних пристроїв для підслуховування і запису розмов на ринку не піддається обліку. З їх допомогою можна приймати, підсилювати, очищати й записувати будь-які розмови (зокрема ті, що ведуться пошепки або під звук води, що ллється з крана) досить чітко і надійно.

Існують і складніші методи підслуховування, наприклад за допомогою лазерного опромінювання шибок у приміщенні, де ведуться розмови. Або спрямованим радіовипромінюванням, що примушує "відгукуватися і говорити" деталі радіоприймача, телевізора, настінного годинника та іншу побутову техніку. Проте подібні методи потребують складної і достатньо дорогої техніки, тому застосовують їх в економічному шпигунстві досить рідко [47, с. 331–338].

5.5. Налагодження охорони комерційної таємниці суб’єктів господарювання

Завдання підприємця – надійно перекрити канали просочування конфіденційної інформації. Коли на підприємстві визначено перелік відомостей, що становлять комерційну таємницю, то потрібно зазначити джерела витоку цієї конфіденційної інформації. Потенційними джерелами витоку комерційної таємниці можуть бути:

1. Документація підприємства або просто документи (накази, бізнес-плани, ділове листування тощо). Це найпоширеніша форма обміну інформацією, її накопичення та зберігання. Важливою особливістю документів є те, що вони іноді є єдиним джерелом найважливішої інформації (наприклад, контракт, боргова розписка та ін.), а отже, їх втрата, викрадання, знищення можуть завдати непоправного збитку. Структура документів підприємства є предметом окремого розгляду, оскільки документи можуть мати не тільки різний зміст, а й різні фізичні форми – матеріальні носії. Різноманітність форм і змісту документів за призначенням, спрямованістю, характером руху і використанням є вельми принадним джерелом для зловмисників, що, природно, привертає їх увагу до можливості отримання інформації, яка їх цікавить.

2. Персонал підприємства (усі, хто працює тут, у тому числі й керівник). У деяких джерелах конфіденційної інформації люди відіграють осо-

бливу роль, оскільки здатні виступати не тільки джерелом, а й суб'єктом зловмисних дій. Вони не тільки володіють і розповсюджують інформацію в рамках своїх функціональних обов'язків, а й можуть аналізувати, узагальнювати її, робити певні висновки, а також за певних умов приховувати, продавати її та вчиняти інші кримінальні дії, аж до злочинних зв'язків із зловмисниками.

3. Партнери, контрагенти або клієнти, що користуються або користувалися послугами підприємства, найбільш обізнані із джерелами найважливіших секретів фірми. Тому вони заслуговують ретельної уваги під час аналізу системи захисту.

4. Вироблена продукція або надані послуги. Продукція є особливим джерелом інформації, за характеристиками якої активно полюють конкуренти. Заслуговує на увагу нова або така, яку готують для виробництва, продукція. Враховують етапи її "життєвого циклу": задум, макет, дослідний зразок, випробування, серійне виробництво, експлуатація, модернізація і зняття з виробництва. Кожен із цих етапів супроводжується специфічною інформацією, що виявляється різними фізичними ефектами, які у вигляді демаскувальних ознак можуть розкрити відомості, що охороняються.

5. Технічні засоби забезпечення виробничої діяльності. Ці засоби є широкою і ємкою групою джерел конфіденційної інформації. До групи засобів забезпечення виробничої діяльності належать, зокрема, телефони і телефонний зв'язок, телевізори і промислові телевізійні установки, радіоприймачі, радіотрансляційні системи, системи гучномовного зв'язку, підсилювальні системи, кіносистеми, охоронні й пожежні системи та інші, які за своїми параметрами можуть бути джерелами перетворення акустичної інформації в електричні й електромагнітні поля, здатні утворювати електромагнітні канали просочування конфіденційної інформації.

6. Непрямі джерела (відходи виробництва, реклама, публікації у пресі). Більшість інформації можна отримати саме з непрямих джерел. Професійно проведена аналітична робота іноді дає чудовий результат, Зазвичай цьому джерелу не надають особливої уваги, тому воно є найбільш доступним. Наприклад, відходи виробництва, які називають непотрібом, можуть багато про що розповісти щодо використовуваних матеріалів, їх складу, особливостей виробництва, технології. І отримати їх можна майже безпечним і законним шляхом на звалищах, смітниках, у місцях збору металобрухту, в корзинах для сміття в робочих кабінетах.

Умілий аналіз цих відходів може багато що розповісти про секрети виробництва. У публікаціях – книгах, статтях, монографіях, оглядах, повідомленнях, рекламних проспектах, доповідях, тезах тощо, можна мимовільно розкрити всі виробничі таємниці.

Із джерел конфіденційної інформації можна мати дані про склад, зміст і напрям діяльності підприємства (організації), що цікавить конкурентів. Природно, що така інформація їм украй потрібна, і вони знайдуть способи отримати її.

Тому грамотна система захисту, розроблена з урахуванням усіх її особливостей, дасть змогу запобігти багатьом проблемам [47, с. 350–352].

6. Ділова розвідка

6.1. Передумови виникнення та актуальність ділової розвідки

Сучасна ситуація на українському і світовому ринках характеризується ускладненням комерційних схем та умов здійснення операцій, використанням комплексних продуктів, посиленням конкуренції між компаніями. Фінансові потоки, рух капіталу, управління ресурсами і персоналом стають складним завданням, що пов’язане із зростанням обсягів звітності і документообігу, збільшенням швидкості інформаційних потоків та своєчасності отримання комерційної інформації.

В умовах гострої конкуренції проблема пріоритетів використання досягнень науки й техніки є найважливішою. Інструментом її розв’язання стає промислове шпигунство, а в позитивному аспекті – ділова розвідка. Як іманентна складова сучасної ринкової конкуренції, ділова розвідка виступає складовою економічної розвідки і посідає відповідне місце у правовому полі України, однак має ще недостатньо визначений і досліджений науковцями вплив на економічну безпеку. Реалії сучасного ділового світу такі, що більшість підприємців і керівників підприємств розуміють, що без глибокого аналізу інформації, якою нині наповнені ринки, неможливе успішне ведення бізнесу. Потоки інформації, що генеруються учасниками ділової активності, за її кваліфікованого опрацювання, аналізу й синтезу здатні забезпечити підприємство конкурентною перевагою стосовно інших гравців ринку, які не володіють потрібною інформацією в потрібний час.

У ринкових умовах науково-технічний прогрес перетворюється на сферу гострої конкуренції, метою якої стає отримання надприбутку, який мають ті суб'єкти господарської діяльності, які швидше за всіх впроваджують інновацію у виробництво і монополізують її: засекречують, захищають патентом.

У будь-якому бізнесі за будь-яких умов, перш ніж вкладати гроші, розвивати або змінювати сферу діяльності та напрям бізнесу, вибирати партнерів з бізнесу, потрібно активно збирати інформацію для прийняття управлінських рішень. Підприємці змушені щодня і постійно вирішувати завдання конкурентної розвідки.

До розв'язання суперечливих проблем бізнесу та розвитку добросовісної конкуренції виявляє інтерес ділова розвідка, яку можна трактувати як окремий, більш звужений напрям економічної розвідки.

У публіцистичних творах економічну розвідку часто ототожнюють з промисловим шпигунством, вважаючи, що для організатора – це економічна розвідка, а для суб'єкта протидії – промислове шпигунство. У вивченні й визначенні меж діяльності економічної розвідки, як і в її історії та розвитку, чимало таємниць і недомовок. Етапи економічної розвідки чітко визначають, що вона є складовою історичного розвитку продуктивних сил та науково-технічного прогресу.

Характер, форми і способи ведення економічної розвідки змінювалися зі зміною суспільно-політичних формацій, з еволюцією виробництва та рівня розвитку науки й техніки. В історичному плані економічну розвідку можна вважати більш давньою, ніж політичну та військову.

Враховуючи, що сьогодні без отримання інформації та її аналізу, проведення маркетингових досліджень і розвідувальної діяльності неможливо успішно вести бізнес, роль і актуальність впровадження ділової (корпоративної) розвідки, як однієї з розгалужень економічної, є беззаперечною і важливою [47, с. 380, 382–384].

6.2. Особливості ділової розвідки

Поняття "ділова (корпоративна) розвідка" увійшло до українського лексикону порівняно недавно.

Фактично ділова розвідка забезпечує керівництво підприємства інформацією, необхідною для превентивного ухвалення рішень. Це збирання інформації, її класифікація (за вагомістю, рівнем вірогідності, на-

прямом застосування і та ін.), аналіз, прогноз розвитку ситуації, підготовка рекомендацій керівництву. Розрізняють стратегічну ділову (корпоративну) розвідку та оперативну.

Завдання стратегічної ділової розвідки за змістом близькі до завдань стратегічного планування і маркетингу та зводяться до визначення структури й динаміки тієї сфери господарсько-економічної діяльності, в якій працює (або збирається працювати) підприємство, з виявленням і аналізом усіх конкурентів і контрагентів у цій сфері діяльності.

Оперативна ділова розвідка вирішує гострі завдання негативної взаємодії з конкретним конкурентом і часто діє на межі етично та юридично установлених норм і засобів. Оскільки йдеться про цільову функцію створення труднощів або перешкод конкурентові, то всі ці завдання ставляться з явним акцентом на пошук слабких місць у діяльності конкурента.

Джерела інформації, цінної для вирішення завдань ділової розвідки, численні й різноманітні. Навіть поверхневий огляд дає змогу виявити, що для оперативної ділової розвідки, де потрібна інформація (зокрема, негативна), ретельно приховується й не афішується ні в ЗМІ, ні в ділових чи інших друкованих матеріалах. Основними джерелами інформації здебільшого є люди, а саме – міжособистісне спілкування, переважно неофіційне, з працівниками конкурента.

Водночас для стратегічної ділової розвідки плідна і цікава інформація є в загальнодоступних джерелах. Вона не тільки не приховується, а навпаки, рекламується, організовується і подається у вигляді різних баз даних, довідників, оглядів, наукових статей, публіцистики тощо.

Служба ділової розвідки залежно від масштабу підприємства може складатися з одного штатного працівника, а може бути великим і розгалуженим підрозділом. У практичній діяльності до процесу ділової розвідки залучається багато працівників підприємства, що не мають прямого адміністративного зв’язку з цим підрозділом.

Отже, вирішення конкретного завдання ділової розвідки можна подати як тристадійний процес, зображений у табл. 6.1 [47, с. 411].

Отже, в умовах інформаційного простору приховати щось державі чи окремій фірмі стає дедалі важче, як би ретельно не приховувалися певні факти, особливо коли вони стосуються фінансово-господарської діяльності.

Таблиця 6.1

Процес вирішення конкретного завдання ділової розвідки

Етап	Завдання	Дія
1	1.1. Визначення погреби в інформації	Систематизація запитань
	1.2. Організація ресурсів для збирання інформації	Систематизація джерел інформації
		Збирання інформації
2	2.1. Опрацювання й оцінювання інформації	Класифікація інформації
	2.2. Аналіз інформації і складання висновків	Систематизація інформації
		Генерація вторинної (узагальнюючої) інформації
3	3.1. Передавання інформації особам, що ухвалюють рішення	Забезпечення оперативного зворотного зв’язку із замовником
	3.2. Адресний розподіл інформації між підрозділами	Систематизація адресатів. Забезпечення конфіденційності

Сліди їх або супутніх з ними подій настільки численні й різноманітні, що навіть за відкритими джерелами інформації можна виявити ці факти [47, с. 407–411].

6.3. Роль ділової розвідки у бізнесі

Реалії сучасного ділового світу такі, що багато бізнесменів розуміють, що без глибокого аналізу інформації, яка нині заполонила весь світовий ринок, неможливе успішне ведення бізнесу. Потоки інформації, що генеруються учасниками ділової активності, за її кваліфікованого опрацювання, аналізу та синтезу висновків здатні озброїти компанію конкурентними перевагами стосовно інших гравців ринку, які своєчасно не володіють потрібною інформацією.

Ділова (корпоративна) розвідка не пов’язана з великими постійними витратами, але при цьому надає переваги, які не може забезпечити будь-який інший структурний підрозділ компанії. Ділова розвідка не повторює роботи інших структур із меншою собівартістю, а дає можливість отримувати дані, які в принципі неможливо отримати інакше.

У будь-якому бізнесі та за різних умов кожен власник перш ніж робити грошові заощадження у створення, розвиток чи зміну профілю бізнесу, вибирати партнерів чи співвласників, має активно зібрати інфор-

мацію для прийняття рішення і лише після її аналізу робити висновок. Через це в умовах прогресуючих ринкових відносин треба шукати ніші через чітко побудовану й випробувану часом структуру ділової (корпоративної) розвідки, отримуючи дані про:

ринки збуту;

конкурентів;

партнерів;

продукцію і послуги;

контрагентів;

нові технології;

проекти законодавчих актів;

політичні події в країні і світі.

Розглянемо переваги, що надає бізнесу ділова розвідка.

1. Прогнозування змін на ринку.

Компанія має постійно проводити моніторинг середовища, в якому вона працює, тоді зрідка виникають непередбачувані несподіванки.

2. Прогнозування дій конкурентів і партнерів.

3. Виявлення нових або потенційних конкурентів.

У практиці бувають факти, що в процесі навчання ділової розвідки початківці, що освоюють технології розвідки, виявляють на ринку компанії, невідомі їм, але такі, котрі в майбутньому можуть загрожувати бізнесу як конкуренти. Велику роль у подібному моніторингу відіграють сучасні засоби стеження за новою інформацією в Інтернеті.

4. Можливість використання досвіду інших компаній.

Можливість вчитися на чужих помилках інтуїтивно зрозуміла всім, а копіювання успішних управлінських рішень – тим більше. Тільки ділова (корпоративна) розвідка здатна безкоштовно організувати збирання думок клієнтів про будь-який продукт або швидко проаналізувати судову практику з погляду маркетолога, а не юриста.

5. Відстежування інформації, пов’язаної з патентами і ліцензіями.

Ділова розвідка здатна допомогти фахівцям з патентного законодавства з’ясувати, які напрями діяльності конкурентів відображені в публікаціях, але не захищені патентами. Це нормальна практика, яка має технології, відшліфовані десятиліттями, і може застосовуватися практично в усіх країнах.

Якщо компанія, що має ноу-хау, не змогла або не захотіла їх захистити відповідно до чинного законодавства, то вона не може притягнути

до відповідальності тих, хто відтворив виріб або технологію, подібні до її власних зразків.

Після того, як перспективні ідеї і напрями виявлені фахівцями з патентного права, проводять експертизу, в процесі якої з'ясовують, що технологія нічим не захищена, проводяться її патентування на своє ім'я. Особливо часто подібна ситуація спостерігається в компаніях, що виходять на світовий ринок, проте підприємства і компанії, які не мають зовнішньоекономічних зв'язків, також можуть піддаватися таким ризикам.

6. Оцінювання доцільності придбання нового бізнесу.

Здебільшого власники бізнесу штучно підвищують вартість компанії для отримання максимального прибутку. Тобто створюється імідж перспективної компанії. І лише придбавши бізнес, не маючи умов для прогресивного випуску продукції через слабку автоматизацію процесів, відсутність ринків збуту, зростання цін на оренду, новий власник скорочує виробництво, а часом і покидає придбану сферу бізнесу.

Зрозуміло, що перед купівлею бізнесу треба перевірити всі ці дані. Зазвичай із таким завданням міг впоратися і сам власник без ділової розвідки, проте ділова розвідка може дати відповіді на потрібні запитання значно простіше, ніж хтось інший, оскільки володіє всіма необхідними для цього інструментами.

7. Відкриття чи створення нового бізнесу.

Ця стадія діяльності компанії співзвучна з попереднім етапом і якоюсь мірою подібна до етапу "Можливість використання досвіду інших компаній", однак ширша, оскільки дає змогу не лише визначити досвід окремих компаній, а й стан ринку загалом, зробити аналіз конкурентоспроможності секторів ринку.

Саме ділова розвідка здатна допомогти в організації прибуткового бізнесу.

Здебільшого успіх будь-якого бізнесу залежить від:

якості матеріалів і сировини, які використовують у виробництві;

вміло підібраного кваліфікованого складу компанії;

стилю керівництва та сформованого інформаційно-аналітичного кістяка колективу;

автоматизації технологічних процесів та сильної маркетингової і розвідувальної систем.

8. Вивчення політичних, законодавчих або регуляторних змін, які можуть вплинути на бізнес.

Пріоритетом стратегічної розвідки є моніторинг політики. Політичні рішення впроваджувалися і будуть впроваджуватися в життя незалежно від їх рентабельності, ефективності і витрат грошових коштів на їх впровадження. Тому, щоб не втратити бізнес, потрібно враховувати політичні зміни, тенденції і напрями, прогнозувати і передбачати наслідки політичних подій та інтриг. На основі викладеного можна виокремити такі головні завдання ділової (корпоративної) розвідки за політичними аспектами:

відстежувати законодавчі та адміністративні тенденції в діях влади щодо бізнесу загалом;

відстежувати лобіюючі зміни в законодавстві, які можуть вплинути на власний бізнес на користь інших бізнес-груп або прямих (непрямих) конкурентів;

у період передвиборчих кампаній аналізувати позиції реальних претендентів у владні структури в контексті інтересів свого бізнесу;

збирати й аналізувати інформацію та інформувати керівництво про випадки, коли діяльність компанії чи окремі її напрями починають зачіпати чиїсь політичні інтереси;

відстежувати дрейф політичних інтересів впливових структур та інформувати керівництво структур про ці факти, особливо якщо підприємство вносило зміни у свою діяльність, а ситуація складається так, що вона починає зачіпати інтереси новосформованих політичних владних структур.

9. Вивчення нових технологій, продуктів і процесів, які можуть вплинути на бізнес.

Це один із пріоритетних напрямів роботи стратегічної ділової розвідки, що потребує розуміння, компетентності та знання специфіки продукту компанії. Моніторинг спеціальних періодичних видань і збірок, наукових доповідей та праць дає змогу в наукоємних галузях заощадити значні кошти і час за рахунок використання чужих напрацювань.

10. Погляд на свій бізнес очима сторонньої особи.

Часто самовпевнені керівники найбільших компаній, які справді досягли високих результатів, починають вважати себе всесильними й за підтримки своїх підлеглих вважають усі свої рішення єдино правильними. Якщо таким керівникам не вдається оточити себе творчо мислячими працівниками, які є досить сміливими, щоб висловлювати власну думку, то компанія може зазнати краху. Звідси висновок, що найкрихкішою є саме жорстка структура підприємства. І в структурі будь-якої фірми, і в її

підходах до бізнесу і життя загалом має бути закладена гнучкість, що поєднується із спрямованістю на виконання загальних завдань та потреби розвитку бізнесу.

Ділова розвідка за характером своєї роботи має справу з кращими прогресивними рішеннями і відстежує всі новинки як у виробничій сфері, так і у технології управління. Тому вона не має аналогів для оцінки відповідності методів ведення бізнесу реальним вимогам ринкової конкуренції.

11. Перетворення слабких сторін бізнесу на конкурентні переваги.

12. Виявлення змін і реагування на них раніше за виникнення кризових ситуацій.

13. Виявлення слабких місць конкурента і недомовок у його рекламі.

Ділова розвідка здатна проаналізувати скарги споживачів на продукт конкурента і на підставі виявлення приховуваних ним недоліків дати рекомендації стосовно своєї реклами, щоб вона підкреслювала саме ті переваги власного продукту, яких продукція конкурента не має.

14. Виявлення потенційних джерел просочування конфіденційної інформації через працівників компанії.

Здебільшого функція захисту не належить до компетенції ділової розвідки, і отримана інформація зазвичай передається службі безпеки.

Інколи трапляються резюме працівників підприємства нинішніх, або колишніх, що хочуть знайти нове місце роботи. Саме ці резюме є стабільним джерелом інформації, оскільки за їхніми даними можна спланувати і здійснити незаконне залучення цих осіб до співробітництва.

15. Збирання інформації про партнерів і клієнтів.

З викладеного можна зробити такий висновок: в епоху науково-технічного прогресу та науково-технічної революції економічно-розвідувальна діяльність є одним із найсучасніших засобів конкурентної боротьби. Ставши невід'ємною частиною бізнесу, вона встановлює диктатуру меншості над більшістю, створює всі умови для функціонування системи загальнонаціонального контролю над економікою, наукою, людьми.

Активне й ефективне ведення економічної інформаційно-аналітичної діяльності має особливе значення для держав, у яких з тих чи інших причин на певний час загальмувався економічний та науково-технічний прогрес. Тому в інтересах зміцнення всіх сфер національної безпеки України було б доцільно мати потужну розгалужену розвідувальну структуру та відповідне правове поле її діяльності [47, с. 418–427].

Розділ 2. Основи інформаційної безпеки та її особливості застосування у бізнесі

7. Загальні принципи безпеки інформаційних технологій

7.1. Категоріальний апарат сфери інформаційної безпеки

7.2. Класифікація ресурсів для захисту

7.3. Загрози та уразливості

7.4. Класифікація атак та вірусів

8. Канали витоку інформації

8.1. Класифікація каналів витоку інформації

8.2. Методи та засоби захисту від витоку інформації

8.3. Методи визначення каналів витоку інформації

9. Організація інформаційної безпеки на підприємстві

9.1. Політики інформаційної безпеки

9.2. Моделі систем безпеки

9.3. Методика розробки політики безпеки

9.4. Методи оцінки втрат

9.5. Методи оцінки ризиків

9.6. Служба інформаційної безпеки. Організація її аудиту

10. Організація інформаційної безпеки комп'ютерних мереж

10.1. Стандарти інформаційної безпеки

10.2. Ідентифікація та автентифікації у комп'ютерних мережах

10.3. Методи та засоби інформаційної безпеки в комп'ютерних мережах

11. Правові основи інформаційної безпеки

11.1. Структуризація нормативно-правового забезпечення

11.2. Структуризація класифікаційних ознак у сфері безпеки

11.3. Нормативні положення, що регламентують інформаційну безпеку

Розділ 2. Основи інформаційної безпеки та її особливості застосування у бізнесі

7. Загальні принципи безпеки інформаційних технологій

7.1. Категоріальний апарат сфери інформаційної безпеки

У багатьох аналітичних звітах вітчизняних і закордонних дослідників і експертів досить часто зустрічаються поняття "витік конфіденційної інформації", "розкриття комерційної таємниці" і ряд інших. Усе це аспекти інформаційної безпеки (ІБ). Крім того, усі уявляють обсяги збитків, що з'являються у результаті "виникнення" подібних понять, сьогодні вони обчислюються мільйонними й мільярдними сукупними сумами. І природно, що про це відомо багатьом керівникам фірм. Однак лише невелика кількість дійсно далекоглядних керівників виділяють для забезпечення ІБ на підприємстві достатні обсяги коштів для запобігання (це дешевше), локалізацію й усунення (це вже дорожче) подібних випадків.

Цьому є досить просте пояснення – на підприємствах немає прийнятної концепції ІБ [66], реалізованої через систему ІБ (СІБ) відповідних заходів і засобів [62]. Створення й впровадження СІБ на підприємстві сьогодні сприймається як технічна реалізація деякого комплексу засобів, які в сукупності утворюють аспект ІБ. Інформаційна безпека, як відомо, не оперує поняттями фінансові (грошові) втрати, економічні ризики, рентабельність виробництва, прибуток, податки та іншими економічними термінами, які, як правило, й забезпечують ведення сучасного бізнесу [54; 108].

Для того, щоб прийти до розуміння концепції ІБ, необхідно, у першу чергу, визначитися з понятійним апаратом, що використовується в різних видах діяльності.

Для зручності та з огляду великої чисельності понятійного апарата систематизуємо основні поняття.

Частина видів (типів) визначена законодавчо в державі, де зареєстрований суб'єкт (фірма, організація, підприємство). На Україні також є нормативні акти, які регламентують деякі види (типи) інформації. У першу чергу, це Закон України "Про інформацію" [114].

Інформацію без перебільшення можна віднести до одного з вирішальних ресурсів розвитку сучасного суспільства.

Що автори будуть розуміти під інформацією і якими її властивостями цікавитися з точки зору забезпечення інформаційної безпеки?

Інформація (від лат. "Informatio" – пояснення, виклад) – це фундаментальне наукове поняття, яке існувало в багатьох країнах і європейських мовах ще з часів Стародавнього Риму. Але тлумачилося воно порізному: повідомлення, новину, повчання, рапорт, звіт, дані і т. д. Наприклад, у словнику Брокгауза Ф. А. та Ефрона І. А. говорилося: "інформація – прохання малоросійських гетьманів московському цареві або польському королю". У даний час визначення інформації також відрізняються у рамках багатьох гуманітарних і технічних наук.

Автори будуть розуміти під **інформацією** відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх подання. Таке трактування не розходиться з джерелом [114], де під інформацією розуміється "документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому середовищі". Тут же перераховані основні види інформації:

• статистична інформація;

• масова інформація;

• інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування;

• правова інформація;

• інформація про особу;

• інформація довідково-енциклопедичного характеру;

• соціологічна інформація.

При ринковій економіці інформація є об’єктом товарно-грошових відношень. У цих умовах проблема інформаційної безпеки досить актуальна для організацій з будь-якою формою власності, окремих громадян і держави в цілому.

Найважливішими властивостями інформації з точки зору її захисту є конфіденційність, цілісність і доступність [31; 36; 45].

Конфіденційність – суб’єктивно визначається (приписувана) інформації характеристика (властивість), яка вказує на необхідність введення обмежень на коло суб’єктів, що мають доступ до неї, і забезпечувана здатністю системи (середовища) зберігати вказану інформацію в таємниці від суб’єктів, які не мають повноважень на право доступу до неї. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила її отримання або ознайомлення з нею.

Цілісність – властивість інформації, що полягає в її існуванні в незмінному вигляді на певному проміжку часу. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації і видалення.

Доступність – властивість інформації бути наданою своєчасно і безперешкодно всім суб'єктам, які мають для цього належні повноваження. Інформація зберігає доступність, якщо протягом певного проміжку часу легітимним користувачам немає відмови в її отриманні.

Існують і інші **властивості інформації**: повнота, адекватність, достовірність та інші, які менш істотні в контексті даної проблеми.

Важливою особливістю інформації є і те, що у фізичному сенсі вона має на увазі свій носій. Вираз "отримати доступ до інформації" можна розуміти як отримання доступу до певного носія, що є джерелом інформації. Останні становлять документи та інші матеріальні об'єкти, що зберігають інформацію, а також повідомлення засобів масової інформації, публічні виступи і т. д. (відкриті джерела).

Під **документами** в інформаційних відносинах розуміється матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації її на папері, паперовому носії, магнітній, кіно-, відео-, фотоплівці або іншому носії. У якості останнього може виступати "електронний документ", тобто джерело інформації в електронному вигляді. Такі документи за своєю фізичною природою не мають реквізитів, властивих традиційним паперовим носіям. Тому вони значною мірою уразливі як перед випадковим спотворенням, так і перед зловмисною маніпуляцією. Упровадження систем електронного документообігу, в тому числі і в юридичній практиці, вимагає подальшої регламентації порядку формування, заощадження, поширення та знищення таких документів, а також створення ефективної системи їх захисту.

Слід зазначити, що багато авторів ототожнюють поняття **інформації** та **інформаційного ресурсу**, розглядаючи їх як синоніми. **Інформаційні ресурси** (англ. Information resource) – це окремі документи і окремі масиви документів, у тому числі, які знаходяться в інформаційних системах (бібліотеках, архівах, фондах, банках і базах даних і т. д.).

Інформаційні ресурси – це важливий компонент інформаційної інфраструктури суспільства, база для створення інформаційних продуктів – матеріалізованих результатів інформаційної діяльності [11].

Інформаційні ресурси можуть бути державними і недержавними як елемент складу майна перебувати у власності громадян, органів держа-

вної влади, органів місцевого самоврядування, організацій та громадських об'єднань.

Фізичні та юридичні особи є **власниками** тих документів, масивів документів, які створені на їхні кошти, придбані ними на законних підставах, отримані в порядку дарування чи спадкування.

Основою інформаційного суверенітету України є національні інформаційні ресурси [114].

До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форми, часу і місця створення.

Таким чином, **документування інформації** – обов'язкова умова включення інформації в інформаційні ресурси. Документ, отриманий з інформаційної системи, набуває чинності після його підписання посадовою особою в порядку, встановленому законом. Юридична сила документа, що зберігається, обробляється і передається за допомогою автоматизованих інформаційних і телекомунікаційних систем, може підтверджуватися **електронним цифровим підписом (ЕЦП)**.

Юридична сила ЕЦП визнається при наявності в інформаційній системі програмно-технічних засобів, що забезпечують ідентифікацію підпису, і дотримання встановленого режиму їх використання.

До основних секторів національної критичної інфраструктури відносять системи управління в уряді, обороні, кредитно-фінансовій і банківській системі, промисловості, транспорті, телекомунікаціях і т. д. [80; 102]. Національний інформаційний ресурс став одним з головних джерел економічної могутності держави в цілому, так і окремих фінансових, науково-дослідних і виробничих суб'єктів.

Тому інформаційна безпека виступає як невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки України [86].

У загальному випадку під **інформаційною безпекою** розуміється такий стан інформаційного середовища (інформації, інформаційної системи, інформаційного ресурсу), при якому гарантується розвиток цього середовища і її використання в інтересах особистості, суспільства і держави, а також захищеність від будь-яких загроз.

Для правильного визначення об'єкта захисту необхідно знати основні поняття, пов'язані із секретною інформацією.

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин,

державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом України "Про державну таємницю" [112], державною таємницею і підлягають охороні державою.

Матеріальні носії секретної інформації – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Система захисту державної таємниці – сукупність органів захисту державної таємниці, використовуваних ними засобів і методів захисту відомостей, що становлять державну таємницю та їх носіїв, а також заходів, що проводяться з цією метою.

Допуск до державної таємниці – процедура оформлення права громадян на доступ до відомостей, що становлять державну таємницю, а підприємств, установ і організацій – на проведення робіт з використанням таких відомостей.

Доступ до відомостей, що становлять державну таємницю, – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень [121; 186].

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

Засекречування відомостей та їх носіїв – введення у передбаченому порядку для відомостей, що становлять державну таємницю, обмежень на їх розповсюдження.

Комерційна таємниця – відомості, що не є державними секретами, пов'язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій або фірм, розголошування яких може завдати збитку їх інтересам.

Ступінь секретності – категорія, що характеризує важливість такої інформації, можливі збитки внаслідок її розголошування, ступінь обмеження доступу до неї та рівень її охорони державою. Критерій визначення ступеня секретності інформації встановлює відповідний державний орган.

7.2. Класифікація ресурсів для захисту

Сьогодні в Україні інформаційні відносини розвиваються значно швидше, ніж способи, методи й засоби їхнього регулювання. Внаслідок цього законодавча база повинна змінюватися та доповнюватися в міру виникнення відповідних проблем питань у розглянутій сфері інформаційних відносин. Це, у свою чергу, часто може приводити до протиріч у використанні законодавчої бази [1; 115].

Усю інформацію можна поділити на дві великі групи: **відкриту** й **підлягаючому захисту** (закриту або інформацію з обмеженим доступом (ІОД)). Про відкриту інформацію вести мову з погляду її захисту немає сенсу, оскільки вона є загальнодоступною.

ІОД, як правило, є регламентованою законодавчо, тому її найпростіше класифікувати. Серед такої інформації особливо виділяється група, яка називається **державна таємниця**. Зрозуміти, яка інформація ставиться до даної групи, можна на підставі [112].

Оскільки кількість інформації в системі консолідованої інформації будь-якого суб'єкта з кожним роком збільшується у кілька разів, то класифікувати види (типи) інформації в такому обсязі досить складно, крім того єдиного класифікатора (як нормативного документа) дотепер немає.

Разом з тим багато державних структур (податкові, антимонопольні, правоохоронні органи й т. п.) при виконанні ними своїх функцій одержують від різних організацій або фізичних осіб значна кількість ІОД (відомостей, що становлять комерційну й банківську таємницю, сімейну таємницю, персональні дані та ін.), які вони теж зобов'язані захищати.

Як видно із представлених даних, більша частина інформації в наслідок відсутності класифікації та неможливості обліку, приносить не враховані втрати для підприємств. У першу чергу, це фінансові, кадрові, економічні, грошові та інші види втрат.

Внаслідок зазначених причин, а також на підставі проведеного автором аналітичного дослідження, також був розроблений класифікатор видів інформації (КлВІ), представлений на рис. 7.1. Отриманий КлВІ не є уніфікованим і не може бути таким у принципі, оскільки законодавча база будь-якої розвиненої держави базується на динамічній інфраструктурі.

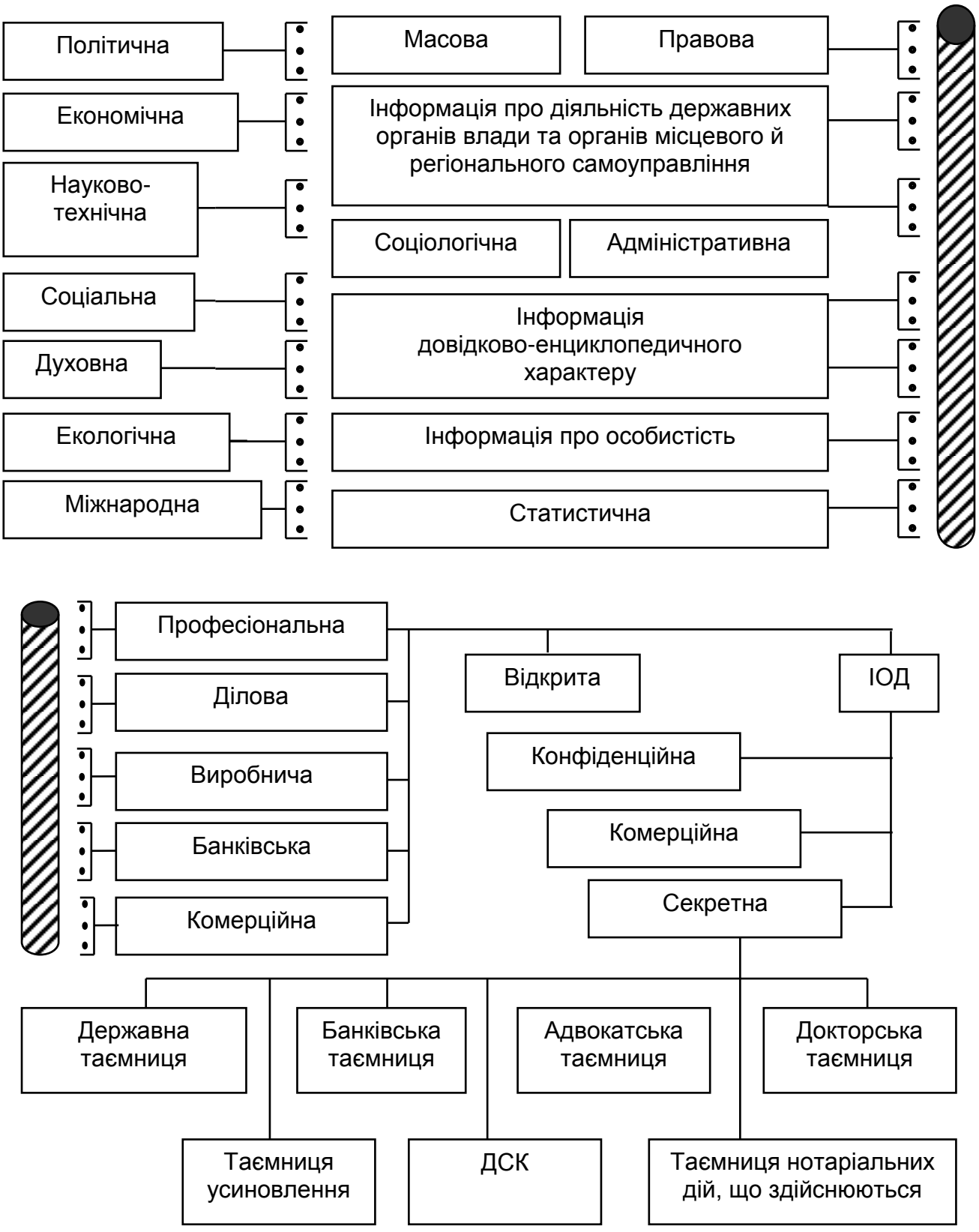


Рис. 7.1. **Класифікатор видів інформації (КлВІ)**

Як відомо, в Україні загальні правові основи отримання, використання, поширення і збереження інформації визначаються Законом України "Про інформацію" [114].

Відповідно до Закону основними принципами інформаційних відносин є: гарантованість права на інформацію, відкритість, доступність інформації й воля її обміну, повнота й точність інформації, об'єктивність, вірогідність інформації, законність одержання, використання, поширення, зберігання.

Таким чином, при використанні даного класифікатора можливо категорування всього документообміну на будь-якому суб'єкті, на підставі якого надалі можна одержати вартісну оцінку інформації, наприклад, у випадку її втрати або викривлення.

Крім того, чітко видна залежність законодавчо-визначених інформаційних відносин і видів інформації, до яких вони відносяться.

До **конфіденційної інформації** належать відомості, які знаходяться у володінні, використанні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно передбачених ними умов.

Відповідно до джерела [114]: громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не є передбаченою законом таємницею, **самостійно визначають режим доступу** до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю та здоров'ю людей.

Прикладами найбільш широко використовуваних конфіденційних відомостей є персональні дані (інформація про особу, ПдН [188]) і комерційна таємниця (КТ) [121].

Не допускається збирання, зберігання, використання та поширення інформації про приватне життя, а так само інформації, яка порушує особисту або сімейну таємницю, таємницю листування, телефонних переговорів, телеграфних та інших повідомлень фізичної особи без її згоди, крім як на підставі судового рішення [88].

При вирішенні правових питань у процесі впровадження сучасних інформаційних технологій не можна забувати про можливі порушення

законних прав та інтересів громадян в силу недобросовісної поведінки користувачів інформаційних систем.

Під **комерційною таємницею** підприємства відповідно до джерела [120] розуміються відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, які не є державною таємницею, проте їх розголошення (передача, витік) може завдати шкоди його інтересам. Склад і обсяг відомостей, що становлять КТ, визначає керівник підприємства.

Відомості, які не можуть бути віднесені до КТ, визначає Кабінет Міністрів України. До них відносять [121]:

■ статутні та інші документи, що дозволяють займатися тією чи іншою діяльністю;

■ інформація за всіма встановленими формами державної звітності;

■ дані, необхідні для перевірки нарахування і сплати податків та інших обов'язкових платежів, відомості про чисельність і склад працюючих, їхню заробітну плату загалом і за професіями, посадами, а також наявність вільних (вакантних) робочих місць;

■ інформація про забруднення навколишнього природного середовища, порушеннях безпечних умов праці, реалізації продукції, яка може нанести шкоду здоров'ю;

■ документи про платоспроможність;

■ відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, організаціях, які займаються підприємницькою діяльністю,

■ відомості, які є відкритими (підлягають оголошенню) відповідно до чинного законодавства.

Таким чином, всі інші відомості, які не входять у вищенаведений список, можуть бути віднесені керівником підприємства (а також фізичною особою, яка займається підприємницькою діяльністю) до КТ.

На підставі введеного КлВІ (рис. 7.1), при подальшому дослідженні [79], були розроблені класифікатори видів документів (КлВД), що використовуються, як базові, практично в будь-якому виді діяльності. Розроблений КлВД представлений в табл. 7.1, 7.2.

При використанні КлВІ й КлВД можливі перехідні процеси, коли один тип інформації може переходити в інший.

Таблиця 7.1

КлВД в управлінської діяльності

№ п\п	Група документів	Форма документа
1	2	3
1	Фінансування, кредитування, податкова політика	Фінансування
		Кредитування
		Державна податкова політика
2	Організація систем управління	Розпорядницька діяльність
		Контроль
		Організаційні основи керування
		Правове забезпечення керування
		Організація документованого забезпечення керування й відомчого зберігання документів
3	Прогнозування, планування, ціноутворення	Організація й методика планування
		Прогнозування й перспективне планування
		Поточне планування
		Ціноутворення
4	Облік й звітність	Оперативний та статистичний облік і звітність
		Бухгалтерський облік і звітність
5	Організація використання трудових ресурсів	Набір і використання трудових ресурсів
		Ринок праці, працевлаштування й допомога безробітним, переселення
		Організація праці, продуктивність праці, трудова дисципліна
		Технічне нормування, тарифікація, заробітна плата
		Охорона праці
6	Робота з кадрами	Підготовка кадрів, підвищення кваліфікації
		Прийом, розподіл, переміщення й облік кадрів
		Проведення атестації й установлення кваліфікації
		Присвоєння вчених звань, надання наукових ступенів
7	Адміністративно-господарське обслуговування	Адміністративно-господарські питання
		Експлуатація службових будинків
		Транспортне обслуговування
		Організація внутрішньовідомчого зв’язку
		Охорона підприємств, організацій, установ
		Приватизація загальнодержавної й комунальної власності
8	Соціально-культурний розвиток населення	Медичне й санітарно-курортне обслуговування
		Соціальне страхування й соціальний захист населення
		Житло-побутові питання й організація харчування
		Оздоровчо-виховна робота із дітьми
		Організація дозвілля, підвищення культурного рівня населення, розвиток самодіяльної творчості
		Фізкультурно-спортивна робота
9	Матеріально-технічне забезпечення	Організація матеріально-технічного постачання
		Організація схоронності майново-матеріальних цінностей

Закінчення табл. 7.1

1	2	3
10	Науково-інформаційна діяльність	Науково-технічна інформація
		Видавнича діяльність
11	Економічне, науково-технічне й культурне співробітництво із закордонними країнами	-"-
12	Діяльність суспільних організація	-"-

Таблиця 7.2

КлВД у науково-технічній і виробничій діяльності

№ п\п	Група документів	Форма документа
1	2	3
1	Науково-дослідна й дослідно-конструкторська робота	Організація й координація НДР і ДКР
		Науково-дослідна й дослідно-конструкторська робота
		Випробування дослідницьких зразків продуктів
		Впровадження НДР і ІКР
2	Винахідництво, раціоналізація й патентно-ліцензійна робота	Винахідництво й раціоналізація
		Патентно-ліцензійна робота
3	Проектування, будівництво, реконструкція	Організація проектних і будівельних робіт
		Проектно-розвідувальна робота
		Проектно-планова робота
		Проектування об’єктів капітального будівництва
		Експертиза проектів і кошторисів
		Будівництво й реконструкція
		Капітальний і поточний ремонт
4	Виробництво	Організація виробництва (В)
		Впровадження нової техніки й технологій
		Механізація й автоматизація виробничих процесів
		Конструкторська робота з виробів серійного й масового виробництва

Закінчення табл. 7.2

1	2	3
		Технологія виробництва
		Технічне оснащення В і розподіл устаткування
		Енергетичне й паливне забезпечення виробництва
		Експлуатація й ремонт устаткування
5	Якість продукції, технічний контроль, стандартизація	Якість продукції й технічний контроль
		Стандартизація
6	Охорона навколишнього середовища	Організація діяльності
		Охорона навколишнього середовища
7	Автоматизовані системи (АС)	Організація робіт зі створення АС
		Проектування АС
		Функціонування АС

Таким чином, представлені структуровані класифікатори КлВІ й КлВД, розроблені на основі системного підходу, використання яких дозволить застосувати категоріальний аналіз та одержати вартісну оцінку інформації в подальших дослідженнях [73].

7.3. Загрози та уразливості

Використовуючи результати досліджень, одержаних на першому етапі, далі необхідно виявити повну множину загроз та їх джерел для виділених об’єктів захисту (об’єктів інформаційної діяльності).

Під загрозою розуміється подія, яка потенційно може порушити одну з властивостей інформації, що захищається. Якщо джерелом загроз є діяльність людини, то говорять про *порушника*, якщо об’єктивні явища, то говорять про *техногенні та стихійні джерела загроз.* Результатом даного етапу для виділених об’єктів повинні стати розробки окремих моделей таких видів:

окрема модель загроз – опис загроз і схематичне представлення шляхів їх здійснення для об’єкта захисту;

окрема модель техногенних і стихійних джерел загроз – абстрактний формалізований або неформалізований опис чинників і джерел загроз для об’єкта захисту;

окрема модель порушника – абстрактний формалізований або неформалізований опис злочинця, здатного реалізувати загрозу (атаку) на об’єкт захисту.

Класифікація загроз інформації

Загрози циркулюючої в системі консолідованої інформації (СКІ), як правило, залежать від структури та конфігурації СКІ, технології обробки інформації в ній, стану навколишнього фізичного середовища, дій персоналу і структури самої інформації.

З множини способів класифікації загроз інформації найбільш узагальненою (базовою) є їх класифікація за наслідками можливого впливу на інформацію [84; 112; 114; 117; 121; 124; 186; 188]:

загрози порушення *конфіденційності*;

загрози порушення *цілісності*;

загрози порушення *доступності.*

Загрози конфіденційності направлені на розголошування конфіденційної або секретної інформації. У разі реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступу. Загроза порушення конфіденційності має місце кожного разу, коли можливий несанкціонований доступ до певної закритої інформації, що зберігається в комп’ютерній системі або передається від однієї системи до іншої.

Інформація зберігає *конфіденційність*, якщо дотримуються встановлені правила її отримання.

Загрози цілісності інформації направлені на її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена умисно, а також у результаті об’єктивних дій з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації, комп’ютерних мереж і систем телекомунікацій [178]. Умисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка виконується повноважними особами з обґрунтованою метою (наприклад, такою зміною є періодична корекція певної бази даних).

Інформація зберігає *цілісність*, якщо дотримуються встановлені правила її модифікації (знищення).

Загрози доступності (відмова в обслуговуванні) направлені на створення таких ситуацій, коли певні умисні дії або знижують працездатність СКІ, або блокують доступ до деяких її ресурсів. Наприклад, якщо

один користувач системи запитує доступ до певної служби, а інший чинить дії, які призводять до блокування цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурсів може бути постійним або тимчасовим.

Загрози для інформації, яка обробляється в СКІ, залежать від характеристик обчислювальної системи, фізичного середовища, персоналу, технологій обробки та інших чинників.

Єдиної й загальноприйнятої класифікації погроз ІБ не існує й, швидше за все, не буде взагалі, тому що згодом з'являються нові погрози, які все складніше ідентифікувати. Однак можна привести класифікацію за різними аспектами їх реалізації (табл. 7.3). Наведена класифікація не претендує ні на строгість, ні на повноту. Єдина її мета полягає в тому, щоб показати читачам весь спектр можливих погроз ІБ.

Крім того, серед основних загроз інформації можуть бути такі:

- розкрадання (копіювання інформації);
- знищення інформації;
- модифікація (перекручування) інформації;
- порушення доступності (блокування) інформації;
- заперечення дійсності інформації;
- нав'язування помилкової інформації.

Інформація зберігає *доступність*, якщо зберігається можливість її отримання або модифікації тільки відповідно до встановлених правил упродовж певного часу.

Отже, загрози, реалізація яких призводить до втрати інформацією вказаних властивостей, відповідно є *загрозами конфіденційності, цілісності* або *доступності інформації.*

Джерелами названих загроз інформації можуть бути люди, апаратно-програмні засоби і середовище, що оточує СКІ та її компоненти, які можуть впливати на інформацію ззовні (зовнішні джерела загроз) або знаходитися всередині СКІ (внутрішні джерела загроз).

За природою *походження* джерела загроз можуть бути *природними* і *штучними*.

Природні – це загрози, викликані впливом на СКІ та її елементи фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні – це загрози СКІ, викликані діяльністю людини. Серед них, виходячи з мотивацій дій (безвідповідальність, самоствердження, цікавість, корисливий інтерес і т. д.), можна виділити:

Таблиця 7.3

Класифікація загроз ІБ

За метою реалізації загрози			
несанкціоноване читання даних	несанкціонована зміна даних	несанкціоноване знищення даних	повне/часткове руйнування системи/мережі
За принципом впливу			
які використовують відомі (легальні) КПІ (до цього класу ставиться, наприклад, загроза несанкціонованого читання файла, доступ користувачів до якого визначений некоректно: дозволений доступ користувачу, якому, згідно ПІнБ, доступ повинен бути заборонений)	які використовують сховані КПІ (наприклад, загроза використання зловмисником недокументованих можливостей ОС)	які створюють нові КПІ за допомогою програмних закладок (наприклад, "троянських коней")	
За характером впливу			
активний вплив – НСД зловмисника в системі	пасивний вплив – несанкціоноване спостереження зловмисника за процесами, що відбуваються в системі		
За способом дій зловмисника			
в інтерактивному режимі (вручну)	у пакетному режимі (за допомогою спеціально написаної програми, що виконує негативні впливи на ОС без особистої участі користувача-зловмисника – Exploits)		
За типом слабості захисту, що використовується			
використовуючи неадекватну ПІнБ, у тому числі й помилки адміністратора системи	використовуючи помилки й недокументовані можливості ПЗ ОС, у тому числі й так звані люки – випадково або навмисно вбудовані в систему "службові входи" (Backdoors), що дозволяють обходити систему захисту (звичайно люки створюються розроблювачами ПЗ для тестування й налагодження і іноді розроблювачі забувають їх видалити або залишають спеціально [86])	використовуючи раніше впроваджену програмну закладку [61] ("троянський кінь", що спрацьовує за таймером)	
За способом впливу на об’єкт атаки			
безпосередній вплив	перевищення користувачем своїх повноважень	робота від імені іншого користувача	використання результатів роботи іншого користувача (наприклад, несанкціоноване перехоплення інформаційних потоків, ініційованих іншим користувачем)
За об’єктом атаки			
система в цілому	об’єкти системи (файли, пристрої й т. д.)	суб’єкти системи (користувачі, системні процеси й т. д.)	КПІ
За типом засобів атаки, що використовуються			
штатними засобами ОС без використання додаткового ПЗ	ПЗ третіх фірм (до цього класу ПЗ ставляться як комп’ютерні віруси й інші шкідливі програми (exploits), які можна легко знайти в Інтернет, так і ПЗ, споконвічно розроблене для інших цілей (відладчики, мережні монітори, сканери й т. д.)		спеціально розробленим ПЗ
За станом об’єкта ОС, що атакується на момент атаки			
зберігання	передача	обробка	

не умисні (випадкові) загрози, викликані помилками в апаратно-програмному забезпеченні та діях персоналу;

умисні загрози – задумані (заборонені) дії людей, направлені на порушення конфіденційності, цілісності або доступності інформації.

Поширена також класифікація інформаційних загроз за характером, *типами* і способам їх реалізації.

За характером реалізації загрози інформації поділяють на *пасивні* (без порушення цілісності СКІ та будь-якого впливу на її елементи) і *активні*, здійснювані шляхом прямого або непрямого контакту джерела загроз з елементами СКІ за допомогою якоїсь дії. Особливість пасивних способів полягає в тому, що їх складніше виявити. Реалізація активних способів дозволяє злочинцям отримати результати, досягнення яких у випадках реалізації пасивних загроз неможливе.

До основних *типів реалізації загроз* відносяться: стихійні лиха; зловмисні дії; побічні явища; відмови, збої, помилки елементів СКІ.

Більш непередбачуваними з погляду загрози захищеності інформації і, як наслідок, менш опрацьованими є заходи щодо запобігання зловмисним діям і побічним явищам [32].

До *побічних явищ* відносяться: електромагнітні випромінювання (ЕМВ) пристроїв СКІ; паразитні наведення; зовнішні ЕМВ; вібрація; зовнішні атмосферні умови.

До *зловмисних дій* відносять такі категорії порушень безпеки, як розкрадання, підміна, підключення, пошкодження, диверсія.

Зловмисні дії можуть здійснюватися безвідносно до обробки інформації або в процесі її обробки, з доступом до елементів СКІ або без нього, активно або пасивно (тобто із зміною стану системи або без).

Залежно від цього основні типи зловмисних загроз інформації в СКІ можна класифікувати таким чином:

безвідносно до обробки інформації і без доступу зловмисника до елементів СКІ: підслуховування розмов; використання оптичних, візуальних або акустичних засобів;

у процесі обробки без доступу зловмисника до елементів СКІ: ЕМВ; паразитні наведення; зовнішні ЕМВ; підключення апаратури реєстрації;

безвідносно до обробки інформації з доступом зловмисника до елементів СКІ, але без зміни останніх: копіювання магнітних та інших носіїв, вихідних та інших документів; розкрадання виробничих відходів;

у процесі обробки з доступом зловмисника до елементів СКІ, але без зміни останніх: копіювання інформації в процесі обробки; маскування під зареєстрованого користувача; використання недоліків мов програмування, програмних пасток, недоліків операційних систем і вірусів;

безвідносно до обробки інформації з доступом зловмисника до елементів СКІ із зміною останніх: підміна машинних носіїв, вихідних документів, апаратури, елементів програм, елементів баз даних, розкрадання носіїв і документів; включення в програми "троянських коней", "бомб" і т. п.; читання залишкової інформації в запам'ятовуючих пристроях після виконання санкціонованих запитів;

у процесі обробки з доступом зловмисника до елементів СКІ із зміною останніх;

незаконне підключення до апаратури і ліній зв'язку, зняття інформації на шинах живлення.

За *способами* реалізації загрози можуть здійснюватися:

за **технічними каналами**, що включають канали побічних електромагнітних випромінювань і наведень (ПЕМВН), акустичні, оптичні, радіотехнічні, хімічні та інші канали витоку інформації (КВІ);

за **каналами спеціального впливу** за рахунок формування спеціальних полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

шляхом несанкціонованого доступу (НСД) у результаті підключення до апаратури та ліній зв'язку, маскування під зареєстрованих (законних) користувачів, подолання заходів захисту для отримання (використання) інформації або нав'язування помилкової, застосування закладних пристроїв і вбудованих програм і впровадження комп'ютерних вірусів.

Несанкціонований доступ до систем консолідованої інформації

Сучасна СКІ на сьогодні не може ефективно функціонувати без автоматизованої (комп'ютерної) системи, і в більшості випадків, коли говорять про СКІ.

Існує цілий ряд нормативних документів, які регламентують аспекти захисту інформації [86; 88; 113; 124; 188] у СКІ.

Для ефективного опису загроз у СКІ необхідно за наслідками аналізу першого етапу побудови СЗІ точно представляти фізичну та логічну структуру СКІ. У загальному випадку корпоративну СКІ можна представити у вигляді сукупності:

локальної обчислювальної мережі (ЛОМ) (рис. 7.2):

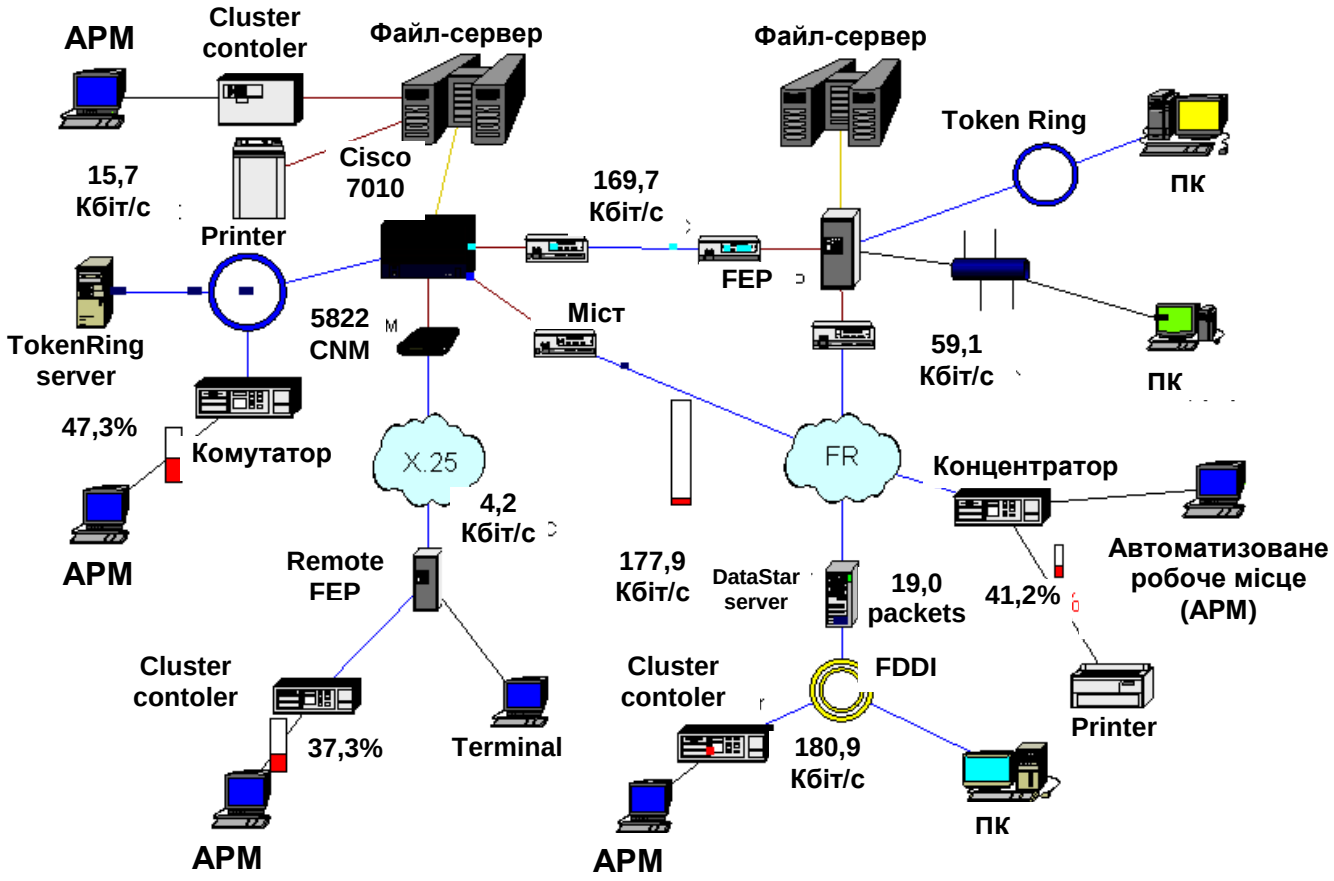


Рис. 7.2. **Приклад моделювання локальної обчислювальної мережі**

автоматизованого робочого місця (АРМ) користувача на базі персонального комп'ютера (ПК);

мережних файл-серверів;

службових робочих місць технічного персоналу, адміністратора мережі, адміністратора безпеки, програмістів;

системи передачі даних ЛОМ (рис. 7.3):

мережних адаптерів;

мостів, повторювачів, концентраторів, комутаторів;

маршрутизаторів (шлюзів);

модемів;

каналоутворюючого устаткування;

зовнішніх систем передачі даних, що використовують різні технології:

цифрові мережі з комутацією каналів;

цифрові мережі з комутацією пакетів;

виділені цифрові та аналогові канали;

телефонні мережі загального користування;

мереж віддалених користувачів.

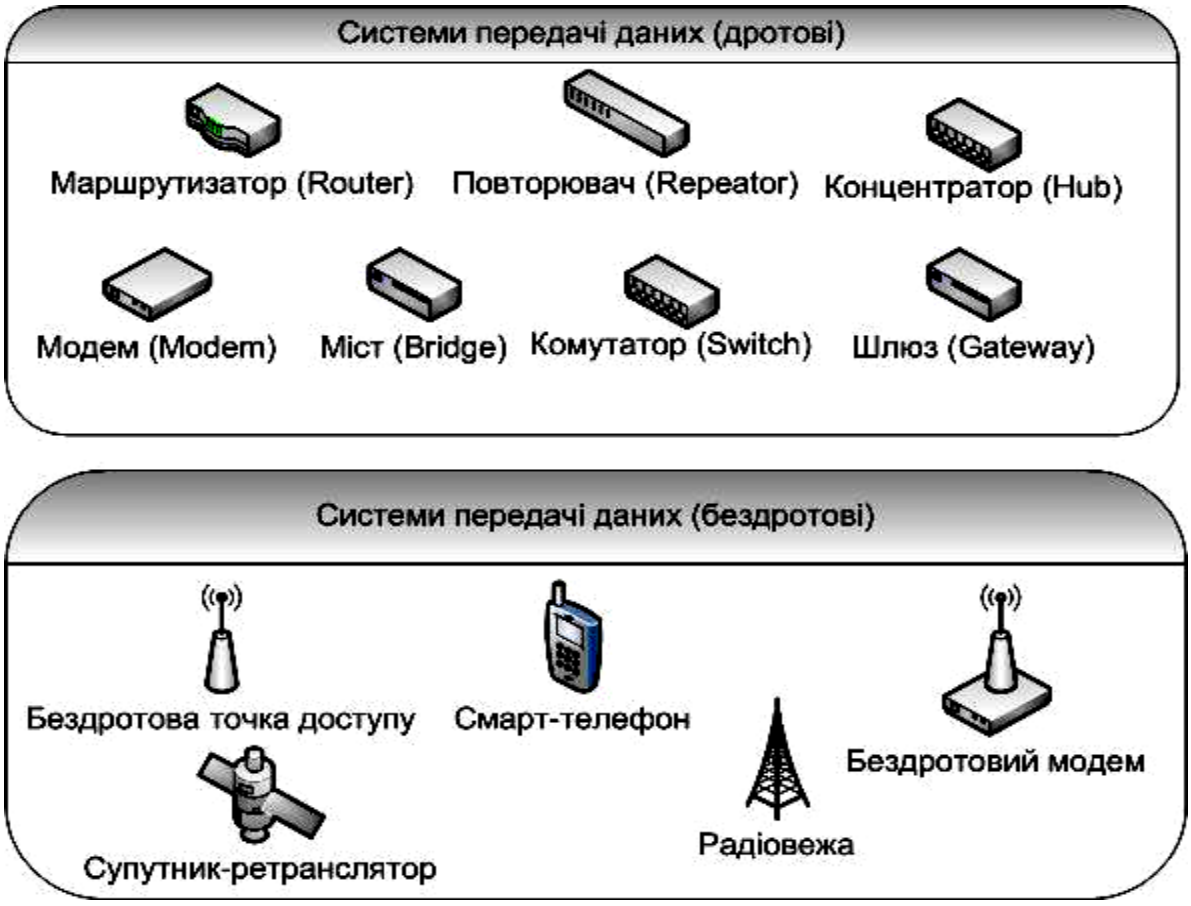


Рис. 7.3. **Системи передачі даних**

Класифікація загроз DSECCT (Digital Security Classification of Threats)

При розробці алгоритму оцінки інформаційних ризиків, заснованого на аналізі загроз і вразливостей СКІ, були розглянуті й проаналізовані різні існуючі класифікації загроз ІБ. Спроби використання даних класифікацій для опису по можливості більшої кількості загроз показали, що в багатьох випадках реальні загрози або не підходили ні під жодну із класифікаційних ознак, або навпаки – задовольняли декілька.

Таким чином, основна **мета створення класифікації загроз** – найбільш повна, детальна класифікація, що описує усі існуючі загрози ІБ, за якою кожна із загроз підпадає тільки під одну класифікаційну ознаку, і яка, таким чином, найбільш застосовна для аналізу ризиків реальних СКІ.

Крім того, фахівцями Digital Security [62] був розроблений каталог загроз і вразливостей, що відповідають розробленій класифікації.

Розроблені класифікація загроз і каталог загроз і уразливостей увійшли в новий алгоритм ГРИФ програмного комплексу Digital Security Office 2006.

Опис класифікації

За характером загрози ІБ розділяються на технологічні й організаційні (рис. 7.4). Відповідно одержимо верхній рівень класифікації:

1. Загрози технологічного характеру.

2. Загрози організаційного характеру.

Розглянемо технологічні загрози ІБ, які за видом впливу поділяються на (для отримання специфікації введемо ознаки – КЗ A.B.C.D.E, де A.B.C.D.E – відповідні рівні класів та підкласів загроз):

1.1. Фізичні (КЗ 1.1).

1.2. Програмні (логічні) (КЗ 1.2).

Наступний щабель класифікації – джерело загрози.

Джерелами фізичних загроз можуть бути:

1.1.1. Дії порушника (людини) (КЗ 1.1.1).

1.1.2. Форс-мажорні обставини (КЗ 1.1.2).

1.1.3. Відмова устаткування й внутрішніх систем життєзабезпечення.

Незалежно від джерела фізичні загрози впливають:

1.1.1.1. На ресурс (КЗ 1.1.1.1).

1.1.1.2. На канал зв’язку (КЗ 1.1.1.2).

Далі перейдемо до розгляду програмних загроз.

Джерелами програмних загроз можуть бути:

1.2.1. Локальний порушник (КЗ 1.2.1).

1.2.2. Віддалений порушник (КЗ 1.2.1).

Об’єктом локального порушника може бути тільки ресурс. При цьому на ресурсі локальний порушник може реалізувати загрози, спрямовані:

1.2.1.1.1. На ОС (КЗ 1.2.1.1.1).

1.2.1.1.2. На прикладне ПЗ (КЗ 1.2.1.1.2).

1.2.1.1.3. На інформацію (КЗ 1.2.1.1.3).

Загрози, що виходять від віддаленого порушника, можуть впливати:

1.2.2.1. На ресурс (КЗ 1.2.2.1).

1.2.2.2. На канал зв’язку (КЗ 1.2.2.2).

При доступі до ресурсу віддалений порушник може впливати:

1.2.2.1.1. На ОС (КЗ 1.2.2.1.1).

1.2.2.1.2. На мережні служби (КЗ 1.2.2.1.2).

1.2.2.1.3. На інформацію (КЗ 1.2.2.1.3).

При впливі на КПІ порушник реалізує загрози, що спрямовані:

1.2.2.2.1. На мережне устаткування (КЗ 1.2.2.2.1).

1.2.2.2.2. На протоколи зв’язку (КЗ 1.2.2.2.2).

Класифікація загроз Digital Security
(Digital Security Classification of Threats)

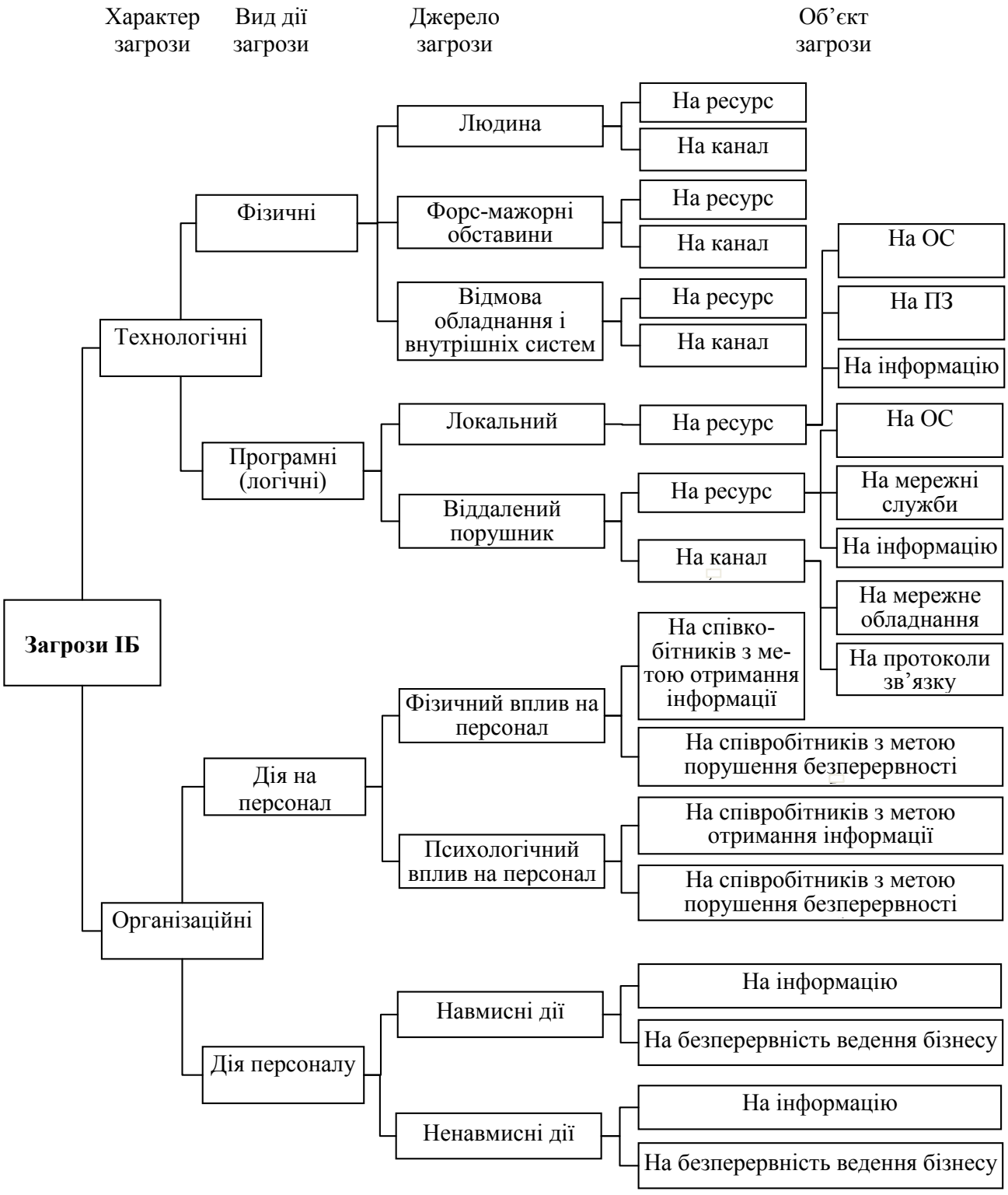


Рис. 7.4. **Класифікація загроз безпеки DSECCT**

Розглянемо організаційні загрози. Організаційні загрози за джерелом впливу поділимо на:

2.1. Вплив на персонал (КЗ 2.1).

2.2. Дії персоналу (КЗ 2.2).

Вплив на персонал може бути:

2.1.1. Фізичним (КЗ 2.1.1).

2.1.2. Психологічним (КЗ 2.1.2).

Як фізичний, так і психологічний вплив на персонал спрямовано на співробітників компанії з метою:

2.1.1.1. Одержання інформації (КЗ 2.1.1.1).

2.1.1.2. Порушення безперервності ведення бізнесу (КЗ 2.1.1.2).

Причинами дій персоналу, здатних викликати загрози ІБ:

2.2.1. Навмисні дії (КЗ 2.2.1).

2.2.2. Ненавмисні дії (КЗ 2.2.2).

Загрози, викликані навмисними діями персоналу, спрямовані:

2.2.1.1. На інформацію (КЗ 2.2.1.1).

2.2.1.2. На безперервність ведення бізнесу (КЗ 2.2.1.2).

Загрози, викликані ненавмисними діями персоналу, спрямовані:

2.2.2.1. На інформацію (КЗ 2.2.2.1).

2.2.2.2. На безперервність ведення бізнесу (КЗ 2.2.2.2).

Таким чином, можливо побудувати матрицю зв’язності типових підрозділів підприємства будь-якої сфери діяльності та класів загроз та атак, як наведено у табл. 7.4.

Таблиця 7.4

Матриця зв’язності підрозділів підприємства й класів загроз та атак

Назва підрозділу	**Клас загрози (КЗ)**						**Клас атаки (КВА)**					
	1.1.1	**1.2.1**	**…**	**2.1.1**	**2.2.2**	**∑**	**1.1**	**3.1**	**…**	**4.2**	**5.1**	**∑**
Юридичний відділ	1	1	0	0	1	**3**	0	0	1	0	1	**2**
Бухгалтерія	0	1	0	0	1	**2**	0	1	0	0	0	**1**
Виробничий цех	0	0	0	0	0	**0**	0	0	0	0	0	**0**
Економічний відділ	1	1	1	1	0	**4**	1	1	1	1	1	**5**
Дирекція	1	0	1	0	1	**3**	1	0	0	1	1	**3**
Відділ кадрів	0	1	0	1	1	**3**	0	0	1	1	0	**2**

Також на основі використання методиці, що наведена нижче за допомогою формул (7.1 – 7.4) за аналогією можливо отримати відповідні коефіцієнти зв’язності та їх нормалізований вигляд.

На основі введених класифікаторів й способів одержання НСД до ІОД, можна побудувати табличну (матричну) модель їх залежностей для будь-якого підприємства [69], як, наприклад, наведено в табл. 7.5.

Таблиця 7.5

Взаємозв'язок способів НС до об'єктів і джерел охоронюваної інформації

Способи НСД	Типи КВІ			
	Візуально оптичні	**Акустичні**	**Електромагнітні (магнітні, електричні)**	**Матеріально-речовинні**
Підслуховування	0	1	1	0
Візуальне спостереження	1	0	0	0
Розкрадання	0	0	1	1
Копіювання	1	0	1	1
Підробка	0	0	1	1
Незаконне підключення	0	1	1	0
Перехоплення	0	1	1	0
Фотографування	1	0	0	0
Разом за типом КВІ	**3**	**3**	**6**	**3**

У результаті проведення подібних дій можна одержати частотний (або нормований частотний) аналіз НСД до об'єктів і джерел ІОД із прив'язкою до типів КВІ в часі. Тим самим одержимо динамізм виникнення НСД і використання КВІ на підприємстві, результати аналізу якого необхідно використовувати при розробці й впровадженні ПІнБ.

Якщо реалізувати підсумкову суму типів КВІ у вигляді коефіцієнта зв'язності, що буде показувати умовну важливість КВІ стосовно типів НСД, які використовуються, до ІОД, то одержимо:

$$K_B^i = \sum_j x_{ij}, \qquad (7.1)$$

де K^i_B – введений коефіцієнт зв'язності для і-го (і = 4) типу КВІ;

X_{ij} – змінна, визначальний факт використання j-го (j = 8) типу НСД для і-го типу КВІ.

Тоді:

$$K_B = \{K^i_B\} = \{3, 3, 6, 3\}. \qquad (7.2)$$

Для одержання можливості обліку коефіцієнта зв'язності K_i в інтегральних показниках фізичної природи проведемо його нормування. Тоді:

$$ {}^{н}K_B^i = \frac{K_B^i}{\sum_{i=1}^{q} K_B^i}; \qquad (7.3) $$

де ${}^{н}K^i_B$ – нормований коефіцієнт зв'язності;

$q = j = \{n-1\}$.

Тоді:

$$ {}^{н}K_B = \{{}^{н}K^i_B\} = \{0,2;\ 0,2;\ 0,4;\ 0,2\}. \qquad (7.4) $$

Таким чином, на основі отриманих даних можна оцінити необхідність введення спеціальних заходів для запобігання використання й усунення КВІ.

За допомогою отриманих коефіцієнтів зв'язності та їх нормалізованого вигляду можливо формування експертних рекомендацій щодо визначення необхідних заходів щодо запобігання або нейтралізації можливих загроз та атак.

7.4. Класифікація атак та вірусів

Мережні системи характерні тим, що **поряд зі звичайними (локальними) атаками, здійснюваними в межах однієї СКІ**, до них застосовуємо специфічний вид атак, обумовлений розподільністю ресурсів та інформації в просторі. Це так звані **мережні (або віддалені) атаки**. Вони **характерні**, по-перше, тим, що злочинець може перебувати за тисячі кілометрів від об'єкта, що атакується, і, по-друге, тим, що нападу може піддаватися не конкретний комп'ютер, а інформація, що передається мережними з'єднаннями. Специфіка СКІ полягає у тому, що якщо в локальних СКІ найбільш частому минулому загрози розкриття й цілісності, то в мережних системах на перше місце виходить загроза відмови в обслуговуванні.

Під віддаленою атакою (ВА) будемо розуміти інформаційний руйнуючий вплив на СКІ, програмно здійснюваний каналами зв'язку [65]. Це визначення охоплює обидві особливості мережних систем – розподіленість комп'ютерів та інформації. Тому для більш точного опису віддалених атак і пропонується класифікація (рис. 7.5).

Тому будуть розглянуті два види таких атак:

ВА на інфраструктуру й протоколи мережі;

УА на телекомунікаційні служби.

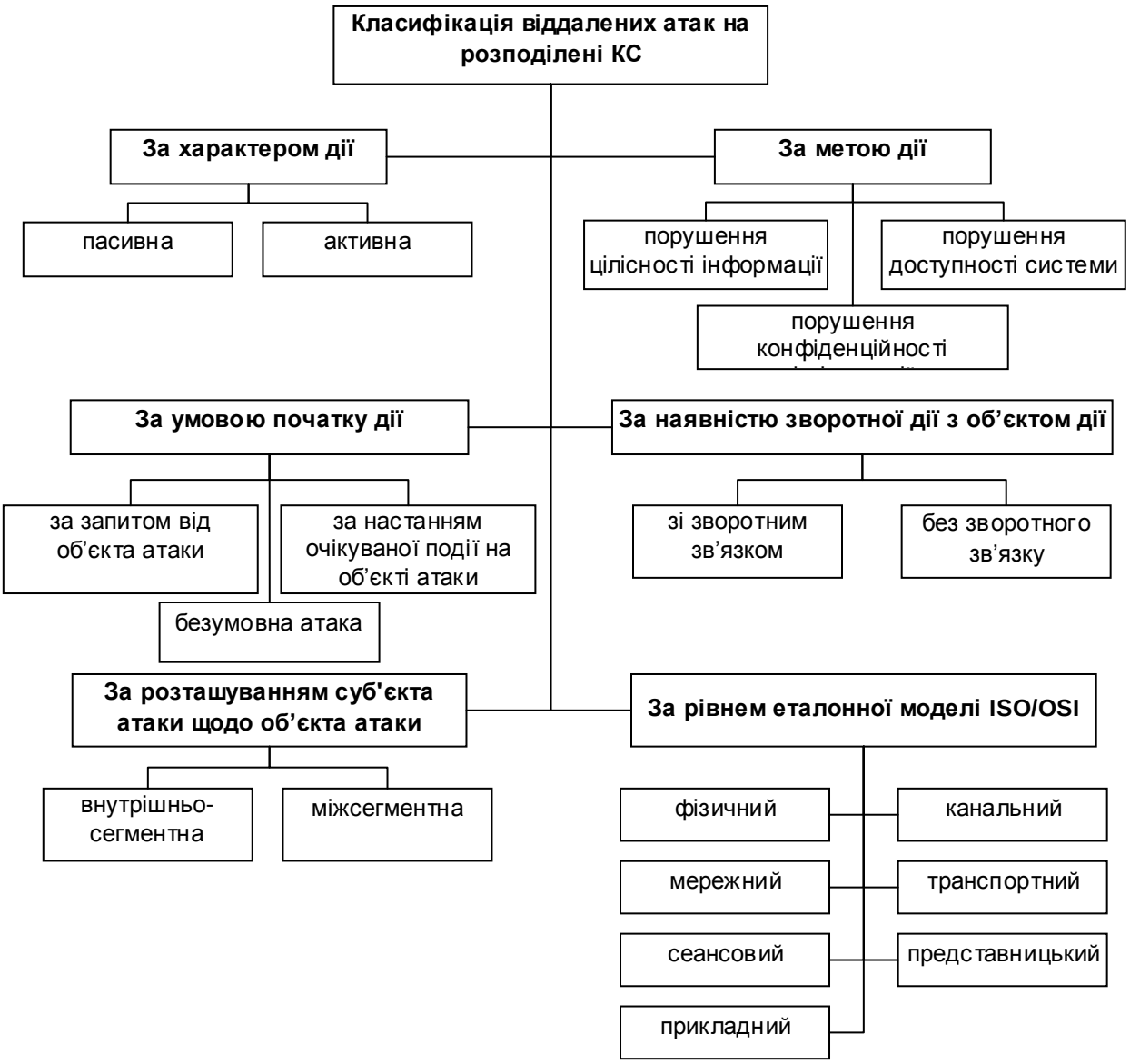


Рис. 7.5. **Загальна класифікація віддалених атак** [63]

Перші використовують вразливості у мережних протоколах та інфраструктурі мережі, а другі – вразливості у телекомунікаційних службах. При цьому під **інфраструктурою** мережі розуміється сформована система організації відносин між об'єктами мережі й використовувані в мережі сервісні служби.

Основне завдання хакера полягає у тому, щоб, досліджуючи СКІ, виявити слабкі місця (вразливості) у її системі ІБ й інформувати користувачів і розроблювачів системи з метою наступного усунення знайдених уразливостей. Інше завдання хакера – проаналізувавши існуючу безпеку СКІ, сформулювати необхідні вимоги й умови підвищення рівня її захищеності.

Основне завдання кракера полягає у безпосередньому здійсненні злому системи з метою одержання НСД до чужої інформації – інакше кажучи, для її крадіжки, підміни або для оголошення факту злому.

Кракерів можна розділити на три класи залежно від мети, з якою здійснюється злом: вандали, "жартівники", професіонали.

Вандали – найвідоміша й незчисленна частина кракерів. Їхня основна мета – зламати систему для її руйнування.

"Жартівники" – найбільш необразлива частина кракерів, основна мета яких – популярність, що досягається шляхом злому СКІ і внесення різних ефектів, що виражають їхнє незадоволене почуття гумору.

Зломщики – професійні кракери, що користуються найбільшою пошаною й повагою у кракерському середовищі, основне завдання яких – злом СКІ із серйозною метою, як ось: крадіжка або підміна інформації, що зберігається там.

У загальному випадку для того, щоб здійснити злом системи, необхідно пройти три основні стадії:

дослідження СКІ із виявленням вад у ній;

розробка програмної реалізації атаки;

безпосереднє її здійснення.

Таким чином, віддалені атаки можна класифікувати за ознаками, показаним на рис. 2.24:

1. За характером впливу:

пасивне (клас 1.1);

активне (клас 1.2).

Пасивний вплив на СКІ не робить безпосереднього впливу на роботу СКІ, але може порушувати її політику ІБ (ПІнБ).

Активний вплив на СКІ – безпосередній вплив на роботу системи й порушення прийнятої в ній ПІнБ. Усі типи ВА є активними впливами.

2. За метою впливу:

порушення конфіденційності інформації або ресурсів системи (клас 2.1);

порушення цілісності інформації (клас 2.2);

порушення працездатності (доступності) системи (клас 2.3).

Ця класифікаційна ознака є прямою проекцією трьох основних типів загроз – розкриття, цілісності й відмови в обслуговуванні.

Основна мета практично будь-якої атаки – одержати НСД до інформації. Існують дві принципові можливості доступу до інформації: перехоплення й перекручування.

Можливість **перехоплення** інформації означає одержання до неї доступу, але неможливість її модифікації. Отже, перехоплення інформації веде до порушення її конфіденційності.

Можливість **перекручування** інформації означає або повний контроль над інформаційним потоком між об'єктами системи, або можливість передачі повідомлень від імені іншого об'єкта.

Принципово іншою метою атаки є порушення працездатності системи. У цьому випадку не передбачається одержання атакуючою стороною НСД до інформації. Її основна мета – досягти, щоб ОС на об'єкті, що атакується, вийшла з ладу й для всіх інших об'єктів системи доступ до ресурсів атакованого об'єкта був би неможливий.

3. За умовою початку здійснення впливу

Віддалений вплив, також як і будь-яке інше, може почати здійснюватися тільки за певних умов. У СКІ існують три види умов початку здійснення ВА:

атака за запитом від об'єкта, що атакується, (клас 3.1): атакуючий очікує передачі від потенційної мети атаки запиту певного типу, що й буде умовою початку здійснення впливу;

атака з настання очікуваної події на об'єкті, що атакується (клас 3.2): атакуючий здійснює постійне спостереження за станом ОС віддаленої мети атаки й при виникненні певної події в цій системі починає вплив;

безумовна атака (клас 3.3): початок здійснення атаки, безумовно, стосовно мети атаки, тобто атака здійснюється негайно й безвідносно до стану системи й об'єкта, що атакується.

4. За наявності зворотного зв'язку з об'єктом, що атакується:

зі зворотним зв'язком (клас 4.1);

без зворотного зв'язка (односпрямована, клас 4.2).

ВА, здійснювана за наявності зворотного зв'язку з об'єктом, що атакується, характеризується тим, що на деякі запити, передані на об'єкт, що атакується, потрібно одержати відповідь. А, отже, між атакуючим і метою атаки існує зворотний зв'язок, що дозволяє атакуючій стороні адекватно реагувати на всі зміни, що відбуваються на об'єкті, що атакується.

ВА без зворотного зв'язку не потрібно реагувати на які-небудь зміни, що відбуваються на об'єкті, який атакується. Атаки даного виду, звичайно, здійснюються передачею на об'єкт, що атакується, одиночних запитів, відповіді на які атакуючої стороні не потрібні.

5. За розташуванням суб'єкта атаки щодо об'єкта, що атакується:

внутрішньосегментне (клас 5.1);

міжсегментне (клас 5.2).

У випадку **внутрішньосегментної атаки**, як випливає з назви, суб'єкт і об'єкт атаки перебувають в одному сегменті.

При **міжсегментній атаці** суб'єкт і об'єкт атаки перебувають у різних сегментах.

Далі буде показано, що на практиці міжсегментну атаку здійснити значно складніше, ніж внутрішньосегментну. Важливо зазначити, що міжсегментна ВА становить більшу небезпеку, ніж внутрішньосегментна. Це пов'язано з тим, що її об'єкт і безпосередньо атакуючий можуть перебувати на відстані багатьох тисяч кілометрів один від одного, і це може істотно перешкодити відбиттю ВА.

6. За рівнем еталонної моделі ISO/OSI, де здійснюється вплив:

фізичний (клас 6.1);

канальний (клас 6.2);

мережний (клас 6.3);

транспортний (клас 6.4);

сеансовий (клас 6.5);

представницький (клас 6.6);

прикладний (клас 6.7).

Будь-який мережний протокол обміну, як і будь-яку мережну програму, можна з тим або іншим ступенем точності спроектувати на модель OSI. ВА є мережною програмою. У зв'язку із цим логічним є розглядати ВА на СКІ, проектуючи їх на модель ISO/OSI.

Типові віддалені атаки

Аналіз мережного трафіка. Особливість СКІ – розподіленість об'єктів – призводить до появи специфічного для СКІ типового віддаленого впливу, що полягає у прослуховуванні каналу зв'язку. Назвемо даний типовий віддалений вплив *аналізом мережного трафіка* (або скорочено мережним аналізом).

Аналіз мережного трафіка дозволяє вивчити логіку роботи СКІ, тобто одержати взаємно однозначну відповідність подій, що відбуваються в

системі, і команд, що пересилаються один одному її об’єктами, у момент появи цих подій. Це досягається шляхом перехоплення й аналізу пакетів обміну на канальному рівні. Знання логіки роботи СКІ дозволяє на практиці моделювати й здійснювати типові віддалені атаки. Класифікація типових ВА [62] наведена в табл. 7.6.

Таблиця 7.6

Класифікація типових віддалених атак на СКІ

Типова ВА	Характер впливу		Мета впливу			Умова початку здійснення впливу			Наявність зворотного зв’язку з об’єктом, що атакується		Розташування суб’єкта атаки щодо об’єкта, який атакується		Рівень моделі OSI						
Клас впливу	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	6.5	6.6	6.7
Аналіз мережного трафіка	+	-	+	-	-	-	-	+	-	+	+	-	-	+	-	-	-	-	-
Підміна довіреного об’єкта СКІ	-	+	+	+	-	-	+	-	+	+	+	+	-	-	+	+	-	-	-
Впровадження в СКІ помилкового об’єкта (нав’язування помилкового маршруту)	-	+	+	+	+	-	-	+	+	+	+	+	-	-	+	-	-	-	-
Впровадження в СКІ помилкового об’єкта (використання недоліків алгоритмів віддаленого пошуку)	-	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	-	-	-
Відмова в обслуговуванні	-	+	-	-	+	-	-	+	-	+	+	+	-	+	+	+	+	+	+

Він також дозволяє перехопити потік даних, якими обмінюються об'єкти СКІ. Таким чином, ВА даного типу полягає в одержанні на віддаленому об'єкті НСД до інформації, якою обмінюються два мережних абоненти. Зазначимо, що при цьому відсутня можливість модифікації трафіка й сам аналіз можливий тільки усередині одного сегмента мережі. Прикладом перехопленої інформації за допомогою даної ВА можуть бути ім'я й пароль користувача, що пересилаються в незашифрованому вигляді по мережі.

За характером впливу аналіз мережного трафіка є пасивним впливом (клас 1.1). Здійснення даної атаки без зворотного зв'язку (клас 4.2) веде до порушення конфіденційності інформації (клас 2.1) усередині одного сегмента мережі (клас 5.1) на канальному рівні OSI (клас 6.2). При цьому початок здійснення атаки, безумовно, стосовно мети атаки (клас 3.3).

Далі наведемо деякі описи конкретних ВА [65].

Land attack. Хакер намагається уповільнити роботу вашої машини, пославши пакет з ідентичними адресами одержувача й відправника. Для стека протоколів Інтернет така ситуація ненормальна. ПК намагається вийти з нескінченної петлі звертань до самого себе. Є патчі для більшості ОС.

Teardrop attack. Небезпечне перекриття IP-фрагментів, сформоване програмою teardrop. ОС може стати нестабільною або зруйнуватися. Є патчі для більшості ОС. Адреса відправника найімовірніше не є правдивою. Це означає, що відправник використовує фальшиву IP-адресу.

NewTear attack. Небезпечне перекриття IP-фрагментів, сформоване програмою newtear. ОС може стати нестабільною або зруйнуватися. Є патчі для більшості ОС. Адреса відправника найімовірніше не є правдивою.

SynDrop attack. Небезпечне перекриття IP-фрагментів, сформоване програмою syndrop. ОС може стати нестабільною або зруйнуватися. Є патчі для більшості ОС.

Ping of death. Перевищення максимально можливого розміру IP-пакета. У максимальний розмір IP-пакета (65 535 байт) включається довжина IP-заголовка й довжина поля даних в IP-пакеті. Тому що IP-заголовок має мінімальний розмір в 20 байт (максимальний в 60), то, відповідно, розмір переданих в одному IP-пакеті даних не може перевищувати 65 535 - 20 = 65 515 байт. Тестувати свої програми на мінімальних і, найголовніше, на максимальних значеннях, тобто на граничних критичних значеннях – стандартний для будь-якого програміста хід. Подібні тести дозволяють виявити такі неприємні помилки, як усілякі переповнення.

У принципі ніщо не заважає атакуючий стороні сформувати набір фрагментів, які після складання перевищать максимально можливий розмір IP-пакета. Можливо, у цій фразі й сформульована основна ідея даної атаки.

18 грудня 1996 року на інформаційному сервері CERT з'явилися повідомлення про те, що більшість мережних ОС, які підтримує протоколи TCP/IP, мають таку вразливість: при передачі на них IP-пакета довжиною більше максимально припустимого значення в них переповняється буфер або змінна, і система зависає або перезавантажується – відмова в обслуговуванні. Також був наведений наступний список потенційно небезпечних платформ: Berkeley Software Design, Inc. (BSDI); Computer Associates, Intl. (products for NCR); Cray Research; Digital Equipment Corporation; FreeBSD, Inc.; Hewlett-Packard Company; IBM Corporation; Linux Systems; Open Software Foundation (OSF); Sun Microsystems, Inc.

Але перш ніж почати експерименти, було вирішено звернути увагу на WWW-сервер, де експертами проводилися подібні дослідження на різних ОС. Там, можливо, як і в CERT, ця атака називалася "Ping Death". На цьому WWW-сервері пропонувалося реалізувати атаку в такий спосіб: на робочій станції з ОС Windows '95 або Windows NT необхідно виконати таку команду:

ping -l 65527 victim.destination.IP. address (тому – "Ping Death").

Тому що звичайний розмір IP-заголовка становить 20 байт, розмір ICMP-заголовка – 8 байт, то подібний ICMP-пакет буде перевищувати максимально можливий розмір IP-пакета на 20 байт

(65 527 + 20 +8 – 65 535 = 20).

Таким чином, ці "експерти" декларували, що звичайною командою ping нібито можна порушити працездатність практично будь-який мережний ОС. На завершення на цьому сервері наводилася наступна таблиця тестування різних ОС, на які дана ВА нібито зробила необхідний ефект. Далі автор наводить таблицю з істотними скороченнями (табл. 7.7).

Було почато тестування й жодна з досліджуваних ОС – ні IRIX, ні AIX, ні VMS, ні SunOs, ні FreeBSD, ні Linux [56], ні Windows NT 4.0, ні навіть Windows '95 і Windows for WorkGroups 3.11 – абсолютно ніяк не реагували на подібний некоректний запит і продовжували нормально функціонувати. Тоді були розпочаті спеціальні пошуки ОС, яку б дійсно вивела з ладу дана атака. Нею виявилася Windows 3.11 з WinQVT – ця ОС дійсно "зависла".

Таблиця 7.7

Уразливі ОС

ОС	Версія	Симптоми
Solaris (x86)	2.4, 2.5, 2.5.1	Перезавантаження
Minix	1.7.4, v2.0 and probably others	Руйнування
HP3000 MPE/i	4.0, 5.0, 5.5	System abort
Convex SPP-UX	All version	Руйнування
Apple Mac	Mac Os 7.x.x	Руйнування
Windows 3.11 with Trumpet Winsock	?	Mixed reports
Novell NetWare	3.x	Mixed results
Windows ’95	All of ’em	Руйнування
AIX	3 and 4	Формування дампа ОС
Linux	? 2.0.23	Спонтанне перезавантаження або помилка ядра
DEC Unix/OSF1	2.0 and above	Помилка ядра
HP-UX	9.0 to 10.20	Руйнування, перезавантаження, "зависання"...
Windows NT	3.5.1	Змішаний звіт
Irix	5.3	Помилка ядра
Windows NT	4.0	Руйнування
SCO Openserver	4.2, 5.0.x	Вразливість
DEC TOPS-20, TOPS-10	All	Помилки
Digital Firewall	?	Вразливість
AltaVista Firewall for UNIX	?	Вразливість

На запит, надісланий так званим "експертам", яким настільки довіряють CERT і CIAC, де попросили пояснити виниклу ситуацію, а також відомості з табл. 7.7, була отримана відповідь; у ньому говорилося, що успіх даної атаки залежить від багатьох факторів, а саме: ПЗ й апаратного забезпечення, установленого на ПК, і, найголовніше, від фази місяця. Далі наводимо опис exploit’a, створеного для Windows NT 4.0, завдання якого, використовуючи ping, зробити так, щоб "завис" власний ПК. Першим кроком пропонувалося запустити Web Browser. На другому кроці було потрібно запустити taskmgr (Task Manager). У коментарях до цього кроку говорилося, що так Ping Death працює краще. І, нарешті, було потрібно запустити 18 ping-процесів (не більше й не менше; можливо, краще відразу 100). ОС не "зависне" миттєво. У коментарях до exploit’у до одержання ефекту пропонувалося чекати приблизно 10 хвилин, з філо-

софським зауваженням про те, що очікування може протривати дещо більше або дещо менше.

Nestea attack. Небезпечне перекриття IP-фрагментів, сформоване програмою nestea. ОС може стати нестабільною або зруйнуватися. Є патчі для більшості ОС. Адреса відправника найімовірніше не є правдивою. Це означає, що відправник використовує фальшиву IP-адресу. На жаль, не існує простих способів визначити, хто в дійсності посилає кадри з перекрученою адресою відправника.

Traceroute (tracert). Хтось намагається відстежити шлях від своєї машини до вашої. Утиліта traceroute широко використовується в Інтернет для пошуку шляху між машинами. Програма traceroute виконує цю роботу й визначає віртуальний шлях через Інтернет. Програма traceroute не є небезпечною. Не існує способу проникнути у ваш ПК, використовуючи її. Однак вона допомагає хакеру відстежити ваші з'єднання через Інтернет. Ця інформація може використовуватися для компрометації деяких інших учасників ваших зв'язків. Наприклад, у минулому цей вид інформації використовувався хакерами для того, щоб відключити свою "жертву" від Інтернету, змусивши найближчий маршрутизатор, щоб зависла телефонна лінія.

Snork attack. Реєструються UDP-дейтагарами з портом призначення 135 (Microsoft Location Service) і відправник з портом 7 (Echo), 19 (Chargen) або 135. Це спроба замкнути дві служби, якщо вони дозволені/активовані й змусити їх нескінченно обмінюватися пакетами один з одним. Існує патч для блокування таких атак.

AntiSniff DNS exploit. Програма AntiSniff може бути використана шляхом посилання спеціального DNS-кадру. У випадку успіху хакер може використовувати програму, що працює у системі, де працює AntiSniff. AntiSniff – це програма, що розроблена L0pht Heavy Industries у липні 1999. Хакер може використовувати L0pht AntiSniff для одержання інформації про мережу, що може виявитися для нього корисною при наступних атаках. Хакер може також використовувати L0pht AntiSniff для визначення положення компрометуючих ПК, переведених у режим 6 (sniffing), які можуть ним пізніше використовуватися.

HTTP URL directory traversal/climbing. Ситуація виглядає так, начебто хакер намагається прочитати сторонні файли ОС. Звичайна помилка web-браузера полягає у тому, що хакер може специфікувати URL, яке виглядає як /../../../foo/bar.txt. Ця атака вдається, тому що програміст не здійснює подвійної перевірки URL, щоб переконатися, чи коректний файл

web-сайта. Сигнатурою атаки може бути наявність в URL послідовності ../... Іноді така атака може бути імітована некоректними зв'язками, розміщеними на сторінці. Це говорить про некоректну конфігурацію. По-перше, перевірте параметри URL, щоб з'ясувати, до якого файла має намір одержати доступ хакер. Потім перевірте, чи одержав хакер доступ до файла. Якщо це дійсно критичний файл і атака була успішною, необхідно почати термінові дії. Наприклад, якщо хакер одержав доступ до файла паролів, необхідно замінити всі паролі. Варто також перевірити, чи є версія сервера новітньою й чи використані всі існуючі патчі. Більшість таких атак уживається проти "вбудованих" web-серверів (тобто web-серверів, доданих як частина іншого програмного продукту), а не проти реальних web-серверів типу Apache і IIS.

Telnet Backdoor. Хакер намагається скористатися відомим ім'ям/паролем "схованих" дверей telnet Trigger. Протокольний аналізатор витягає login-name і пароль із вхідного рядка Telnet і порівнює їх зі списком відомих параметрів доступу для "схованих" дверей telnet.

Finger forwarding. Спроба використання програми finger для переадресації запиту іншій системі. Часто використовується хакерами, щоб замаскувати свою ідентифікацію. Finger підтримує рекурсивні запити. Запит типу "rob@foo@bar" просить "bar" повідомити інформацію про "rob@foo", змушуючи "bar" надіслати запит "foo". Ця техніка може використовуватися для приховування правдивого джерела запиту. Finger є небезпечним джерелом інформації й із цієї причини повинен бути заблокований в /etc/inetd.conf.

Finger Backdoor. Хтось намагається повторно ввійти в ОС через відомі "таємні" двері в finger. Через те, що система була скомпрометована, хакери можуть залишити для себе відкриті "таємні" двері. Наприклад, одні "таємні" двері допускають посилку finger команди "cmd_rootsh", що відкриває shell із привілеями суперкористувача. Зазначимо, що якщо таємні двері дійсно є, ваша система вже була скомпрометована. У цей час всі відомі таємні двері finger існують тільки в системах UNIX. Якщо ви зіштовхнулися з такою проблемою то, по-перше, перегляньте інформацію відгуків, що може бути в наявності. Якщо ви виявили якісь повідомлення про помилки, то ймовірно спроба вторгнення не була успішною (однак не сподівайтеся). По-друге, якщо ви стурбовані можливістю наявності таємних дверей в системі, виконайте команду finger самі. Щоб усунути вразливість даного виду, треба, по-перше, розглянути можливість видалення

послуги finger взагалі. Це небезпечна послуга, що надає корисну інформацію хакерам. По-друге, якщо ви відчуваєте, що ОС скомпрометовано, варто заново інсталювати ОС. Пошукайте таємні двері. Важко уявити, що якийсь користувач у вашій системі має ім'я "cmd_shell". Багато широкодіапазонних сканерів шукають такі таємні двері.

Back Orifice (BO). Ця скромна програма розміром усього в 120k(!) є "троянським конем". Вона усього лише надає анонімному віддаленому користувачеві повний контроль над Windows 9x, підключеному до Інтернету, отже:

доступ до жорсткого диска "жертви" через браузер;

редагування реєстру;

повний контроль над файловою системою;

звіт про введені паролі;

копія екрана;

перегляд мережних ресурсів, підключених до жертви;

керування списком процесів;

віддалене перезавантаження;

віддалене виконання програм з можливістю перенапряму консолі клієнтові (свого роду телнет).

Наведений список можливостей не повний, тому BO майже серйозно можна рекомендувати мережним адміністраторам як безкоштовну альтернативу таким недешевим продуктам, як Landesk Management Suite або Managewise, точніше, що входить у ці пакети засобам доступу до ПК користувачів. Завантажити BO і знайти повну інформацію можна за адресою http://www.cultdeadcow.com.

Як і всі засоби віддаленого адміністрування, BO складається із двох частин – сервера й клієнта. Сервер запускається один раз на машині "жертви", він швидко відпрацьовує й видаляє себе, але до видалення він устигає сховатися в надрах ОС так, що знайти його сліди нелегко. Поширюється BO дуже просто – деякі вже одержали "прискорювачі IRC", "патчі до ICQ", причому того самого розміру 120 Кб. Клієнти BO існують під Unix, OS/2 і Win32. Крім того, сервер просто представить будь-якому віддаленому браузеру жорсткий диск із ОС. Він же дозволить із браузера зробити download або upload. Клієнт – це текстова оболонка з вбудованою допомогою, досить зручною у використанні. Під win32 є GUI-Клієнт, однак його функціональність викликає сумніви.

PCAnywhere ping. Хтось пінгує ОС для того, щоб перевірити, чи працює PCAnywhere. Це може бути атака, але може бути й інцидент. PCAnywhere є продуктом Symantec, що дозволяє здійснити віддалене керування ПК. Вона є дуже популярною в Інтернеті для легальних цілей, дозволяючи адміністраторам віддалено контролювати сервери. Хакери часто сканують Інтернет з метою пошуку машин, що підтримують цей продукт. Багато користувачів використовують порожні паролі або паролі, які легко вгадати. Це надасть легкий доступ хакеру. Якщо хакер захопив контроль над машиною, він не тільки може украсти інформацію, але й використовувати цю машину для атаки інших ПК в Інтернеті. Випадкові сканування клієнтами PCAnywhere, звичайно, видні з боку сусідів. Програма інсталює іконку, названу "NETWORK", що сканує локальну область. Хоча ці скани не містять ворожих намірів, вони можуть створювати дискомфорт. Щоб перевірити, що насправді має місце, варто розглянути IP-адресу хакера. Якщо IP-адреса ставиться до локального сегмента (тобто подібний вашій IP-адресі), тоді це є нормальним. Інакше (адреса зовнішня) – має місце ВА ОС. PCanywhere сканує діапазон "класу С". Якщо ви не працюєте з PCAnywhere, тоді проблем немає. У такому випадку читайте поради щодо забезпечення безпеки сервера PCAnywhere.

SNMP Crack. Виявлено велику кількість рядків community (паролів), які ініціюють спробу розкрити систему контролю паролів. Велика кількість повідомлень SNMP з різними рядками community за обмежений період часу повинні розглядатися як підозріла активність і як спроба підібрати коректне значення поля community. SNMP використовується для моніторингу параметрів устаткування. Це небезпечний протокол, і ніщо не перешкоджає підбору пароля простим перебором. Варто конфігурувати ОС так, щоб вона була доступна з боку обмеженого кола машин. Рекомендується також використовувати максимально довгі рядки community, що дозволить зареєструвати підбір до того, як він успішно завершиться.

MS rpc dump. Хакер намагається сканувати вашу систему для визначення сервісів RPC/DCOM. Можливо, він шукає слабкі місця в системі доступу. Це спеціальна команда, що може бути послана до "RPC End-Point Mapper", що працює з портом 135. Ця атака не спрямована на вторгнення. Вона є частиною розвідувального етапу. Команда ’epdump’ попросить ОС перелічити всі працюючі сервіси. Хакер, одержавши ці дані, зможе ефективніше шукати слабкі місця. Якщо хакер знайде якісь із цих послуг, він спробує скористатися ними. Наприклад, існують шляхи, за

допомогою яких він може направити e-mail через Microsoft Exchange Servers. Шляхом виконання ’epdump’ він може з’ясувати, чи працює ОС як сервер. Якщо це так, він може потім змусити ОС переадресувати SPAM своїм "клієнтам". Поставте фільтр на порт 135 в firewall як для UDP, так і TCP.

SOCKS port probe. Сканування ОС для перевірки роботи SOCKS. Це означає, що хакер хоче влаштувати переадресацію трафіка через вашу ОС на якийсь інший мережний об’єкт. Це може бути також chat-сервер, що намагається визначити, чи не намагається хтось використовувати ОС для переадресації. SOCKS становить систему, що дозволяє декільком машинам працювати через загальне Інтернет-з’єднання. Багато додатків підтримують SOCKS. Типовим продуктом є WinGate, що легко інсталюється на ПК, який має реальне Інтернет-з’єднання. Усі інші машини в межах даної області підключаються до Інтернет через цей ПК. Проблема з SOCKS і продуктами типу WinGate полягає в тому, що вони не роблять розходження між відправником і одержувачем, що полегшує віддаленим машинам з Інтернет одержати доступ до внутрішніх ПК. Це може дозволити хакеру одержати доступ до інших машин через вашу ОС. При цьому він маскує своє правдиве положення в мережі. Атака проти "жертви" виглядає так, ніби вона була розпочата з боку вашої машини. Цей вид атаки на першому етапі виглядає як сканування. При використанні SOCKs систему варто конфігурувати так, щоб заблокувати сторонній доступ. Хакер розраховує на вашу помилку при конфігурації.

Netbus probe. Одержання доступу до вашого ПК за допомогою "NetBus Trojan Horse". Хакер шукає ПК, скомпрометований за допомогою цієї програми. Програма розсилається клієнтам з надією, що який-небудь користувач її запустить. Завдання такої програми – установити пароль, встановити вірус або переформатувати ваш диск. Популярну спеціальну групу утворюють "троянські коні", що забезпечують віддалений доступ до ПК. Такі програми хакер намагається надіслати поштою, через chat або новини, при цьому він може й не знати, де в Інтернеті знаходиться ваш ПК. Хакер знає тільки, хто є вашим провайдером, і змушений сканувати всіх його клієнтів.

IP-spoofing. **Спуфінгом** називається підміна адреси відправника в заголовку IP-пакета з метою пробити автентифікацію, засновану на визначенні IP-адреси джерела пакета. Незважаючи на те, що відповідний

пакет ніколи не повернеться до атакуючого, спуфинг є кращим другом хакера-злочинця й застосовується як складова безлічі інших атак.

SYN-flooding. Є різновидом атак типу denial-of-service (відмова від обслуговування). Здійснюється вона за допомогою створення напіввідчинених або недовідкритих (half-open) з'єднань. Їй підданий стек будь-який ОС або стек маршрутизатора, якщо він ще й надає який-небудь TCP-сервіс, наприклад, "echo". Розглянемо нормальний процес установлення з'єднання клієнта (ftp, http, telnet) із сервером:

починає клієнт із відправлення запиту SYN на встановлення з'єднання із сервером;

сервер підтверджує одержання запиту SYN-відправленням клієнтові повідомлення SYN-ACK;

клієнт завершує процес установлення з'єднання відправленням повідомлення ACK.

Таким чином, з'єднання відкрите і сервер може обмінюватися із клієнтом специфічними для конкретного додатка даними. Якщо сервер не одержав повідомлення ACK, то буде очікувати його протягом деякого часу (timeout), перш ніж закриє напіввідчинене з'єднання. До закриття сервер зберігає в пам'яті структуру даних, що описують очікуючи установки з'єднання. Ця структура згодом переповнюється, і сервер, у найкращому випадку, втрачає можливості відкривати нові з'єднання доти, доки список напіввідчинених з'єднань не очиститься. У найгіршому випадку сервер може вийти з ладу.

SMURF також ставиться до атак типу denial-of-service і працює на базі ICMP. Можливо, не кожен користувач ознайомлений з назвою цього протоколу, однак переважна більшість тих, хто працює із СКІ зіштовхувалися із програмою, яка реалізує одну з його функцій, – командою "PING". Ця необразлива програма призначена для визначення доступності якого-небудь хосту (віддаленого пристрою, що має IP-адресу) посилкою пакета ехо-запиту ICMP. Якщо отримано пакет з ехо-відповіддю, то хост уважається доступним. Однак пакет може бути відправлений не за адресою конкретного хосту, а за широкомовною (broadcast) адресою мережі. Широкомовна адреса становить адресу, в якій розряди, відведені під адресу хосту, дорівнюють одиниці. Наприклад, 10.255.255.255 – це широкомовна адреса для мережі 10.0.0.0. Якщо така мережа класу А розбита на 256 підмереж, то широкомовна адреса для підмережі 10.50.0.0 буде 10.50.255.255. Втім, мережна адреса, у якій розряди, відведені під

адресу хосту, дорівнюють нулю, теж може забезпечити широкомовне ехо. У цьому випадку пакет буде доставлений всім ПК у цій мережі. Очевидно, що якщо на широкомовний пакет дадуть відповідь кілька сотень або тисяч машин, то комп'ютер-ініціатор ехо-запиту m може не впоратися з обробкою ехо-відповідей.

Однак повернемося до підозрілих намірів злочинця. Вони посилають ICMP пакет, у якому адреса відправника є адресою "жертви" (спуфінг), а як одержувач вказується широкомовна адреса якого-небудь посередника. ПК посередника відповідають на отриманий ехо-запит посиланням пакетів за адресою відправника, тобто обраній злочинцем "жертві". Про подальші наслідки говорити важко: ПК може тимчасово виявитися не здатним працювати в мережі, може "зависнути", але можливе й порушення функціонування самої мережі через надмірний трафік.

Унеможливити атаку SMURF можуть маршрутизатори в мережі посередника. Якщо вони фільтрують широкомовний трафік, то сумління їхнього мережного адміністратора, який настроїв його, може бути чистим – комп'ютери в довіреній йому мережі не будуть посередниками в деструктивних діях зовнішнього зловмисника проти невідомої жертви. Однак ініціатор атаки може перебувати й усередині мережі. У цьому випадку маршрутизатори не допоможуть, і відповідальність за атаку буде покладена на хости, які також не повинні відповідати на ці пакети.

Віддалені атаки на хости Інтернет

Розглянемо наступні типи віддалених атак на хости Інтернет (рис. 7.6).

У мережі Інтернет основними базовими протоколами віддаленого доступа є TELNET і FTP (File Transfer Protocol).

TELNET – це протокол віртуального термінала (ВТ), що дозволяє з віддалених хостів підключатися до серверів Інтернет у режимі ВТ.

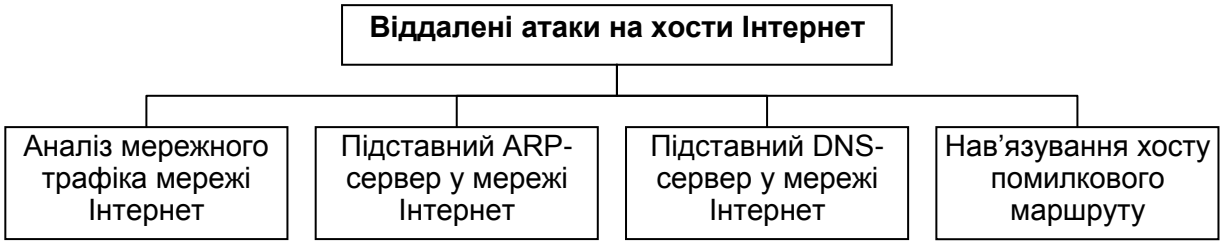


Рис. 7.6. **Класифікація віддалених атак на хости Інтернет** [62]

Аналіз мережного трафіка мережі Інтернет

FTP – протокол, призначений для передачі файлів між віддаленими хостами. Для одержання доступу до сервера за даними протоколами користувачеві необхідно пройти на ньому процедуру ідентифікації й автентифікації. Як інформація, що ідентифікує користувача, виступає його ідентифікатор (ім'я), а для автентифікації використовується пароль.

Особливістю протоколів FTP і TELNET є те, що паролі й ідентифікатори користувачів передаються мережею у відкритому, незашифрованому вигляді. Таким чином, необхідною й достатньою умовою для одержання віддаленого доступу до хостів за протоколами FTP і TELNET є ім'я і пароль користувача [63].

Одним зі способів одержання паролів і ідентифікаторів користувачів у мережі Інтернет є аналіз мережного трафіка. Мережний аналіз здійснюється за допомогою аналізатора пакетів, що перехоплює всі пакети, передані сегментом мережі, і виділяє серед них ті, у яких передаються ідентифікатор користувача і його пароль. Мережний аналіз протоколів FTP і TELNET показує, що TELNET розбиває пароль на символи й пересилає їх по одному, поміщаючи кожен символ з пароля у відповідний пакет, а FTP, навпаки, пересилає пароль цілком в одному пакеті (рис. 7.7).

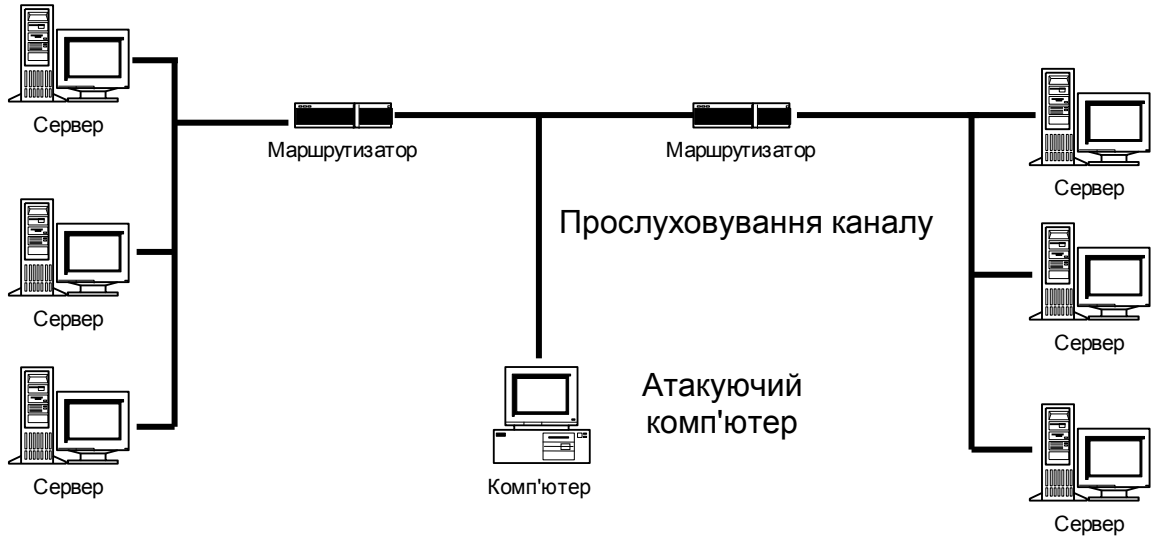


Рис. 7.7. **Аналіз мережного трафіка**

Аксіома. Рекомендується використовувати один із наступних методів запобігання аналізу мережного трафіка або сніфінга, але не забувайте при цьому про доцільність застосування того або іншого.

1. Користуйтеся активними інтелектуальними мережними пристроями (хабами, свічами, мостами, роутерами), які надсилають вузлам для призначення тільки ті пакети, які їм призначені.

2. Метод ефективний проти початківців хакерів, перешкоджає запуску, але не самій роботі. Працює на *nix подібних ОС – перекомпілюйте ядро ОС із підтримкою режиму BPF (Packet Filter support).

3. Будь-якими доступними ПЗ, наприклад, IPSec (вбудована підтримка), deslogin, swIPe, використовуйте шифрування трафіка, що перебуває за адресою: ftp.csua.berkeley.edu:/pub/cypherpunks/swIPe/.

4. Використання протоколу KERBEROS, що, незважаючи на всі відомі свої недоліки, забезпечує досить надійний захист з'єднання.

5. Використання реалізації протоколу SSH для сеансів з'єднань за протоколом TCP-з'єднань, наприклад, за допомогою програми F-secure-SSH на сайті фірми www.DataFellows.com.

Використання технології одноразових паролів за допомогою програми SYSKEY, хоча це й не дуже сильний захист [65].

Підставний ARP-сервер у мережі Інтернет

У загальному випадку переданий мережею пакет, незалежно від використовуваного протоколу й типу мережі (Token Ring, Ethernet, X.25 та ін.), складається із заголовка пакета й поля даних. У заголовок пакета зазвичай, заноситься службова інформація, обумовлена використовуваним протоколом обміну й необхідна для адресації пакета, його ідентифікації, перетворення й т. д. У полі даних містяться або безпосередньо дані, або інший пакет більш високого рівня OSI. Так, наприклад, пакет транспортного рівня може бути вкладений у пакет мережного рівня, що, у свою чергу, вкладений у пакет канального рівня. Спроектувавши це твердження на мережну ОС, що використовує протоколи TCP/IP, можна стверджувати, що пакет TCP (транспортний рівень) вкладений у пакет IP (мережний рівень), який, у свою чергу, вкладений у пакет Ethernet (канальний рівень).

Розглянемо схему адресації пакетів у мережі Інтернет і виникаючі при цьому проблеми ІБ. Як відомо, базовим мережним протоколом обміну в мережі Інтернет є протокол IP (Internet Protocol). Для адресації на мережному рівні (IP-рівні) у мережі Інтернет кожний хост має унікальний 32-розрядну IP-адресу. Для передачі IP-пакета на хост необхідно вказати в IP-заголовку пакета в поле Destination Address IP-адресу даного хосту.

Однак, як видно з рис. 7.8, IP-пакет перебуває усередині апаратного пакета (у випадку середовища передачі Ethernet IP-пакет перебуває усередині Ethernet-пакета), тому кожен пакет у мережах будь-якого типу й з будь-якими протоколами обміну адресується на апаратну адресу мережного адаптера, безпосередньо здійснюючий прийом і передачу пакетів у мережу.

Розглянемо узагальнену функціональну схему помилкового ARP-сервера (рис. 7.8 – 7.10): очікування ARP-запиту;

Рис. 7.8. **Підставний ARP-сервер. Фаза очікування ARP-запиту**

при одержанні ARP-запиту передача мережею помилкової ARP-відповіді на хост, що запросив, у якому вказується адреса мережного адаптера атакуючої станції (помилкового ARP-сервера) або та Ethernet-адреса, на яку буде приймати пакети помилковий ARP-сервер (зовсім не обов'язково вказувати в помилковій ARP-відповіді свою справжню Ethernet-адресу, тому що при роботі безпосередньо з мережним адаптером його можна запрограмувати на прийом пакетів на будь-яку Ethernet-адресу);

прийом, аналіз, вплив і передача пакетів обміну між взаємодіючими хостами.

Далі необхідно звернути увагу на те, що в маршрутизатора теж є ARP-таблиця, у якій утримується інформація про IP- і відповідні їм Ethernet-адреси всіх хостів із сегмента мережі, підключеного до маршрутизатора. Інформація в цю ARP-таблицю на маршрутизаторі також заноситься не вручну, а за допомогою протоколу ARP. Саме тому так легко в одному сегменті IP-мережі привласнити чужу IP-адресу: видати команду мережній ОС на установлення нової IP-адреси, потім звернутися в мережу – відразу ж буде надісланий широкомовний ARP-запит, і маршрутизатор, одержавши цей запит, автоматично обновить запис у своєї ARP-

таблиці (поставити відповідно до чужої IP-адреси Ehternet-адресу вашої мережної карти), у результаті чого власник даної IP-адреси втратить зв'язок із зовнішнім світом (всі пакети, які адресуються на його колишню IP-адресу й ті, які будуть приходити на маршрутизатор, направлятимуться атакуючим маршрутизатором на Ethernet-адресу). Однак деякі ОС аналізують всі передані мережею широкомовні ARP-запити.

Рис. 7.9. **Фаза атаки**

Тепер повернемося безпосередньо до описаної раніше схеми атаки "помилковий ARP-сервер" [63]. З аналізу механізмів адресації, описаних вище, стає зрозуміло, що пошуковий ARP-запит, крім атакуючого хоста, одержить і маршрутизатор, і в його таблиці з'явиться відповідний запис про IP- і Ethernet-адреси хоста, що атакується. Отже, коли на маршрутизатор прийде пакет, спрямований на IP-адресу хоста, що атакується, то він буде переданий не на помилковий ARP-сервер, а безпосередньо на хост. При цьому схема передачі пакетів у цьому випадку буде наступна:

атакований хост передає пакети на помилковий ARP-сервер;

помилковий ARP-сервер передає прийнятий від атакованого хоста пакет на маршрутизатор;

маршрутизатор, у випадку одержання відповіді на переданий запит, передає його безпосередньо на атакований хост, обминаючи помилковий ARP-сервер.

У цьому випадку остання фаза, пов'язана з "прийомом, аналізом, впливом і передачею пакетів обміну" між атакованим хостом і, наприклад, маршрутизатором, буде проходити вже не в режимі повного перехоплення пакетів помилковим сервером (мостова схема), а в режимі "напівперехоплення" (петльова схема). Дійсно, у режимі повного перехоплення маршрут всіх пакетів, що відправляються як в одну, так і в іншу

сторони, обов’язково проходить через помилковий сервер-міст; а в режимі "напівперехоплення" маршрут пакетів утворить петлю, яку можна побачити на рис. 7.10.

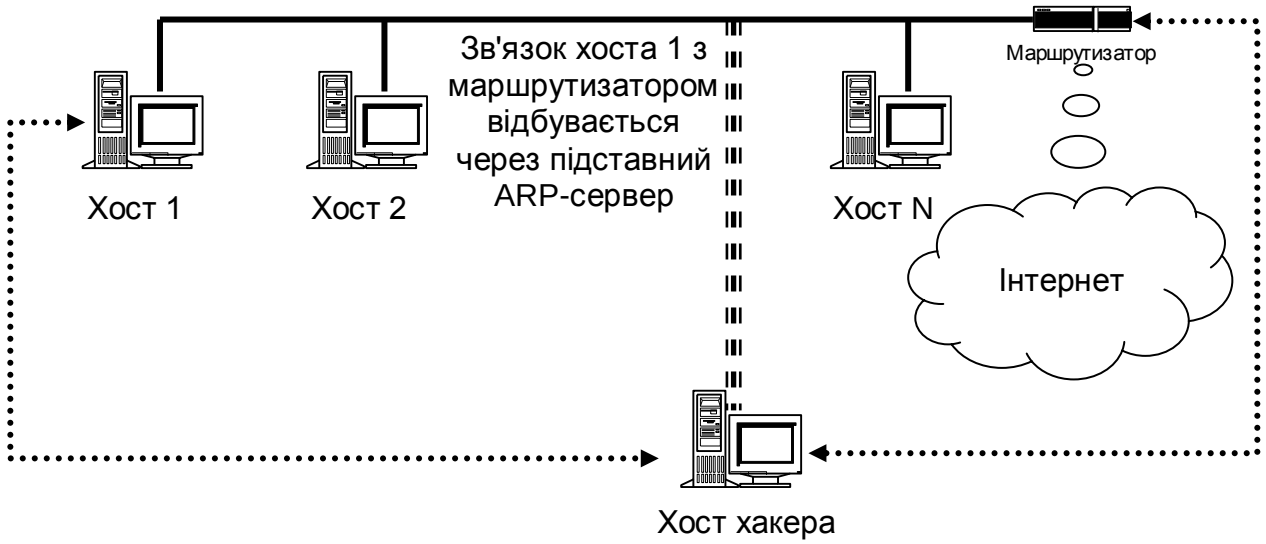


Рис. 7.10. **Фаза прийому, аналізу, дії та передачі перехопленої інформації на підставному ARP-сервері**

Досить нескладно придумати декілька способів, що дозволяють функціонувати помилковому ARP-серверу за мостовою схемою перехоплення (повне перехоплення). Наприклад, можна, одержавши ARP-запит, самому послати такий же запит і привласнити собі дану IP-адресу (однак у цьому випадку помилковому ARP-серверу не вдасться залишитися непоміченим, то деякі мережні ОС, перехопивши цей запит, видадуть попередження про використання їх IP-адреси). Інший, значно кращий спосіб: надіслати ARP-запит, зазначивши як свою IP-адресу будь-яку вільну у даному сегменті IP-адресу, і надалі сповісти про роботу з даної IP-адреси як з маршрутизатором, так і з "обманутими" хостами (до речі, це типова proxy-схема).

Підставний DNS-сервер у мережі Інтернет

Для звертання до хостів у мережі Інтернет використовуються IP-адреси, що унікально ідентифікують кожен мережний комп’ютер у мережі. Однак для користувачів застосування IP-адрес при звертанні до хостів є не занадто зручним і далеко не найнаочнішим.

На початку зародження мережі Інтернет для зручності користувачів було ухвалено рішення надати всім комп’ютерам у мережі імена. Вико-

ристання імен дозволяє користувачеві краще орієнтуватися в кіберпросторі мережі Інтернет – для користувача легше запам'ятати, наприклад, ім'я **www.ferrari.it**, ніж ланцюжок IP-адреси. Використання в Інтернет зрозумілих мнемонічних імен призвело до виникнення проблеми перетворення імен в IP-адреси. На етапі раннього розвитку Інтернет, коли в мережу була об'єднана невелика кількість комп'ютерів, **NIC (Network Information Center)**, для вирішення проблеми перетворення імен в адреси було створено спеціальний файл (hosts file), у який вносилися імена й відповідні їм IP-адреси всіх хостів у мережі. Даний файл регулярно обновлявся й поширювався по всій мережі. Але, у міру розвитку Інтернету, число об'єд-наних у мережу хостів збільшувалося, і дана схема ставала усе менш працездатною. Тому була створена нова система перетворення імен, що дозволяє користувачеві у випадку відсутності в нього інформації про відповідність імен і IP-адрес одержати необхідні відомості від найближчого інформаційно-пошукового сервера (ІПС). Ця система одержала назву доменної системи імен – **DNS (Domain Name System)**.

З метою реалізації DNS був створений спеціальний мережний протокол DNS, для забезпечення ефективної роботи якого в мережі створюються спеціальні виділені DNS-сервери..

1. Упровадження у мережу Інтернет помилкового DNS-сервера шляхом перехоплення DNS-запиту.

У цьому випадку це ВА на базі стандартної типової ВА, пов'язаної з очікуванням пошукового DNS-запиту.

По-перше, за замовчуванням служба DNS функціонує на базі протоколу UDP (хоча можливе й використання протоколу TCP), що природно, робить її менш захищеною, тому що протокол UDP на відміну від TCP взагалі не передбачає засобів ідентифікації повідомлень. Для того, щоб перейти від UDP до TCP, адміністраторові DNS-сервера необхідно дуже серйозно вивчити документацію. І тільки в тому випадку, якщо їй прийде спеціальна відповідь від DNS-сервера, мережна ОС відішле DNS-запит з використанням TCP.

По-друге, значення поля "порт відправника" в UDP-пакеті спочатку приймає значення 1023 і збільшується з кожним переданим DNS-запитом.

По-третє, значення ідентифікатора (ID) DNS-запиту залежить від конкретного мережного додатка, що виробляє DNS-запит. Експерименти показали, що у випадку передачі запиту з оболонки командного інтерпретатора (SHELL) ОС Linux і Windows це значення завжди дорівнює

одиниці. Якщо запит передається безпосередньо DNS-сервером, то сервер збільшує це значення ідентифікатора на одиницю з кожним знову переданим запитом.

Для реалізації атаки шляхом перехоплення DNS-запиту атакуючому необхідно перехопити DNS-запит, вилучити з нього номер UDP-порту відправника запиту, двобайтове значення ідентифікатора DNS-запиту та шукане ім'я й потім відіслати помилковий DNS-відповідь на вилучений із DNS-запиту UDP-порт, у якому вказати як шукану IP-адресу справжню IP-адресу помилкового DNS-сервера. Це дозволить надалі повністю перехопити трафік між хостом, що атакується і сервером та активно впливати на нього. Розглянемо узагальнену схему роботи помилкового DNS-сервера (рис. 7.11 – 7.13):

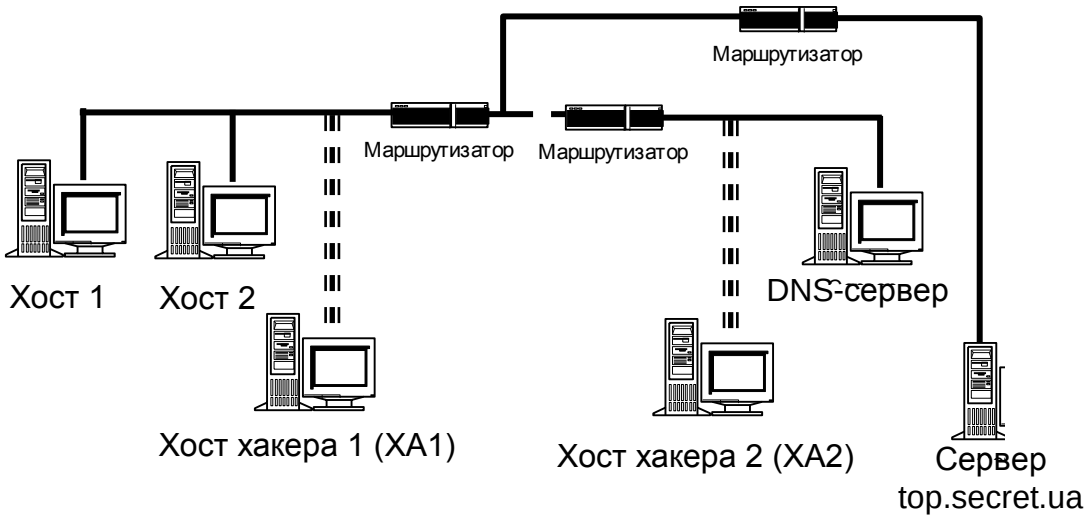


Рис. 7.11. **Функціональна схема підставного DNS-сервера. Фаза очікування хакером DNS-запиту (він знаходиться на ХА1 або на ХА2)**

очікування DNS-запиту;

добування з отриманого запиту необхідних відомостей і передача мережею, на що запросив хост, помилкові DNS-відповіді, від імені (з IP-адреси) сьогодення DNS-сервера, у якому вказується IP-адреса помилкового DNS-сервера;

у випадку одержання пакета від хоста, зміна в IP-заголовку пакета його IP-адреси на IP-адресу помилкового DNS-сервера й передача пакета на сервер (помилковий DNS-сервер веде роботу із сервером від свого імені);

у випадку одержання пакета від сервера, зміна в IP-заголовку пакета його IP-адреси на IP-адресу помилкового DNS-сервера й передача пакета на хост (для хоста помилковий DNS-сервер і є справжній сервер).

Необхідною умовою здійснення ВА є перехоплення DNS-запиту. Це можливо тільки у випадку, якщо атакуючий перебуває або на шляху основного трафіка, або в сегменті сьогодення DNS-сервера. Виконання однієї із цих умов робить подібну ВА важко здійсненною на практиці (потрапити в сегмент DNS-сервера й тим більше в міжсегментний канал зв'язку атакуючому, швидше за все, не вдасться). Однак у випадку виконання цих умов, можливо здійснити ***міжсегментну*** ВА на мережу Інтернет [64].

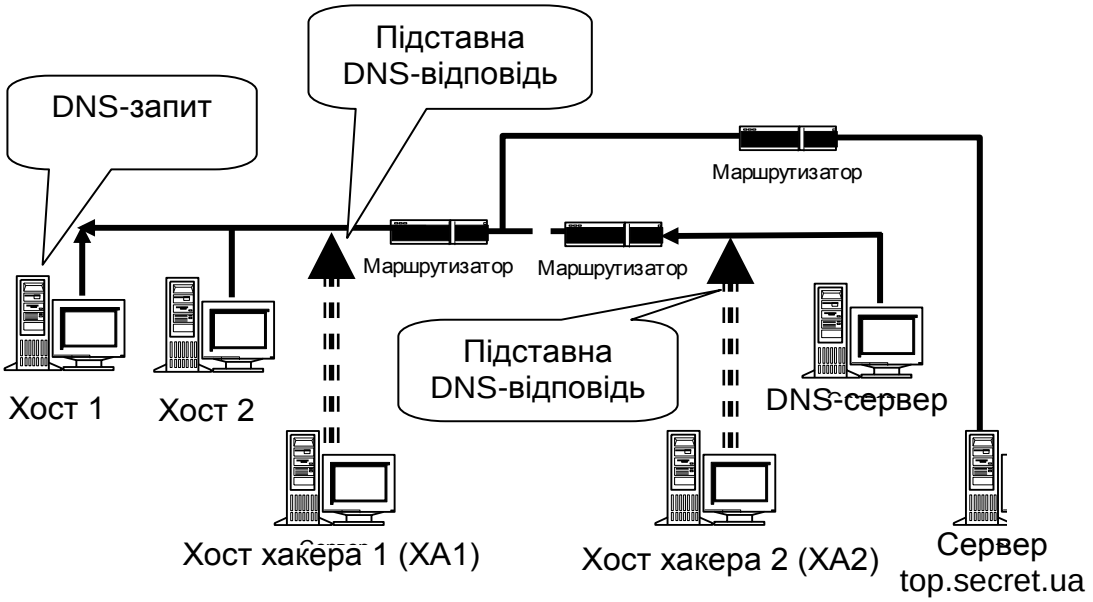


Рис. 7.12. **Фаза передачі атакуючим підставної відповіді DNS-сервера**

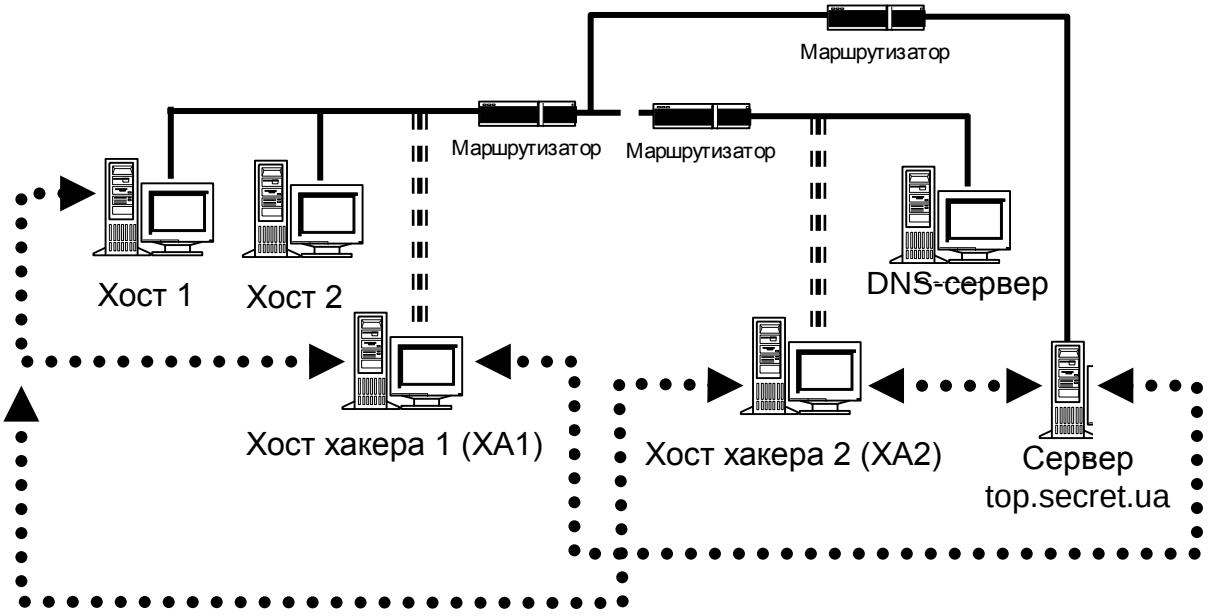


Рис. 7.13. **Фаза прийому, аналізу, дії та передачі перехопленої інформації на підставному сервері**

Аксіома. У випадку, коли FTP-клієнт на хості підключався до віддаленого FTP-сервера через помилковий DNS-сервер, виявлялося, що щоразу після видачі користувачем прикладної команди FTP (наприклад, ls, get, put і т. д.) FTP-клієнт здійснював команду PORT, що полягала в передачі на FTP-сервер у поле даних TCP-пакета номера порту й IP-адреси клієнтського хоста (особливий зміст у цих діях важко знайти – навіщо щоразу передавати на FTP-сервер IP-адресу клієнта).

Це приводило до того, що, якщо на помилковому DNS-сервері не змінити передану IP-адресу в поле даних TCP-пакета й передати цей пакет на FTP-сервер за звичайною схемою, то наступний пакет буде переданий FTP-сервером на хост FTP-клієнта, обминаючи помилковий DNS-сервер, і, що найцікавіше, цей пакет буде сприйнятий як нормальний пакет, і надалі помилковий DNS-сервер втратить контроль над трафіком між FTP-сервером і FTP-клієнтом. Це пов’язано з тим, що звичайний FTP-сервер не передбачає жодної додаткової ідентифікації FTP-клієнта, а перекладає всі проблеми ідентифікації пакетів і з’єднання на більш низький рівень – рівень TCP (транспортний).

Комп’ютерні віруси

Комп’ютерний вірус – це спеціально написана невелика (як правило) за розмірами програма, що виконує різні небажані (частіше шкідливі) дії на ПК і може "приписувати" себе до інших програм, тим самим "заражаючи" їх [65]. Все це відбувається у невидимому для користувача й системи (якщо вона функціонує без установленого антивірусного ПЗ) режиму [94]. Програма, усередині якої перебуває вірус, називається **"зараженою"**. Коли така програма починає роботу, то спочатку, як правило, керування одержує вірус. Сам термін "вірус" запропонував Фред Кохен в 1983 році, коли був студентом в одному з університетів США [65].

Німецька фірма AV-Test, що спеціалізується на СІБ (http://www.av-test.org), яка допомагала в дослідженнях, стверджує, що щодня виявляється від 70 до 100 нових злочинців.

Вірус знаходить і "заражає" інші програми або здійснює які-небудь шкідливі впливи: псує файли або таблицю розміщення файлів на диску (FAT), "засмічує" оперативну пам’ять ПК, змінює адресацію звертань до зовнішніх пристроїв і т. д. Більше того, заражені програми можуть бути перенесені на інший комп’ютер за допомогою фізичних носіїв або комп’ютерної мережі.

Порада. *З вірусами треба "дружити", їх треба розуміти, особливо – як вони працюють і що вони можуть зробити поганого для вас.*

У цей час відомо більше 500 тис. вірусів і більше 5 млн їх **штамів** – похідних програмних продуктів від самих вірусів з невеликими змінами в декількох функціях [63]. Умовно їх можливо класифікувати (рис. 7.14), але на сьогодні не існує єдиної загальноприйнятої класифікації вірусів.

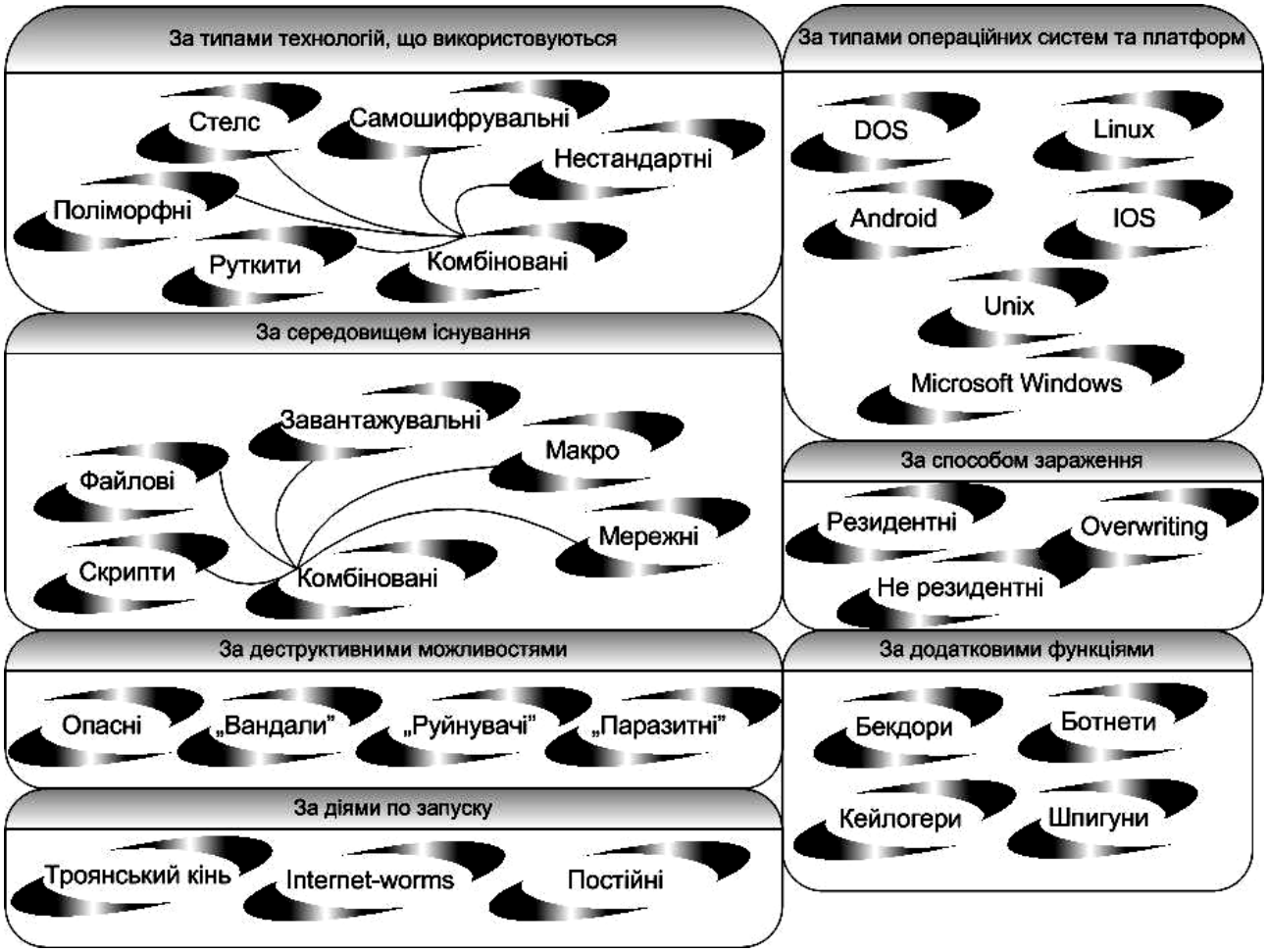


Рис. 7.14. **Можлива класифікація вірусів** [65]

Ця класифікація поєднує, природно, далеко не всі можливі типи вірусів; у кожній категорії зустрічаються варіанти, не названі через їх екзотичність, наприклад, CMOS-віруси, FLASH-віруси або вірусоподібні структури (макровіруси), "які мешкають" у середовищі Microsoft Word.

Крім того, зустрічається ряд програм, що не володіють всіма властивостями вірусів, але здатних становити серйозну небезпеку (наприклад, "троянські коні" або програми типу spyware).

Для захисту й боротьби з вірусами застосовуються спеціальні антивірусні програми, які можна розділити на кілька видів [62]:

програми-детектори, що дозволяють виявити файли, заражені вірусом. Робота детектора ґрунтується на пошуку ділянки коду (називається **сигнатура**), що належить тому або іншому відомому вірусу. На жаль, детектори не гарантують виявлення "свіжих" вірусів, хоча в деяких з них для цього передбачені особливі засоби. Найбільш відомими детекторами є Dr. Web, Norton Antivirus, AVP. Крім того, самі сигнатури, відомі раніше, можуть бути пізніше видозмінені в ході життєдіяльності вірусу, що природно, і зводить до нуля ймовірність його виявлення;

програми-доктори (або фаги), які "лікують" заражені програми або диски, знищуючи тіло вірусу. При цьому в ряді випадків ваша інформація може бути загублена, тому що деякі віруси настільки спотворюють середовище перебування, що її вихідний стан не може бути відновлено. Широко відомими програмами-докторами є AVP, Dr. Web, Norton Antivirus;

програми-ревізори, вони спочатку запам'ятовують відомості про стан програм і системних областей дисків, а надалі порівнюють їхній стан з вихідним. При виявленні невідповідностей видають повідомлення користувачеві. Робота цих програм заснована на перевірці цілісності (незмінності) файлів шляхом підрахунку контрольної суми і її порівняння з еталонною, обчисленою при першому запуску ревізора; можливо також використання контрольних сум, що включаються до складу програмних файлів виготовлювачами. Можуть бути створені й зустрічаються віруси, що не змінюють при зараженні контрольної суми, розрахованої традиційним чином – підсумовуванням всіх байтів файла, однак практично неможливо замаскувати модифікацію файла, якщо підрахунок ведеться за довільною, заздалегідь невідомою схемою (наприклад, парні байти додатково множаться на 2), і зовсім малоймовірно, що розраховане значення збіжиться при використанні двох або більше контрольних сум. До широко розповсюджених програм-ревізорам ставляться AVP, Norton Antivirus;

доктори-ревізори – це програми, що поєднують властивості ревізорів і фагів, які здатні виявити зміни у файлах і системних областях дисків і за необхідності (у випадку патологічних змін) можуть автоматично повернути файл у вихідний стан. До широко розповсюджених докторів-ревізорам ставляться AVP, Panda, Norton Antivirus, NOD32, PC Cillin;

програми-фільтри, які розташовуються резидентно в оперативній пам'яті комп'ютера, перехоплюють ті звертання до ОС, які можуть використовуватися вірусами для розмноження й нанесення шкоди, і повідом-

ляють про їх користувачеві. Програми-фільтри контролюють дії, характерні для поводження вірусу, такі, як:

відновлення програмних файлів;

запис на жорсткий диск за фізичною адресою (прямий запис);

форматування диска;

резидентне розміщення програм в оперативній пам'яті.

Виявивши спробу здійснення однієї із цих дій, програма-фільтр видає опис ситуації й жадає від користувача підтвердження. Користувач може дозволити операцію, якщо її робить "корисна" програма, або скасувати, якщо джерело даної дії не зрозуміле. До широко розповсюджених програм-фільтрів ставляться Spider, AVP, Norton Antivirus. Це досить надійний метод захисту, але який створює істотні незручності для користувача.

Деякі антивірусні функції вбудовані в сучасні версії BIOS, але, як правило, ними ніхто не користується.

Антивірусні програмні продукти, що випускаються, а їх дуже багато, поєднують основні функції детектора-доктора-ревізора.

Слід зазначити, що антивірусні програми постійно обновляються, у середньому не рідше одного разу на місяць, і здатні захистити комп'ютери від вірусів, відомих програмі на даний момент. І, крім того, за рахунок використання евристичних аналізаторів дані програми здатні виявити частину невідомих вірусів.

Насамперед, необхідно підкреслити, що **захистити ПК від вірусів може тільки сам користувач.** Тільки правильне й своєчасне застосування антивірусних засобів може гарантувати його від зараження або забезпечити мінімальний збиток. Необхідно правильно організовувати роботу на ПК і уникати безконтрольного перепису програм з інших комп'ютерів, у першу чергу це стосується розважальних програм і комп'ютерних ігор.

Наприклад, вірус Морріса – класичний приклад мережного вірусу. 2 листопада 1988 року Роберт Морріс-молодший, аспірант факультету інформатики Корнельского університету, за допомогою написаного ним вірусу інфікував велику кількість комп'ютерів, підключених до мережі Інтернет. Вірус Морріса вражав тільки комп'ютери типу SUN 3 і VAX, які використовували варіанти ОС UNIX версії 4 BSD.

Для свого поширення вірус використовував деякі дефекти стандартної ОС UNIX, установленої на багатьох системах. Він також використовував механізм, призначений для доступу до віддалених комп'ютерів у локальних мережах.

Вірус складався із двох частин: головної програми й програми, що забезпечує його поширення. Головна програма після запуску на черговій машині збирала інформацію щодо інших машин у мережі, з якими вона має зв'язок. Вона виконувала цю роботу за допомогою аналізу конфігураційних файлів і шляхом запуску системної утиліти, що подає інформацію про поточний стан з'єднань у мережі. Потім вироблялося пересилання програми поширення на знайдені машини, запускалася й забезпечувала пересилання й компіляцію іншої частини вірусу. Потім весь процес повторювався [62].

Найбільш помітним ефектом при поширенні вірусу було все-таки те, що безупинно зростало завантаження уражених вірусом машин. Після закінчення деякого часу ряд машин виявився настільки завантаженим поширенням копій вірусу, що не був здатний виконувати ніякої корисної роботи; деякі машини вичерпували пам'ять для свопінга або таблицю поточних процесів, і їх доводилося перевантажувати.

8. Канали витоку інформації

8.1. Класифікація каналів витоку інформації

Уся інформація, що підлягає захисту, у силу свого динамізму міняється згодом, а також міняє своє місце розміщення. Внаслідок чого завжди виникає процес її переміщення (передачі, копіювання) від джерела до одержувача. Отже, при переміщенні інформації в середовищі інформаційної системи використовуються різні канали передачі. Якщо ці або інші канали передачі інформації використовуються для НСД, перехоплення й інших видів незаконних дій, то ці канали передачі інформації (КПІ) називаються **каналами витоку інформації (КВІ)**. Таким чином, утвориться перехідний процес, представлений на рис. 8.1.

Рис. 8.1 показує також можливість виникнення зворотного переходу, від КВІ до КПІ, внаслідок припинення використання КПІ в зловмисних цілях.

Крім того, всі ці перехідні процеси виникають у часі, при досягненні деякого "критичного" значення. Наприклад [61],

t_i – час початку використання КПІ за своїм призначенню при його активації;

$\{t_i; t_{i+1}\}$ – період часу нормального функціонування КПІ в споконвічно призначених цілях використання;

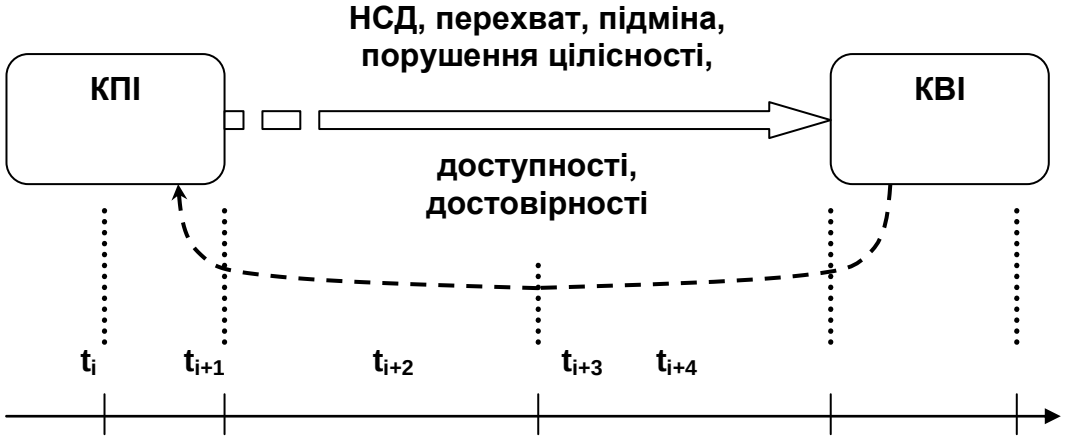


Рис. 8.1. **Динамізм перехідних процесів КПІ→КВІ** [63]

t_{i+1} – час, при якому ймовірність виникнення інциденту (погрози, уразливості) у системі ІБ $p_i > 0$;

$\{t_{i+1}; t_{i+2}\}$ – період часу, протягом якого інцидент проявляється (не візуально) на повну силу і його протікання починає впливати на функціонування організації (підприємства);

t_{i+2} – час, при якому наступає переломний момент у процесі протікання інциденту, його виявляють, локалізують, формують комплекс заходів щодо усунення;

$\{t_{i+2}; t_{i+3}\}$ – період часу, протягом якого дія інциденту слабшає, внаслідок використання контрзаходів, функціонування організації (підприємства) відновлюється на нормальному рівні, керівництво "приходить у себе", проводиться аналіз нанесеного збитку;

t_{i+3} – час, при якому готовий звіт про нанесений збиток, підрахований грошовий еквівалент, сформовані планові заходи щодо подальшого запобігання, проведений аналіз можливості виникнення інциденту;

$\{t_{i+3}; t_{i+4}\}$ – період часу, протягом якого реалізуються планові заходи щодо подальшого запобігання, виявлене джерело інциденту, якщо це суб'єкт (людина), то формується механізм повернення втрат (позов у суд), якщо це об'єкт, то оцінюється необхідність його існування;

t_{i+4} – час, при якому організація (підприємство) вертається в русло нормального функціонування, відновлюються втрачені зв'язки, домовленості, можливо організація (підприємство) переходить на новий рівень розвитку.

Різні періоди й тимчасові звіти можуть, при цьому, мати різну тривалість. Причому вона буде мати пряму залежність від виникаючих і супровідних обставин (а вони, як відомо, бувають різні), тому говорити про уніфікованість динамізму процесів не має змісту.

Класифікаторів КВІ розроблено досить багато, вводити новий – особливого сенсу немає, тому наведемо як приклад класифікатор, побудований з використанням джерела [79] і представлений у табл. 8.1.

Таблиця 8.1

Класифікатор КВІ

Класифікаційна ознака	Приклад КВІ
Форма проявлення інформації	Засоби контролю акустичної (мовної) інформації
	Засоби контролю аналого-цифрової сигнальної інформації
	Засоби контролю об'ємно-видової сигнальної інформації
Технологія використання	Внесені й швидко встановлювані спеціальні пристрої
	Заздалегідь установлювані заставні пристрої
	Засоби дистанційного контролю
Схеми й способи використання енергії	Активні (випромінюючі) пристрої
	Пасивні (перевипромінюючі) пристрої
	Природні КВІ
Тип КВІ	Оптичний (візуальний)
	Провідний
	Бездротовий (радіо)
	що візуально контролюється (спостереження)
	Акустичний (звуковий)
	Електромагнітний
	Матеріально-речовинний

Для продовження аналізу отриманих даних досліджень наведемо порядок розрахунку важливості каналів витоку інформації з метою визначення рекомендацій щодо виділення коштів та відповідних засобів для усунення каналів витоку інформації або зменшення втрат від витоків інформації з обмеженим доступом.

З прикладу типової організаційно-функціональної схеми (рис. 8.2) умовно виділимо на підприємстві декілька відділів [76]. Тоді після виявлення типів (видів) інформації з обмеженим доступом та документів, можна одержати необхідні дані за визначений період (табл. 8.2).

У якості одержуваних даних використовуються частоти появи того або іншого типу (виду) інформації з обмеженим доступом, що розраховуються як відношення певних типів інформації (у вигляді файлів) до загальної кількості інформації (у вигляді файлів).

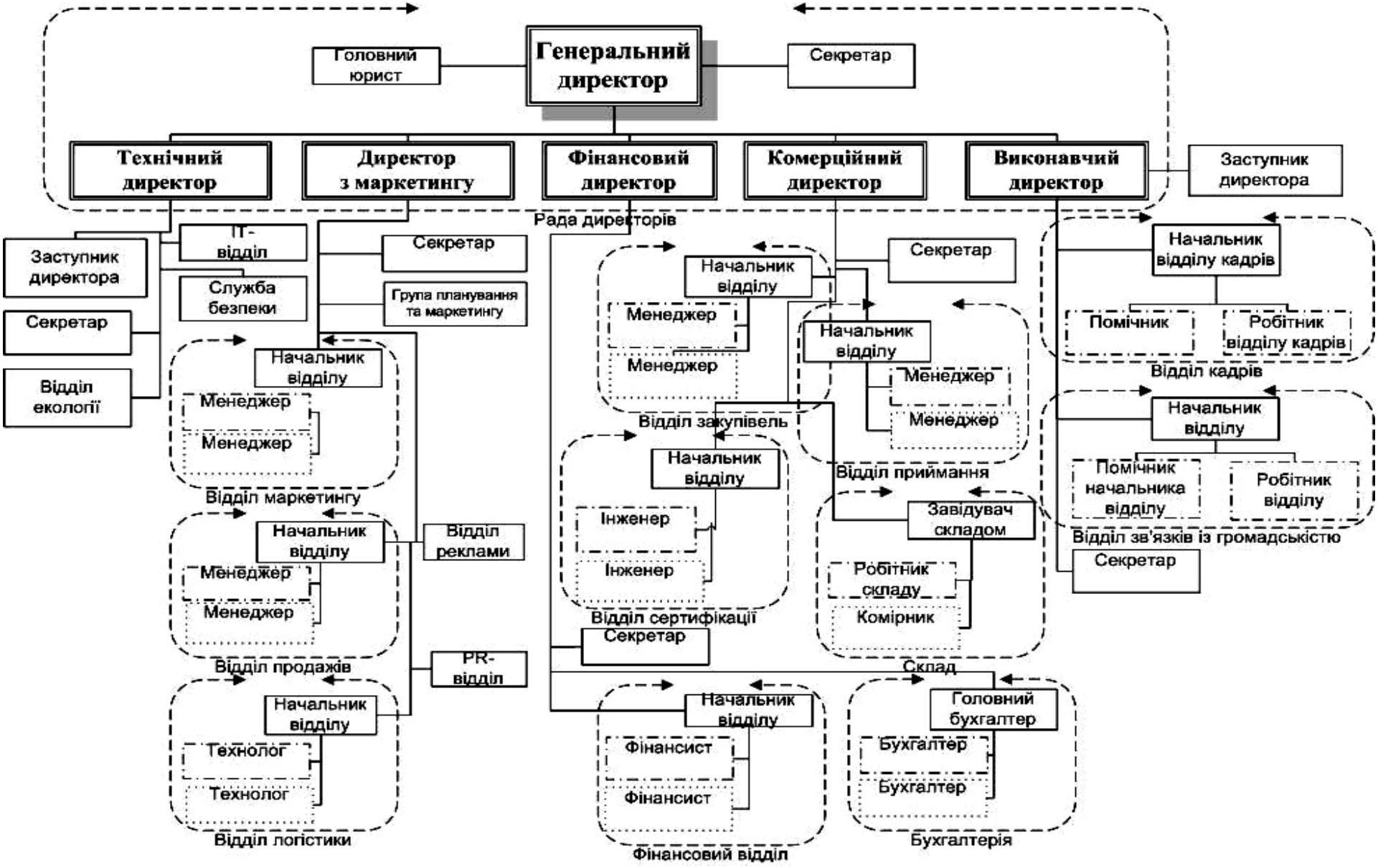


Рис. 8.2. **Типова організаційно-функціональна схема**

Таблиця 8.2

Статистичні дані витоків ІОД на підприємстві (частота)

Показник / Відділ	$n_i = 1$ (ДСП)	$n_i = 2$ (держ. таємниця)	$n_i = 3$ (комерційна інформація)	$n_i = 4$ (персональні дані)	$n_i = 5$ (таємниця суду)
Фінансовий	0,2	0	0,41	0,2	0,01
…	…	…	…	…	…
Сертифікації	0,04	0	0,36	0,33	0

Тобто [73]

$$n_i = \frac{N_i}{\sum_{i=1}^{k} N_i}, \qquad (8.1)$$

де n_i – частота появи і-го типу (виду) ІОД (наприклад, ПДн, таємниця наслідку, державна таємниця, комерційна інформація та ін.);

N_i – загальна кількість і-го типу (виду) ІОД, знайденого у вигляді файлів;

k – загальна кількість файлів у системі.

Крім того, на підприємстві у рамках синтезу СІБ пропонується ввести критерії (після узгодження з керівництвом) для визначення відповідних рекомендацій [72]:

1. Якщо $0 < n_i < 0,25$, то вводиться усна вказівка щодо використання та правил роботи відносно і-го типу (виду) інформації з обмеженим доступом.

2. Якщо $0,26 < n_i < 0,45$, то вводиться доповнення у вигляді окремих параграфів щодо використання та правил роботи відносно і-го типу (виду) інформації з обмеженим доступом.

3. Якщо $0,46 < n_i < 0,75$, то вводиться окрема інструкція щодо використання та правил роботи відносно і-го типу (виду) інформації з обмеженим доступом.

4. Якщо $0,76 < n_i < 0,99$, то вводиться зміна в устав організації щодо використання та правил роботи відносно і-го типу (виду) інформації з обмеженим доступом.

Крім того, якщо досить більші значення частот спостерігаються у різних відділах, то можна провести групування (кластерізацію), за результатами якого цілком може бути рекомендація скорочення кількості персоналу в тій або іншій категорії. Наприклад, один інженер може пра-

цювати з однієї й тією інформацією в різних відділах, отже, немає необхідності тримати двох інженерів.

Крім того, загальна кількість типів КВІ на підприємстві [56; 57] залежіть від різних факторів, а з урахуванням існуючих технологій вона складе таку чисельність (табл. 8.3).

Таблиця 8.3

Чисельність каналів витоку інформації

Тип пристрою	№ п/п	Тип каналу витоку інформації
ПК і сервер	1	електронна пошта
	2	FTP-сервіс
	3	HTTP-сервіс
	4	P2 P-сервіс
	5	CHAT-сервіс
	6	ICQ-сервіс
	7	IRC-сервіс
	8	Wi-Fi-канал
	9	IrDA-канал
	10	Bluetooth-канал
	11	WWW-сервіс
	12	USB-Інтерфейс
	13	COM-Інтерфейс
	14	Cardreader-канал
	15	Skype-сервіс
	16	SCSI-інтерфейс
	17	LPT-інтерфейс
	18	FDD-інтерфейс
	19	HDD-інтерфейс
	20	simple copying (просте копіювання по мережі з використанням множини $\{K_{NE}\}$)
стільникові телефони та їм подібні пристрої	1	Wi-Fi-канал
	2	IrDA-канал
	3	ICQ-сервіс
	4	CHAT-сервіс
	5	Skype-сервіс
	6	EMS-сервіс
	7	WWW-сервіс
	8	FTP-канал
	9	P2P-сервіс
	10	WAP-сервіс
	11	MMS-сервіс
	12	SMS-сервіс
	13	IRC-сервіс
	14	USB-канал
	15	HTTP-сервіс
	16	Bluetooth-канал
	17	електронна пошта

Існує також можливість (рис. 8.2) виникнення зворотного переходу, від каналів витоку інформації до каналів передачі інформації внаслідок припинення використання каналів передачі інформації у зловмисних цілях, тобто КПІ → КВІ → КПІ.

Тоді при використанні введеного класифікатора кількість каналів витоку інформації буде визначатися за формулою [70]:

$$K_{CTI} = \lceil (20 + K_{NE}) \times (K_{PC} + K_S) + 17 \times K_{CE} + 2 \times (K_F + K_T) \rceil, \qquad (8.2)$$

де K_{CTI} – кількість трактів (каналів) передачі інформації (channel of transfer information, CTI), що утворюють канали витоку інформації;

K_T – кількість стаціонарних телефонів (telephones, T);

K_F – кількість стаціонарних факсів (faxes, F), причому факс має два канали витоку інформації: акустичний та передачі даних;

K_{NE} – кількість одиниць мережного устаткування (network equipment, NE), що беруть участь у забезпеченні функціонування робочих станцій і серверів, за умови, що кількість портів для підключення мережного устаткування Z = 5, 8, 12, 16, 32, 64, залежно від фірми виробника й технічних характеристик мережного устаткування, то:

$$K_{NE} = \lceil (K_{PC} + K_S)/Z \rceil,$$

де K_{PC} – кількість робочих станцій (workstations, personal computers, PC), що беруть участь у забезпеченні функціонування СЕБП, якщо припустити, що в середньому 85 % [57] співробітників (*M*) на сучасному підприємстві мають на робочому місці комп'ютери, а також з обліком того, що $V_{ST} = \{V_{VCO}\} \cup \{V_{VSSF}\} \cup \{V_{AR}\}$, то:

$$K_{PC} = \lceil 0{,}85 \times M \rceil.$$

K_S – кількість серверів (servers, S), що беруть участь у забезпеченні функціонування СЕБП, якщо припустити, що в середньому на 20-25 робочих станцій доводиться один сервер, то:

$$K_S = \lfloor K_{PC} / 25 \rfloor.$$

K_{CE} – кількість комунікаційного устаткування (communication equipment, CE), що беруть участь у забезпеченні діяльності співробітників підприємства (КПК, стільникові телефони, комунікатори, смартфони, netbook, miniPC), тому у найпростішому випадку K_{NE} дорівнює кількості співробітників (*M*), однак з обліком того, що кожний 5-й співробітник має кілька подібних пристроїв [2], то:

$$K_{CE} = 0{,}2 \times M + M = \lceil 1{,}2 \times M \rceil.$$

Таким чином, на основі отриманих даних можна оцінити необхідність введення спеціальних заходів та виділення коштів для запобігання використання та усунення каналів витоку інформації.

Канали втрати конфіденційної інформації

Утрата інформації припускає незаконний перехід конфіденційних відомостей до особи, не має права використовувати ці відомості з власною метою для одержання прибутку або передачі іншій особі.

У тому випадку, коли втрата інформації відбувається з вини персоналу – втрата інформації позначається терміном розголошення або розголос інформації.

Розголошення інформації завжди здійснюється людиною усно, письмово, за допомогою жестів, міміки, умовних сигналів.

Термін "витік інформації" більшою мірою стосується втрати ІОД за рахунок її перехоплення за допомогою технічних засобів розвідки. Втрата інформації можлива за наявності каналів розголошення або витоку.

Канал втрати інформації означає перехід цінних відомостей від закінченого джерела, по-перше або безпосередньо, до конкурента або зловмисника, по-друге, до третьої особи в несанкціонованому режимі.

Під третьою особою розуміються будь-які особи, які одержали знання конфіденційної інформації через обставини або в результаті безвідповідальності персоналу варто враховувати, що ці особи не зацікавлені в отриманій інформації.

Перехід інформації до третьої особи утворить випадковий або стихійний канал втрати інформації у результаті:

1) втрати документів або конфіденційних записів;

2) незнання або ігнорування персоналу фірми вимог щодо захисту інформації;

3) зайва балакучість співробітників з колегами по роботі, іншими особами в місцях загального користування, у транспорті й т. д.;

4) роботи з конфіденційними документами при сторонніх особах за рахунок несанкціонованої передачі їх іншому співробітникові;

5) у результаті наявності в документах зайвої конфіденційної інформації;

6) у результаті самовільного копіювання співробітником документів зі службовою або колекційною метою.

На відміну від третьої особи зловмисник цілеспрямовано намагається одержати конкретну інформацію й тому навмисно і таємно знаходить або формує канал розголошення або витоку інформації.

КВІ діляться на організаційні й технічні [158].

Організаційні канали розголошення інформації, заснованої на встановленні різноманітних, у тому числі законних взаєминах з фірмою або співробітником фірми для наступного несанкціонованого доступу до інформації, що цікавить зловмисника. Основними видами організаційних каналів можуть бути:

влаштування зловмисника на роботу у фірму, як правило, на технічну, допоміжну або другорядну посаду;

установлення зловмисником довірчих взаємин зі співробітником фірми або особами, що мають право вільного доступу в даній фірмі;

кримінальний, силовий доступ до інформації, тобто крадіжка документів, справ, дискет, дисків, комп'ютерів, шантаж до співробітництва окремих працівників, підкуп працівників, інсценування екстремальних ситуацій;

одержання інформації з випадкового каналу.

Витік конфіденційної інформації – це безконтрольний вихід конфіденційної інформації за межі СКІ або кола осіб, яким вона була довірена по службі, відома в процесі роботи. Цей витік може бути наслідком;

розголошення конфіденційної інформації;

відходу інформації з різним, головним чином технічним каналам;

несанкціонованого доступу до ІОД різними способами.

Розголошення інформації її власником або іншими власником є навмисні або необережні дії посадових осіб і користувачів, яким відповідні відомості у встановленому порядку були довірені по службі або по роботі, що призвели до ознайомлення з ним осіб, не допущених до цих відомостей.

Можливий безконтрольний відхід конфіденційної інформації з візуально-оптичних, акустичних, електромагнітних та інших каналів [148].

Несанкціонований доступ – це протиправне навмисне оволодіння конфіденційною інформацією особою, що не має права доступу до охоронюваних відомостей.

Найпоширенішими шляхами НСД до інформації є:

перехоплення електронних випромінювань;

примусове електромагнітне опромінення (підсвічування) ліній зв'язку з метою одержання паразитної модуляції несучої частоти;

застосування підслухових пристроїв (закладок);

дистанційне фотографування;

перехоплення акустичних випромінювань і відновлення тексту принтера;

читання залишкової інформації в пам'яті системи після виконання санкціонованих запитів;

копіювання носіїв інформації з подоланням мір захисту;

маскування під зареєстрованого користувача;

маскування під запити системи;

використання програмних пасток;

використання недоліків мов програмування й операційних систем;

незаконне підключення до апаратури й ліній зв'язку спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;

злочинний вивід з ладу механізмів захисту;

розшифровка спеціальними програмами зашифрованої інформації;

інформаційні інфекції.

Перераховані шляхи несанкціонованого доступу вимагають досить більших технічних знань і відповідних апаратних або програмних розробок з боку зломщика. Наприклад, використовуються технічні канали витоку – це фізичні шляхи від джерела конфіденційної інформації до зловмисника, за допомогою яких можливе одержання охоронюваних відомостей. Причиною виникнення каналів витоку є конструктивні й технологічні недосконалості схемних рішень або експлуатаційне зношування елементів. Усе це дозволяє зломщикам створювати діючі на певних фізичних принципах перетворювачі, що утворять властивий цим принципам канал передачі інформації – канал витоку [140].

Однак є й досить примітивні шляхи НСД [137]:

розкрадання носіїв інформації й документальних відходів;

ініціативне співробітництво;

відмінювання до співробітництва з боку зломщика;

випитування;

підслуховування;

спостереження й інші шляхи.

Будь-які способи витоку конфіденційної інформації можуть призвести до значного матеріального й морального збитку як для організації, де функціонує СКІ, так і для її користувачів.

Менеджерам варто пам'ятати, що досить значна частина причин і умов, що створюють передумови й можливість не правочинного оволо-

діння конфіденційною інформацією, виникає через декількох елементарних недоробок керівників організацій і їхніх співробітників. Наприклад, до причин і умов, що створюють передумови для витоку комерційних секретів, можуть ставитися такі:

недостатнє знання працівниками організації правил захисту конфіденційної інформації й нерозуміння необхідності їхнього ретельного дотримання;

використання неатестованих технічних засобів обробки конфіденційної інформації;

слабкий контроль за дотриманням правил захисту інформації правовими, організаційними й інженерно-технічними мірами;

плинність кадрів, у тому числі тих, які володіють відомостями, що становлять комерційну таємницю;

організаційні недоробки, у результаті яких винуватцями витоку інформації є люди – співробітники СКІ і ІТ.

Більшість із перерахованих технічних шляхів несанкціонованого доступу піддаються надійному блокуванню при правильно розробленій і реалізованій на практиці системі забезпечення безпеки. Але боротьба з інформаційними інфекціями становить значні труднощі, тому що існує й постійно розробляється величезна кількість шкідливих програм, мета яких – псування інформації в БД і ПЗ комп'ютерів. Велика кількість різновидів цих програм не дозволяє розробити постійних і надійних засобів захисту проти них.

Технічні КВІ виникають при використанні зловмисником спеціальних технічних засобів розвідки, що дозволяє одержувати захищену інформацію без безпосереднього контакту із джерелом цієї інформації [132].

Основними видами цих каналів є акустичні, електромагнітні й візуально-оптичні акустичні канали, пов'язані з утворенням акустичного поля, що виникає за наявності звукової хвилі. Канал утворюється в кабінетах, офісах, будівельних конструкціях, вентиляційних шахтах; вібрує скло у вікнах, перегородки в приміщеннях, дверях і т. д. Акусто-перетворювальний канал утворюється за рахунок мікрофонного ефекту, при якому з метою радіоелектронної апаратури з'являються сторонні й ритмічні сигнали. Ці сигнали обумовлені механічним впливом звукової хвилі. Канал утворюється в електродинаміках, динаміках радіотрансляції, елементах телефонних мереж, а також у холодильниках, електродзвінках і т. д.

Електромагнітні канали витоку інформації виникають у лініях радіозв'язку при роботі радіотелефонів, побутових приладах аудіо-, відеотехніки й будь-якої обчислювальної техніки.

Візуальний або візуально-оптичний канал утворюється за рахунок спостереження за об'єктом, у тому числі за допомогою оптичних приладів фото- й відеоапаратури.

Конфіденційна інформація

Під документом, який відносимо до категорії обмеженого доступу до нього персоналу, мається на увазі документована на будь-якому носії цінна текстова, образотворча або електронна інформація.

Цінна ІОД може бути недокументованою.

Документи з ІОД поділяються на секретні й несекретні [102].

Обов'язковою ознакою секретного документа є наявність на ньому відомостей, які відповідно до закону належать до державної таємниці.

Несекретні документи обмеженого доступу містять у собі:

1. У державних структурах – документи, проекти документів і супутні матеріали, що містять відомості, віднесені до службової таємниці.

2. У підприємницьких структурах і напрямку подібної діяльності – документи, що містять відомості, які їх власник (власники) відносить до комерційної, банківської таємниці й іншим, технологічним і технічним нововведенням.

3. Незалежно від приналежностей – документи й бази даних, що фіксують будь-які персональні дані про громадян, а також утримуючу професійну таємницю, наприклад лікарську, адвокатську, підприємств зв'язку й т. д.

Документи, віднесені до будь-якого виду недержавної таємниці називаються конфіденційними.

Особливістю конфіденційного документа є те, що він одночасно є:

1) носієм цінної захищеної інформації;

2) основним джерелом нагромадження й поширення цієї інформації, у тому числі її розголошення й витоку;

обов'язковим об'єктом захисту.

Джерела й канали втрати конфіденційної інформації

Джерела конфіденційної інформації становлять накопичувачі цієї інформації. Це секрети носіїв, що відрізняються пасивністю.

До числа основних видів джерел інформації відносяться:

1) публікації про організацію та її розробки;

2) рекламні видання й виставкові матеріали;

3) персонал організації й оточуючих її людей;

4) документи;

5) фізичні поля, електромагнітні хвилі, що супроводжують роботу обчислювальної й іншої офісної техніки.

Джерело конфіденційної інформації, яка містить персонал, і людей, які оточують організацію, включає:

1) всіх співробітників даної організації, включаючи перших керівників;

2) співробітників інших організацій і фірм, які підтримують ділові відносини з даною організацією, наприклад посередники, співробітники торговельних фірм, рекламних агентств і т. д.;

3) співробітників держустанов, до яких фірма звертається відповідно до закону, наприклад співробітники податкових і інших інспекцій, муніципальних органів керування, правоохоронних органів і т. д.;

4) журналістів засобів масової інформації, що співпрацюють із фірмою;

5) відвідувачів фірми – працівників комунальних служб, поштових службовців, працівників служб екстремальної допомоги;

6) сторонніх осіб, що проживають поруч із приміщеннями фірми; вуличних перехожих.

Документація як джерело конфіденційної інформації містить у собі:

1) конфіденційну документацію;

2) звичайну ділову й науково-технічну документацію, що містить відкриті відомості.

У кожній із зазначених груп документів можуть бути документи на традиційних паперових носіях, документи на технічних носіях (магнітні, фотографічні й т. д.), документи електронні.

Часто поза зоною контролю перебуває особиста, творча, наукова й технічна інформація, чорнові матеріали книг, статей, звітів і т. д.

Інформація джерел завжди поширюється в зовнішнє середовище. Канали поширення інформації, у тому числі конфіденційної, носять об’єктивний характер, відрізняються активністю й містять у собі:

1) документопотоки;

2) ділові, торговельні, наукові й інші комунікативні регламентовані зв’язки;

3) інформаційні мережі;

4) природні технічні канали випромінювання або створення тла.

Схема взаємозв'язку між джерелами та КВІ наведена на рис. 8.3.

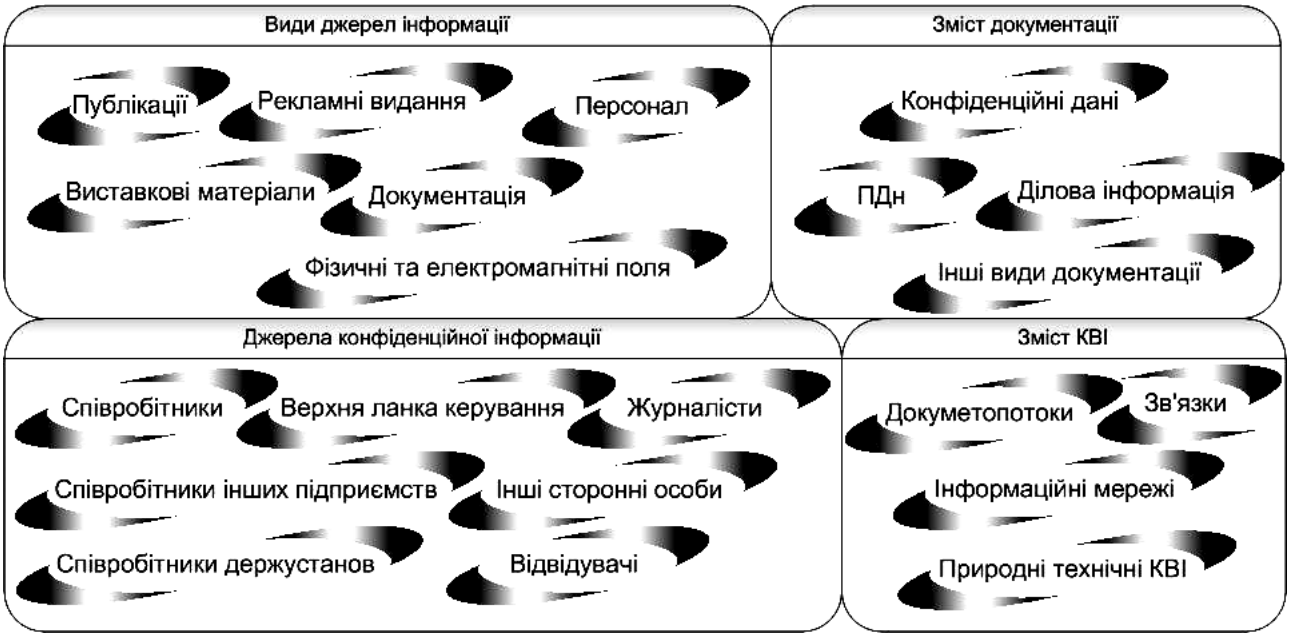


Рис. 8.3. **Взаємозв'язок між джерелами та КВІ** [65]

Джерело конфіденційної інформації, яке називається працююча офісна техніка, містить у собі обчислювальну техніку й організаційну техніку, наприклад апарати зв'язку й лінії зв'язку, факси й іншу техніку.

Легальні й нелегальні методи добування інформації

Легальні способи одержання цінної інформації, тобто так зване безневинне шпигунство, відрізняються правовою безпекою й не вимагають великих витрат. В основі цих методів лежить аналітична робота фахівців, аналітиків під опублікованими й загальнодоступними матеріалами.

При аналітичній роботі здійснюється зіставлення наявних відомостей за конкретним питанням отриманих з різних джерел.

Професійний аналіз доступних матеріалів дає до 95 % цінної інформації про конкурента і його технологічні нововведення, інші 5 % містять секрет фірми й можуть бути отримані зловмисником за допомогою нелегальних дій [105].

Добування документованої, службової інформації завжди ґрунтується на нелегальних діях і на несанкціонованому доступі до інформації.

Нелегальні дії містять у собі:

злодійство;

навмисний обман;

хабарництво;

використання слабкості або хворобливого стану співробітника;

шантаж співробітника;

використання екстремальних ситуацій і т. д.

Нелегальні дії виконують або безпосередньо зловмисник, що працює у фірмі, або працівник фірми, який співробітничає з ним. Таке співробітництво утворює так званий агентурний канал.

Отже, фірми можуть уживати такі нелегальні способи одержання цінної інформації:

1) регулярне візуальне спостереження приміщень фірми, роботи персоналу;

2) прослуховування приміщень фірми, розмов співробітників у неслужбовій обстановці;

3) помилкові переговори щодо ділового співробітництва й одержання цінної інформації у процесі переговорів;

4) перехоплення інформації, яка циркулює в технічних каналах поширення інформації;

5) аналіз відходів виробництва, огляд сміття й т. д.

До персоналу можуть застосовувати такі нелегальні способи одержання цінної інформації:

1) використання співробітника фірми для усвідомленого співробітництва:

а) ініціативне співробітництво працівника через помсту керівництву фірми, підкуп, психічну неврівноваженість, постійну матеріальну скруту і т. д.;

б) відмінювання або примус до співробітництва шляхом шантажу, погрози, облудних дій, зміна поглядів шляхом переконання, фізичного насильства, використання негативних рис характеру й т. д.;

2) використання працівника для неусвідомленого співробітництва:

а) помилкова ініціатива під час прийому на роботу в конкуруючу фірму працівника, що володіє цінною інформацією, вивідування в процесі співбесіди необхідних відомостей і, потім, відмова в прийомі на роботу;

б) одержання цінної інформації у співробітників фірми на науково-технічних конференціях, виставках, в особистих бесідах, використання диспуту між фахівцями;

в) одержання від співробітника потрібної інформації під час спілкування з ним зловмисника, особливо, коли співробітник перебуває в стані алкогольного сп'яніння, дії наркотиків, психотропних препаратів, гіпнозу й т. д.

3) добування інформації за рахунок:

а) слабкого знання персоналом принципів захисту інформації;

б) безвідповідального невиконання співробітником цих правил;

в) помилкових дій персоналу, спровокованих або неспровокованих зловмисником;

г) використання екстремальних ситуацій у приміщеннях фірми й подій з персоналом.

Технічні канали витоку інформації

Для перехоплення, обробки та аналізу інформації за допомогою КВІ можуть використовуватися різноманітні технічні засоби, а також люди (порушники). Тоді існуючі КВІ залежно від джерел і одержувачів інформації утворюють чотири основних типи каналів: "людина – людина", "людина – технічні засоби", "технічні засоби – технічні засоби" і "технічні засоби – людина" [91].

Якщо інформаційний потік поширюється в напрямку від носія до одержувача, то утворюється *узагальнений канал витоку*, якщо ж інформаційний потік у вигляді явної або прихованої дії направлений за згаданими чотирма типами каналів від порушника до носія інформації, то виникає так званий *узагальнений канал інформаційного впливу на носій інформації* (*канал спеціального впливу*). Залежно від того, на який параметр носія інформації задумано здійснити вплив, порушником можуть бути застосовані психічні, фізичні, програмно-математичні, радіоелектронні та інші способи і засоби. Параметрами, на які задумано здійснити вплив, можуть бути різні характеристики матеріальних носіїв, у тому числі й власні характеристики головного прямого носія інформації – людини.

Найбільший потенціал інформативності мають КВІ, у яких для отримання конфіденційної інформації використовуються різні технічні засоби. Такі канали одержали назву технічних (ТКВІ). Структура будь-якого

ТКВІ (рис. 8.4), що утворюється в результаті перехоплення, може бути представлена у вигляді системи передачі інформації.

Схема можливих каналів витоку і несанкціонованого доступу до інформації в типовому одноповерховому приміщенні показана на рис. 8.5, 8.6.

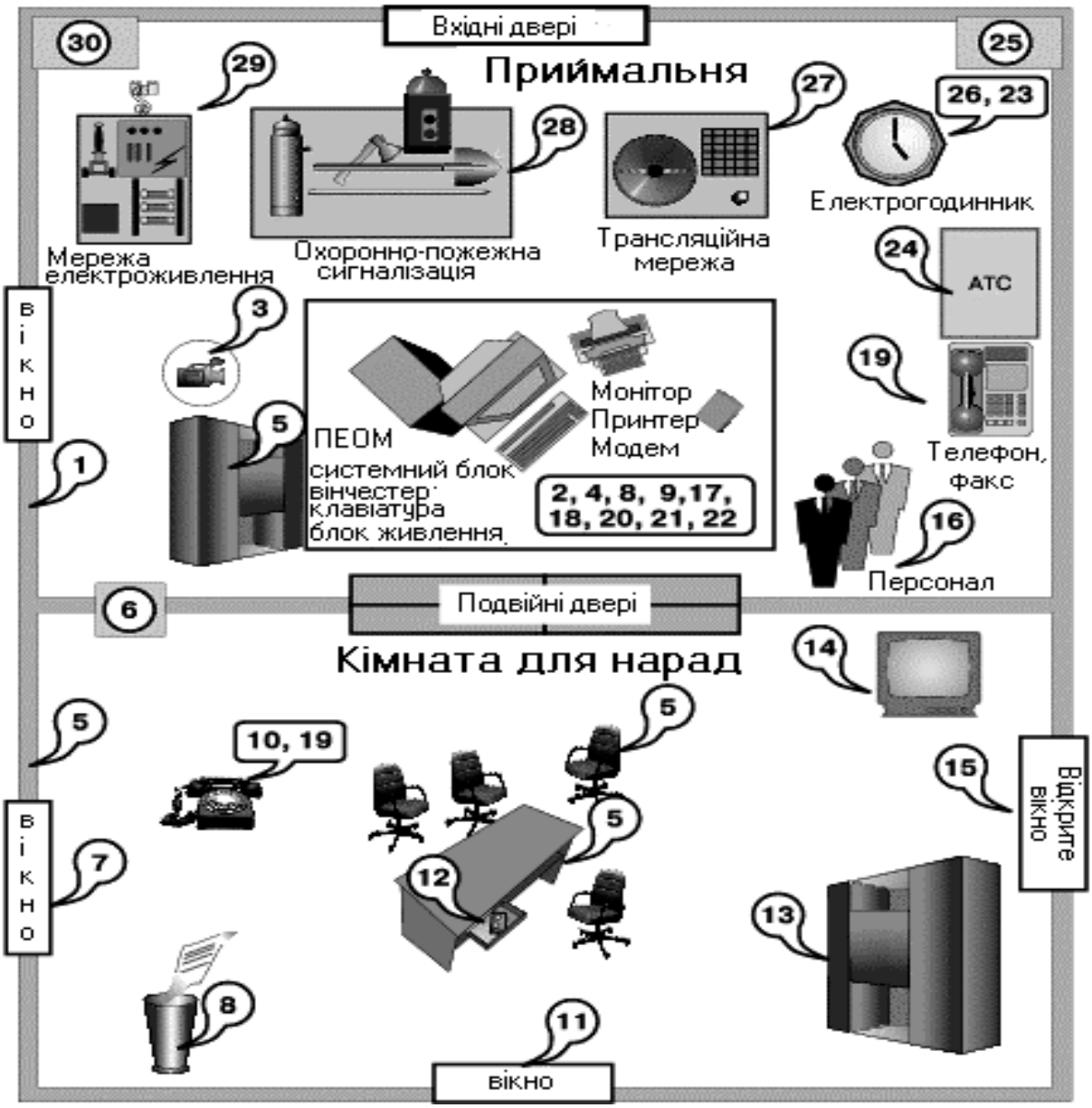
Фізичні принципи утворення ТКВІ і використовувані технічні засоби розвідки є окремою досить великою темою, і в даному посібнику не розглядаються.

Рис. 8.4. **Класифікація технічних КВІ** [63]

Компрометація інформації (один з видів *інформаційних* інфекцій). Реалізується, як правило, за допомогою несанкціонованих змін у базі даних, у результаті чого її споживач змушений або відмовитися від неї, або докладати додаткових зусиль для виявлення змін і відновлення правдивих відомостей. При використанні скомпрометованої інформації споживач піддається небезпеці прийняття правильних рішень.

Несанкціоноване використання інформаційних ресурсів, з одного боку, є наслідком її витоку й засобом її компрометації. З іншого боку, воно має самостійне значення, тому що може завдати великої шкоди керованій системі (аж до повного виходу ІТ з ладу) або її абонентам.

Помилкове використання інформаційних ресурсів, які є санкціонованими, може призвести до руйнування, витоку або компрометації зазначених ресурсів. Дана загроза найчастіше є наслідком помилок, наявних у ПЗ ІТ [127].



Умовні позначення: 1 – витік за рахунок структурного звуку в стінах і перекриттях; 2 – зняття інформації із стрічки принтера, погано стертих дискет і т. п.; 3 – зняття інформації з використанням відеозакладок; 4 – програмно-апаратні закладки в ПК; 5 – радіозакладки у стінах і меблях; 6 – зняття інформації із системи вентиляції; 7 – лазерне зняття акустичної інформації з вікон; 8 – виробничі й технологічні відходи; 9 – комп'ютерні віруси, логічні бомби і т. п.; 10 – зняття інформації шляхом наведень і "нав'язування"; 11 – дистанційне зняття відеоінформації (оптика); 12 – зняття акустичної інформації з використанням диктофонів; 13 – крадіжка носіїв інформації; 14 – високочастотний канал витоку в побутовій техніці; 15 – зняття інформації направленим мікрофоном; 16 – внутрішні канали витоку інформації (через обслуговуючий персонал); 17 – несанкціоноване копіювання; 18 – витік за рахунок побічного випромінювання терміналу; 19 – зняття інформації за рахунок використання "телефонного вуха"; 20 – зняття з клавіатури і принтера за акустичним каналом; 21 – зняття з монітора з електромагнітного каналу; 22 – візуальне зняття з монітора і принтера; 23 – наведення на лінії комунікацій і сторонні провідники; 24 – витік через лінії зв'язку; 25 – витік ланцюгами заземлення; 26 – витік мережею електрогодиннику; 27 – витік трансляційною мережею та гучномовним зв'язком; 28 – витік охоронно-пожежною сигналізацією; 29 – витік мережею електроживлення; 30 – витік мережею опалювання, газо- і водопостачання

Рис. 8.5. **Схема можливих КВІ** [63]

Несанкціонований обмін інформацією між абонентами може привести *до* одержання одним із них відомостей, доступ *до* яких йому заборонений. Наслідки ті ж, що й при несанкціонованому доступі.

Відмова від інформації полягає в невизнанні одержувачем або відправником цієї інформації фактів її одержання або відправлення.

Це дозволяє одній із сторін розривати укладені фінансові угоди "технічним" шляхом, формально не відмовляючись від них, наносячи тим самим другій стороні значний збиток.

Рис. 8.6. **Приклади КВІ у складі ПК** [65]

Порушення інформаційного обслуговування – загроза, джерелом якої є сама ІТ. Затримка з наданням інформаційних ресурсів абонентові може призвести до тяжких для нього наслідків. Відсутність у користувача своєчасних даних, необхідних для ухвалення рішення, може викликати його нераціональні дії.

Незаконне використання привілеїв. Будь-яка захищена система містить засоби, використовувані в надзвичайних ситуаціях, або засоби, які здатні функціонувати з порушенням існуючої політики безпеки. Наприклад, на випадок раптової перевірки користувач повинен мати можливість доступу до всіх наборів системи. Зазвичай ці засоби використовуються адміністраторами, операторами, системними програмістами й іншими користува-

чами, що виконують спеціальні функції. Більшість систем захисту в таких випадках використовують набори привілеїв, тобто для виконання певної функції потрібний певний привілей. Звичайно користувачі мають мінімальний набір привілеїв, а адміністратори – максимальний.

Набори привілеїв охороняються системою захисту. Несанкціоноване (незаконне) захоплення привілеїв можливе за наявності помилок у системі захисту, але найчастіше відбувається у процесі керування системою захисту, зокрема при недбалому користуванні привілеями.

Суворе дотримання правил керування системою захисту, а також принципу мінімуму привілеїв дозволяє уникнути таких порушень.

Під час опису в різній літературі різноманітних загроз для СКІ і способів їх реалізації широко використовується поняття атаки на СКІ. *Атака* – зловмисні дії зломщика (спроби реалізації ним будь-якого виду загрози). Наприклад, атакою є застосування кожної зі шкідливих програм. Серед атак на СКІ часто виділяють "маскарад" і "злом системи", які можуть бути результатом реалізації різноманітних загроз (або комплексу загроз).

Під *"маскарадом"* розуміється виконання яких-небудь дій одним користувачем СКІ від імені іншого користувача. Такі дії іншому користувачеві можуть бути дозволені. Порушення полягає у присвоєнні прав і привілеїв, що називається симуляцією або моделюванням. Мета "маскараду" – приховування яких-небудь дій за ім’ям іншого користувача або присвоєння прав і привілеїв іншого користувача для доступу до його наборів даних або для використання його привілеїв. Можуть бути й інші способи реалізації "маскараду", наприклад створення й використання програм, які в певнім місці можуть змінити певні дані, у результаті чого користувач одержує інше ім’я. "Маскарадом" називають також передачу повідомлень у мережі від імені іншого користувача. Найнебезпечніший "маскарад" у банківських системах електронних платежів, де неправильна ідентифікація клієнта може призвести до величезних збитків. Особливо це стосується платежів з використанням електронних карт. Використовуваний у них метод ідентифікації за допомогою персонального ідентифікатора досить надійний. Але порушення можуть відбуватися внаслідок помилок його використання, наприклад втрати кредитної картки або використанні очевидного ідентифікатора (свого ім’я й т. д.) [61].

Для запобігання "маскараду" необхідно використовувати надійні методи ідентифікації, блокування спроб злому системи, контроль входів у неї. Необхідно фіксувати всі події, які можуть свідчити про "маскарад",

у системному журналі для його наступного аналізу. Також бажано не використовувати програмні продукти, що містять помилки, які можуть привести до "маскараду".

Під зломом *системи* розуміють навмисне проникнення в систему, коли зломщик не має санкціонованих параметрів для входу. Способи злому можуть бути різними, і при деяких з них відбувається збіг з раніше описаними загрозами. Так, об'єктом полювання часто стає пароль іншого користувача. Пароль може бути розкритий, наприклад, шляхом перебору можливих паролів. Злом системи можна здійснити також, використовуючи помилки програми входу.

Основне навантаження захисту системи від злому несе програма входу. Алгоритм уведення ім'я й пароля, їхнє шифрування, правила зберігання й зміни паролів не повинні містити помилок. Протистояти злому системи допоможе, наприклад, обмеження спроб неправильного уведення пароля (тобто виключити досить великий перебір) з наступним блокуванням термінала й повідомленням адміністратора у випадку порушення. Крім того, адміністратор безпеки повинен постійно контролювати активних користувачів системи: їхні імена, характер роботи, час входу й виходу й т. д. Такі дії допоможуть вчасно встановити факт злому й почати необхідні дії.

Умовою, що сприяє реалізації багатьох видів загроз СКІ, є наявність "люків". Люк-схованка, не документована точка входу в програмний модуль, що входить до складу ПЗ СКІ і ІТ. Люк вставляється в програму, зазвичай на етапі налагодження для полегшення роботи: даний модуль можна викликати в різних місцях, що дозволяє налагоджувати окремі частини програми незалежно. Наявність люка дозволяє викликати програму нестандартним чином, що може відбитися на стані системи захисту. Люки можуть залишитися в програмі з різних причин [102]:

їх могли забути забрати;

для подальшого налагодження;

для забезпечення підтримки готової програми;

для реалізації таємного доступу до програми після її установки.

Більша небезпека люків компенсується високою складністю їх виявлення (якщо, звичайно, не знати заздалегідь про їх наявність), тому що виявлення люків – результат випадкового й трудомісткого пошуку. Захист від люків один – не допускати їхньої появи в програмі, а при прий-

манні програмних продуктів, розроблених іншими виробниками, варто проводити аналіз вихідних текстів програм з метою виявлення люків.

Реалізація загроз СКІ приводить до різних видів прямих або непрямих втрат. Втрати можуть бути пов'язані з матеріальним збитком: вартість компенсації, відшкодування іншого побічно втраченого майна; вартість ремонтно-відбудовних робіт; витрати на аналіз, дослідження причин і величини збитку; додаткові витрати на відновлення інформації, пов'язані з відновленням роботи й контролем даних і т. д.

Втрати можуть виражатися в обмеженні банківських інтересів, фінансових витратах або у втраті клієнтури.

Статистика показує, що у всіх країнах збитки від зловмисних дій безупинно зростають. Причому основні причини збитків пов'язані не стільки з недостатністю засобів безпеки як таких, скільки з відсутністю взаємозв'язку між ними, тобто з нереалізованістю системного підходу. Тому необхідно випереджальними темпами вдосконалювати комплексні засоби захисту.

8.2. Методи та засоби захисту від витоку інформації

Захист інформації від витоку технічними каналами досягається шляхом розробки та реалізації таких заходів [63] (у різних джерелах ці заходи виділяються і формулюються по-різному):

організаційних;

первинних технічних;

основних технічних з використанням засобів забезпечення ТЗІ.

Організаційні заходи захисту інформації – це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом регламентації діяльності персоналу та порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ [63].

Первинні технічні заходи передбачають захист інформації шляхом блокування виявлених загроз без використання спеціальних засобів ТЗІ.

Основні технічні заходи передбачають захист інформації шляхом блокування виявлених загроз із використанням спеціальних засобів ТЗІ.

Усі заходи розробляються одночасно і ув'язуються один з одним.

Організаційні заходи передбачають встановлення:

окремих завдань захисту ІОД та ІПЗ;

структури й технології функціонування ТЗІ;

вимог до забезпечення ТЗІ при організації проектування будівництва (нового будівництва, розширення, реконструкції та капітального ремонту) будівель, споруд і окремих приміщень;

порядку реалізації організаційних, первинних і основних технічних заходів ТЗІ;

прав і обов'язків підрозділів і осіб, що беруть участь в обробці ІОД та ІПЗ;

порядку придбання засобів забезпечення ТЗІ і необхідних нормативних документів;

контролю й обмежень доступу до виділених приміщень;

територіальних, частотних, енергетичних, просторових і тимчасових обмежень у режимах використання технічних засобів, що потребують захисту;

порядку відключення на період проведення закритих заходів технічних засобів, які мають електроакустичні перетворювачі, від ліній зв'язку і т. д.;

порядку залучення до проведення робіт із захисту інформації організацій, які мають ліцензію на діяльність у сфері захисту інформації, видану відповідними органами (Держспецзв'язок);

порядку впровадження захищених засобів обробки інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

порядку контролю функціонування СЗІ за її якісними характеристиками;

порядку проведення атестації СЗІ з розробкою програми атестаційних випробувань;

процедури керування СЗІ, яка полягає у:

- вивченні та аналізі технології проходження ІзОД та ІПЗ у процесі функціонування СКІ;
- оцінці дії загроз на ІзОД та ІПЗ в конкретний момент часу;
- оцінці очікуваного ефекту від застосування засобів забезпечення ТЗІ;
- визначенні додаткової потреби в засобах забезпечення ТЗІ;
- здійсненні збору, обробки й реєстрації даних, що відносяться до ТЗІ;

розробці та реалізації пропозицій щодо коригування "Плану ТЗІ" в цілому або окремих його складових.

Первинні технічні заходи передбачають [63]:

блокування каналів витоку інформації без використання спеціальних засобів ТЗІ, яке може здійснюватися шляхом:

• демонтажу технічних засобів, ліній зв'язку, сигналізації та управління, енергетичних мереж, використання яких не пов'язане з життєзабезпеченням підприємства і обробкою ІОД;

• видалення окремих елементів технічних засобів, які є середовищем поширення полів і сигналів, з приміщень, де циркулює ІОД;

• тимчасового відключення технічних засобів, що не беруть участь в обробці ІОД, від ліній зв'язку, сигналізації, управління і енергетичних мереж;

• застосування способів і схемних рішень із захисту інформації, які не порушують основних технічних характеристик засобів забезпечення інформаційної діяльності;

блокування НСД до інформації або її носіїв без використання спеціальних засобів ТЗІ, яке може здійснюватися шляхом:

• створення умов роботи в межах встановленого регламенту;

• виключення можливості використання (випробування) програмних, програмно-апаратних засобів, які не пройшли перевірку;

перевірку справності та працездатності технічних засобів і систем забезпечення інформаційної діяльності відповідно до експлуатаційних документів. Виявлені несправні блоки та елементи можуть сприяти витоку або порушенню цілісності інформації й підлягають негайній заміні (демонтажу).

Основою первинних технічних заходів є використання захищених засобів (систем) забезпечення інформаційної діяльності, до яких включають:

програмні засоби обробки інформації;

технічні засоби (системи) обробки інформації;

технічні засоби (системи) життєзабезпечення;

оргтехніку;

продукцію, процеси;

інженерно-технічні споруди, будівлі, приміщення.

Основні технічні заходи передбачають:

1. Заходи щодо блокування ТКВІ з використанням *пасивних засобів* [42]:

контроль і обмеження доступу на об'єкти ТСПІ та у виділені приміщення:

• установка на об’єктах ТСПІ та у виділених приміщеннях технічних засобів і систем обмеження й контролю доступу;

локалізація випромінювань:

• екранування ТСПІ та їх сполучних ліній;

• заземлення ТСПІ та екранів їх сполучних ліній;

• звукоізоляція виділених приміщень;

розв’язування інформаційних сигналів:

• установка смугових фільтрів у допоміжних технічних засобах і системах, у яких спостерігається "мікрофонний ефект" і які мають вихід за межі контрольованої зони (див. рис. 8.5);

• установка спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання й каналізації, що мають вихід за межі контрольованої зони (див. рис. 8.5);

• установка автономних або стабілізованих джерел електроживлення ТСПІ;

• установка пристроїв гарантованого живлення ТСПІ (наприклад, генераторів мотора);

• установка в ланцюгах і лініях електроживлення ТСПІ та виділених приміщень спеціальних глушильних фільтрів.

2. Заходи щодо блокування ТКВІ з використанням *активних засобів* [64]:

просторове зашумлення:

просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад (у випадках виявлення та визначення частоти випромінювання закладного пристрою або побічних електромагнітних випромінювань ТСПІ) з використанням засобів створення прицільних завад (див. рис. 8.5);

створення акустичних і вібраційних завад з використанням генераторів акустичного шуму (див. рис. 8.5);

заглушення диктофонів у режимі запису з використанням відповідних пристроїв;

лінійне зашумлення:

лінійне зашумлення ліній електроживлення;

лінійне зашумлення сторонніх провідників і сполучних ліній ДТСЗ, що мають вихід за межі контрольованої зони (див. рис. 8.5);

знищення закладних пристроїв:

знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів (випалювачів "жучків").

3. Заходи щодо блокування ТКВІ з використанням *активно-пасивних засобів* [65]:

розв'язування інформаційних сигналів з одночасним лінійним зашумленням:

установка в ланцюгах і лініях електроживлення ТСПІ та виділених приміщень комбінованих пристроїв, що об'єднують в одному корпусі перешкодоглушильний фільтр і генератор шуму.

4. Заходи щодо виявлення портативних *електронних пристроїв перехоплення інформації (закладних пристроїв)*:

виявлення закладних пристроїв з використанням пасивних засобів:

установка у виділених приміщеннях засобів і систем виявлення лазерного опромінювання (підсвічування) шибок;

установка у виділених приміщеннях стаціонарних виявлювачів диктофонів;

пошук закладних пристроїв з використанням індикаторів поля, інтерсепторів, частотомірів, скануючих приймачів і програмно-апаратних комплексів контролю;

організація радіоконтролю (постійно або на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТСПІ;

виявлення закладних пристроїв з використанням активних засобів:

спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;

спеціальна перевірка виділених приміщень, ТСПІ та допоміжних технічних засобів з використанням рентгенівських комплексів;

спеціальна перевірка виділених приміщень з використанням металошукачів;

спеціальна перевірка виділених приміщень з використанням ендоскопа та комплекту оглядових дзеркал;

5. Заходи щодо *перетворення (шифрування, скремблювання) сигналів* у каналах зв'язку:

використання аналогових і цифрових скремблерів для перетворення мовних сигналів;

використання програмного й апаратного шифрування даних.

Слід зазначити, що викладені методи і засоби захисту інформації від витоку технічними каналами з розвитком технічних засобів розвідки та захисту інформації можуть змінюватися і доповнюватися новими рішеннями.

8.3. Методи визначення каналів витоку інформації

Виявлення каналів несанкціонованого доступу до цінної інформації фірми входить до числа постійних напрямів аналітичної роботи й у загальному вигляді містить у собі:

аналіз джерел конфіденційної інформації;

аналіз каналів об'єктивного поширення інформації;

аналітичну роботу із джерелом загрози інформації.

Аналітичне дослідження джерел конфіденційної інформації передбачає:

виявлення й класифікацію існуючих і можливих конкурентів і суперників фірми, кримінальних структур і окремих злочинних елементів, що цікавляться фірмою;

виявлення й класифікацію максимально можливого числа джерел конфіденційної інформації фірми;

виявлення, класифікацію й ведення переліку реального складу циркулюючої у фірмі конфіденційної інформації;

вивчення даних обліку поінформованості співробітників у таємниці фірми в розрізі кожного керівника й співробітника;

вивчення складу конфіденційної інформації у розрізі документів;

облік і вивчення виявлених внутрішніх і зовнішніх, потенційних і реальних загроз кожному окремому джерелу інформації, контроль процесу формування каналу несанкціонованого доступу до інформації;

ведення й аналіз повноти переліку захисних заходів, розпочатих по кожному джерелу, і захисних заходів, які можуть бути використані при активних діях зловмисника, завчасна протидія зловмисникові.

Обов'язковому обліку підлягають всі санкціоновані й несанкціоновані звернення співробітників фірми до конфіденційної інформації, документам, справам і БД.

Аналіз каналів об'єктивного поширення інформації передбачає:

виявлення й класифікацію реального максимального складу каналів об'єктивного поширення конфіденційної інформації у фірмі;

вивчення складних елементів кожного каналу з метою знаходження небезпечних ділянок, що сприяють виникненню каналу несанкціонованого доступу до інформації;

дослідження й узагальнення способів і сфери поширення інформації в кожному каналі;

вивчення складу конфіденційної інформації, що циркулює в КВІ;

вивчення складу конфіденційної інформації, що циркулює між джерелами;

вивчення сфери поширення інформації при комунікативних зв'язках фірми;

контроль і перекриття каналів несанкціонованого ознайомлення з інформацією обмеженого доступу для третіх осіб, випадкових, сторонніх людей;

дослідження складу й ефективності методів захисту, розпочатих по кожному каналу, і додаткових заходів протидії зловмисникові при активних загрозах, екстремальних ситуаціях.

Аналіз загроз – це один із найважливіших розділів аналітичної роботи і становить відповідь на питання, від чого або кого варто захищати об'єкти захисту. Джерела загрози конфіденційної інформації – об'єктивні й суб'єктивні події. Джерела загрози можуть бути зовнішніми й внутрішніми.

Аналітична робота із джерелом загрози конфіденційної інформації передбачає [97]:

виявлення й класифікацію максимального складу джерел загрози конфіденційної інформації;

облік і вивчення кожного окремого суб'єктивного внутрішнього й зовнішнього джерела, ступеня його небезпеки при реалізації загрози;

розробку заходів щодо локалізації й ліквідації об'єктивних загроз.

У сфері зовнішніх джерел загрози аналітична робота пов'язана з маркетинговими дослідженнями, які регулярно веде будь-яка фірма. Аналіз внутрішніх джерел загрози має на меті виявлення й вивчення несумлінних інтересів і злочинних дій окремих співробітників фірми й партнерів.

Аналітична робота проводиться під час потенційних і пасивних загроз джерелам і каналам поширення інформації. При активній загрозі одночасно здійснюється заздалегідь спланована, продумана й рішуча протидія зловмисникові.

Співробітники ІАС фірми повинні враховувати всі канали несанкціонованого доступу до конфіденційної інформації, виявляти, визначати най-

більш імовірні й контролювати їх. Із цією метою співробітники ІАС повинні брати безпосередню участь у заходах, у ході яких є ймовірність виникнення зазначених каналів доступу до конфіденційної інформації фірми.

Аналітично оброблені відомості вносяться в електронну БД. Аналітичні звіти з кожного напряму подаються з певною періодичністю. У будь-який момент часу на вимогу керівництва ІАС повинна подати зведений огляд в усіх напрямах.

Не менш важливими є періодичні напрями аналітичної роботи, які проводяться через певні проміжки часу з метою контролю ефективності й можливості внесення поліпшень у діючу у фірмі СЗІ. Такий вид напрямів аналітичної роботи насамперед вимагає аналізу ступеня безпеки.

Необхідно також періодично проводити аналіз порушень режиму конфіденційності.

Разові напрями аналітичних досліджень також є дуже важливими через те, що найчастіше бувають викликані надзвичайними обставинами, подіями й тому подібним, вимагають проведення досліджень у найкоротший термін.

Технічні засоби вияву КВІ використовують з метою:

1) виявлення можливості й організації каналів витоку інформації;

2) пошуку та виявлення техніки несанкціонованого знімання інформації в приміщеннях, машинах;

3) визначення необхідних заходів щодо захисту технічних засобів обробки інформації каналами зв’язку.

Виявлення та протидія витоку інформації становить складну систему організаційних і технічних заходів.

Технічні заходи включають:

1) пошук технічних засобів розвідки;

2) кодування (шифрування) переданої інформації;

3) придушення технічних засобів несанкціонованого знімання;

4) проведення заходів пасивного захисту (заземлення, екранування);

5) використання системи обмеження доступу;

6) використання поліграфів (детекторів неправди).

Усі пошукові технічні засоби можна поділити на два типи: техніку дослідження можливих каналів витоку інформації та техніку пошуку і локалізації спеціальних технічних засобів (СТЗ), призначених для несанкціонованого доступу до неї.

Техніка першого типу призначена для дослідження та вияву природних каналів витоку інформації (побічні випромінювання, звукопровідні конструкції, комунікації та ін.) та каналів можливого впровадження СТЗ. Техніка другого типу спрямована на пошук і локалізацію вже впроваджених СТЗ (радіомікрофони, провідні системи та ін.).

Універсальність тієї чи іншої апаратури призводить до зниження її параметрів за кожною окремою характеристикою. У той же час існує значна кількість різноманітних за своєю фізичною природою каналів витоку інформації, а також фізичних принципів, на основі яких працюють СТЗ несанкціонованого доступу до інформації. Ці фактори зумовили різноманітність пошукової апаратури.

Найбільш поширеними засобами візуального огляду при проведенні пошукових заходів важкодоступних місць (підвісні стелі, вентиляційні шахти і та ін.), де можуть бути встановлені СТЗ, є: комплект оглядових дзеркал, засоби візуального контролю (ендоскоп), металошукачі. Важливе місце при проведенні пошукових заходів займають оглядові рентгенівські апарати та тепловізійна техніка. Рентгенівські апарати використовуються як засіб неруйнівного пошуку СТЗ в твердих перешкодах (стіни, декоративні панелі і тощо).

Тепловізори дозволяють виявити енергонасичені об’єкти (джерело автономного живлення радіомікрофона) на фоні природних завад.

Крім того, широко використовуються системи нелінійної локації, призначені для пошуку СТЗ, які вміщують електронні напівпровідникові системи. Принцип дії нелінійного локатора полягає в опромінюванні зондуючим сигналом (звичайно, в діапазоні ЗВЧ) оточуючого простору або предмета, що передбачувано містить напівпровідникові елементи (транзистори, діоди, мікросхеми і та ін.). Надісланий сигнал буде ними прийнятий, перетворений у сигнал з іншим частотним спектром і перевипромінений на другій і третій гармоніках у навколишній простір. Причому зазначені процеси будуть мати місце незалежно від його власної робочої частоти чи від того, включений цей пристрій чи виключений. Перевипромінений сигнал приймається приймачем нелінійного локатора, перетворюється і надходить на пристрій візуальної чи звукової індикації [102].

Таким чином, нелінійний локатор виявляє тільки радіоелектронну апаратуру і, на відміну від класичного лінійного радіолокатора, "не бачить" відображення від навколишніх предметів.

Використання різноманітної пошукової техніки (металошукачів, індикаторів електромагнітних випромінювань і нелінійних радіолокаторів) дозволяє знайти несанкціоновано підключений радіомікрофон за кожною з демаскуючих ознак:

електромагнітне випромінювання;

електронні елементи з нелінійною характеристикою;

металеві елементи конструкції.

Усі складності полягають у тому, що аналогічними властивостями (наявність металевих виробів у будівельних конструкціях) володіють і інші предмети, тому відрізнити один відгук радіомікрофона від другого – перешкодного – дуже складно.

Пристрої моніторингу (контролю) стороннього радіовипромінювання за їхньою функціональною дією можна класифікувати таким чином: індикатори електромагнітних випромінювань (поля) – найпростіші пристрої, що дозволяють знайти мікрофонні чи телефонні радіопередавачі. Вони вже не відповідають повною мірою сучасним вимогам для пошуку та виявлення радіопередавачів.

Лічильники частоти мініатюрні призначені для пошуку й реєстрації активних частот радіопередавачів. Працюють у діапазоні частот від 10 Гц до 2,8 ГГц, відрізняють випадкові шуми від когерентного радіовипромінювання, має функції автозахоплення (утримує частоту як завгодно довго на дисплеї лічильника). Цифровий фільтр і вбудований мікропроцесор у лічильники частоти оцінюють кожен вимір та ігнорують випадкові результати вимірів. Вони визначають переважну частоту і мають більшу чутливість, ніж звичайні індикатори полів. Дозволяють проводити вимір радіосигналів на максимально можливих відстанях за допомогою додаткових антен. Мають інтерфейс типу RS-232 для підключення до ПК. Стаціонарні повнофункціональні лічильники дозволяють вимірювати частоту, період, шпаруватість, тимчасові інтервали.

АМ-інтерсептори працюють у діапазоні від 0,5 мГц до 2,5 ГГц, мають чуттєвий вимірник радіосигналів (різні види модуляції) і оснащені приймачем АМ ближньої області. Прийнятий сигнал обробляється схемою автоматичної установки рівня сигналу для звукового контролю. АМ-інтерсептори реагують на найдужчий сигнал в ефірі, ефективні для оперативного виявлення ЗТЗ, що використовують радіоканал для передачі інформації.

Активний преселектор (високочастотний підсилювач радіосигналів) використовується спільно з лічильниками частот для збільшення відстані прийому від джерела радіовипромінювання в 10 разів (ширина діапазону зменшується від 3 ГГц до 4 ГГц, що дозволяє значно збільшити чутливість, оскільки набагато менша кількість фонових сигналів). Передбачено спільне використання з перерахованими технічними засобами моніторингу стороннього радіовипромінювання.

Автоматизовані програмно-апаратні комплекси радіоконтролю призначені для проведення радіорозвідки на місцевості та виявлення технічних каналів витоку інформації в контрольованих приміщеннях. Дані задачі, незважаючи на їхнє розходження, мають багато спільного як у підходах до рішення, так і у використовуваних технічних засобах [97].

У даний час створені багатофункціональні автоматизовані комплекси радіорозвідки і виявлення КВІ, здатні в рамках обраної конфігурації вирішувати максимальне число задач з високими технічними показниками. Такий підхід до вирішення задач радіоконтролю знижує не тільки вартісні показники (у перекладі на кожну задачу), але й дозволяє скоротити номенклатуру і масогабаритні показники необхідних засобів.

Основними складовими частинами автоматизованих комплексів радіорозвідки є: антенна система; стандартні радіоприймальні пристрої, високочастотні (ВЧ) тюнери чи дороблені радіоприймальні пристрої з дистанційним керуванням; блоки аналого-цифрової обробки; персональні комп'ютери стандартної конфігурації з пакетами спеціального математичного забезпечення (СМЗ); системи електроживлення від мережі перемінного струму, бортової мережі (автомобіля, гелікоптера й інших транспортних засобів) чи автономних акумуляторів.

Автоматизовані комплекси радіоконтролю за конструктивним виконанням можна умовно розділити на стаціонарні, мобільні (на автомобілях, гелікоптерах та інших транспортних засобах) і портативні (як варіант – розміщення в кейсі).

Для захисту інформації від несанкціонованого зняття віброакустичними каналами використовується метод активного віброакустичного зашумлення. Цей метод полягає в наведенні в пружних конструкціях службових приміщень шумових віброколивань, що поширюються по твердим будівельним конструкціям, викликаючи їхні шумові мікродеформації, які, у свою чергу, приглушують мікродеформації, створювані акустичним впливом мовних сигналів.

Система віброакустичного зашумлення реалізується у вигляді стаціонарного та мобільного комплексів. Однак і в тому, і в іншому випадку вона складається з генератора низькочастотних шумових сигналів, декількох віброакустичних датчиків, що зашумлюють віброакустичні та акустичні канали витоку інформації.

Датчики віброакустичного зашумлення (у випадку стаціонарного устаткування об'єкта захисту) монтуються на стінах, перекриттях, водопровідних трубах і опалювальних батареях, вентиляційних шахтах, віконних плетіннях тощо і створюють загороджувальну перешкоду в елементах будівельних конструкцій.

Акустичні мікрофони є чуттєвими акустичними елементами, що включають і виключають генератор низькочастотних шумових сигналів і керують роботою віброакустичних датчиків. Якщо в контрольованому приміщенні не ведуться переговори, сигнал на виході акустичних мікрофонів не досягає порога спрацьовування системи віброакустичного зашумлення. При перевищенні акустичного сигналу порога спрацьовування включається низькочастотний генератор шуму і віброакустичні датчики роблять віброакустичне зашумлення контрольованого приміщення.

Найбільш небезпечними, з погляду несанкціонованого зняття за рахунок ПЕМВН, є монітори комп'ютерів зі стандартами розгорнень телевізійних систем. В усіх зазначених випадках навіть використання могутніх криптографічних методів захисту інформації не приводить до бажаних результатів, і тільки застосування спеціальних методів і апаратури захисту від ПЕМВН здатне усунути виникаючий КВІ.

Такими методами є [135]:

1. Доробка пристроїв обчислювальної техніки з метою мінімізації електромагнітних випромінювань (застосування малоенергетичних мікросхем, пристроїв відображення на рідкісних кристалах, локальне екранування окремих пристроїв персональних комп'ютерів, гальванічна розв'язка за ланцюгами електроживлення і т. д.).

2. Електромагнітне екранування приміщень, у яких розташована обчислювальна техніка, а також інше електронне устаткування, використовуване для обробки як аналогової, так і дискретної інформації.

3. Активне радіотехнічне придушення побічних електромагнітних випромінювань і радіотехнічне маскування працюючої апаратури.

Доробка пристроїв обчислювальної техніки дозволяє істотно зменшити рівень побічних електромагнітних випромінювань, однак цілком їх

не усуває. Необхідно також зазначити, що електромагнітне екранування вносить певний дискомфорт у роботу користувачів і обслуговуючого персоналу, а в деяких випадках зробити таке екранування неможливо.

9. Організація інформаційної безпеки на підприємстві

9.1. Політики інформаційної безпеки

Кінцева мета бізнесу – одержання прибутку. Умови досягнення мети – ефективне використання ресурсів і зниження можливих непередбачених збитків.

Політика ІБ на підприємстві розуміється як комплекс заходів щодо захисту ресурсів і зниження ризиків, спрямованих на створення й підтримку умови досягнення кінцевої мети бізнесу [72].

При виробітку **концепції забезпечення ІБ** для організацій автори роботи виходять з того, що результатом застосування заходів протидії загрозам є захист персоналу, матеріальних, фінансових, інформаційних ресурсів від нанесення їм можливого збитку.

Розрізняють такі **напрями забезпечення ІБ** організації [65]:

правовий захист, тобто наявність таких нормативно-правових елементів, як: патенти, авторські права, ліцензії, закони, положення, накази та ін.;

організаційний захист, тобто регламентація виробничої діяльності й взаємовідносини виконавців (сторін), що виключає завдання збитків: режим і охорона підприємства, забезпечення збереження конфіденційної інформації, підбір і розміщення персоналу;

інженерно-технічний захист, тобто використання різних технічних засобів, що перешкоджають завданню збитків: фізичні й апаратні засоби, програмне забезпечення та ін.

Безпосередньо в організації забезпечення ІБ – це виконання таких **функцій**:

інформаційно-аналітична робота;

забезпечення схоронності матеріальних і фінансових ресурсів;

забезпечення ІБ;

забезпечення безпеки персоналу.

Крім розробки основних заходів і засобів захисту інформації, які передбачається впроваджувати в СКІ, з метою позначення для керівництва й персоналу СКІ *стратегії* захисту інформації в організації (підрозділі) необхідна розробка політики ІБ організації (підрозділу) або політики безпеки, яку можна назвати стратегічним планом, що описує мету, завдання, загальні вимоги, правила, обмеження, рекомендації у сфері ІБ.

Мета та завдання політики безпеки

1. Правила політики інформаційної беспеки (ПІнБ) [72]:

описують безпеку в загальних термінах, сенс яких повинен бути зрозумілий також нефахівцям, і не описують, яким чином її здійснювати;

не замінюють інструкції та стандарти.

2. Правила, необхідні для:

декларації основних принципів забезпечення ІБ;

демонстрації підтримки політики ІБ з боку керівництва;

покладання обов'язків і відповідальності на співробітників щодо підтримки функціонування створеної СЗІ;

для документального підтвердження відповідності підходів до забезпечення ІБ всім необхідним стандартам і нормативним актам (вітчизняним або міжнародним).

3. Мета політики безпеки досягаються формуванням документів (розділів), у яких визначаються:

об'єкти захисту і необхідний рівень їх безпеки;

потенційні порушники ІБ;

інформаційні ризики;

правила розмежування доступу до захищених ресурсів;

підходи до управління програмно-апаратним забезпеченням СКІ;

порядок розробки, супроводу й модернізації програмно-апаратного забезпечення СКІ;

підходи до забезпечення фізичної безпеки об'єктів захисту;

порядок резервного копіювання, архівного зберігання й видалення даних;

правила захисту інтелектуальної власності;

підходи до реагування на інциденти;

стратегія щодо комп'ютерних злочинів.

Обов'язки у сфері інформаційної безпеки

1. Обов'язки керівництва:

участь і підтримка комісії з ІБ;

визначення експертів, які класифікують інформацію за ступенем її важливості та допускають відхилення в її обробці від загальноприйнятої практики;

організація розробки й узгодження планів захисту інформації.

2. Обов'язки відділу (підрозділу) ІБ:

відповідає за впровадження та супровід в організації правил ІБ, а також стандартів, інструкцій і процедур;

відповідає за навчання, використання адміністративних заходів і підтримку з боку керівництва;

у випадках залучення сторонніх організацій або консультантів з ІБ забезпечує їх роботу за інструкціями, прийнятими в організації.

3. Обов'язки адміністраторів ІБ, адміністраторів СКІ, користувачів:

розподілити обов'язки та відповідальність за керування інформаційними ресурсами організації, координувати діяльність кожного, включаючи відповідальних за інформацію та матеріально відповідальних осіб;

призначити адміністратора ІБ для всіх розрахованих на велику кількість користувачів систем, а в кожному підрозділі виділити відповідального за ІБ;

визначити відповідальних осіб за безпеку обміну інформацією із зовнішніми організаціями в реальному масштабі часу;

включити положення про відповідальність за дотримання норм ІБ в посадові інструкції і в договори (контракти) із зовнішніми організаціями.

4. Право на інформацію і відповідальність за її збереження:

призначення за відповідними напрямами відповідальних осіб за поданням доступу до певного типу інформації;

визначення дозволених засобів і методів керування та адміністрування. Необхідно мати інструкції з надання та позбавлення прав доступу до інформаційних ресурсів організації, а також для відновлення інформації у разі її втрати.

5. Поняття керування безпекою і застосування правових норм:

знати і свідомо дотримуватися законів і правил у межах своїх функціональних обов'язків;

дотримуватись правил збору можливих джерел доказів і забезпечити юридичні гарантії ухвалення їх судом;

заздалегідь планувати можливу взаємодію організації з правоохоронними органами у разі вчинення комп'ютерних злочинів.

6. Навчання та підтримка ІБ:

навчатися повинні усі співробітники, що мають доступ до комп'ютерів і мереж організації. Співробітники повинні підписати зобов'язання пройти відповідне навчання, а також мати документ, що підтверджує проходження курсу навчання;

керівництво повинне виділити час на навчання і сприяти його проведенню;

навчання повинно відповідати вимогам політики безпеки.

Забезпечення фізичної безпеки систем консолідованої інформації

1. Розміщення комп'ютерів і монтаж устаткування:

визначити місця розташування комп'ютерів і комунікаційного устаткування, а також розміщення устаткування всередині будівель;

врахувати можливість підключення устаткування до резервних джерел живлення;

врахувати можливість фізичного проникнення або злому, захист від пожеж та інших лих;

передбачити захист від статичної електрики та інших фізичних чинників навколишнього середовища;

включити вимоги щодо забезпечення стабілізованого живлення серверів та інших найбільш важливих вузлів;

промаркувати устаткування СКІ (наприклад, ідентифікаційними штрих-кодами, які можна контролювати за допомогою комп'ютеризованого спеціального устаткування).

2. Системи контролю й керування доступом до устаткування:

створення системи контролю й керування доступом включає розробку правил: фізичного доступу; реєстрації осіб, що мають право доступу; проведення перевірок;

обмеження доступу до приміщень з комп'ютерами й серверами, резервних носіїв і до бібліотек з документацією. Запобігання можливості візуального вивчення комп'ютерного устаткування сторонніми особами;

ідентифікація, реєстрація, супровід відвідувачів, а також забезпечення незалежної охорони місць, де зберігається важлива інформація.

3. Планування дій в екстремальних ситуаціях:

визначення мети й завдань правил і планів реагування на аварійні ситуації. Пріоритетом є безпека співробітників;

створення та перегляд планів відновлення після аварій, проведення аварійних робіт. Забезпечення умов для періодичного контролю і оновлення планів;

повідомлення адміністрації у разі виникнення сигналів тривоги. Повідомлення адміністрацією відповідних робітників про аварійні відключення і про очікувані відключення. Забезпечення можливості контакту в неробочий час з аварійними службами.

4. Загальна безпека комп'ютерних систем:

розробка процедур, що гарантують безперервне функціонування важливих інформаційних ресурсів;

введення обмежень доступу користувачів до допоміжних і забезпечувальних систем.

5. Проведення періодичних перевірок конфігурації системи і мережі для мінімізації ризиків, пов'язаних з установкою нестандартних АЗ і ПЗ.

6. Підбір кадрів на основні технічні посади та інструктаж персоналу.

Загальні вимоги до керування і використання систем консолідованої інформації

1. Адресація мережі та архітектура:

відділення системи з найбільш важливими даними для полегшення керування доступом;

у правилах мережної адресації визначається, яку інформацію про конфігурацію мережі можна публікувати поза організацією. Конфігурувати DNS і систему перетворення мережних адрес (NAT) для приховування імен і адрес від зовнішнього оточення;

визначити процедури розширення мережі;

визначити правила адресації мережі (статична, динамічна).

2. Керування доступом до мережі:

розробити правила підключення до Інтернету, доступу до вхідних/вихідних телефонних каналів, а також інших зовнішніх підключень;

розробити правила використання віртуальних приватних мереж (VPN);

розробити правила для допоміжних систем, до яких відсутні вимоги з автентифікації, або ці вимоги не достатньо жорсткі.

3. Безпека реєстрації:

використовувати призначені для користувача імена, прив'язані до прізвища, імені, по батькові користувача, а не до його функціональних обов'язків. У правилах повинно бути відбито, що робити з призначеними для користувача іменами, визначеними ОС під час її установки;

імена тимчасових користувачів і користувачів, що не є співробітниками організації, повинні особливо ретельно контролюватися. У правила

присвоєння таких імен необхідно включити вимоги щодо контролю за ними та їх анулювання;

у правила необхідно включити положення щодо багаторазових/одноразових сеансів ідентифікації, а також вимоги, що стосуються систем позитивної ідентифікації;

протоколювання успішних, безуспішних спроб реєструватися в системі, час і дата останньої реєстрації в системі;

у правила обмеження числа сеансів реєстрації додати вимогу автоматичного виходу із системи (після закінчення проміжку часу, за часом доби й т. п.);

ввести розпорядження тим, хто має доступ до важливої інформації, виходити із системи у випадках залишення робочих станцій без нагляду;

визначити правила адміністрування облікових записів користувачів;

визначити правила роботи у привілейованому режимі, на основі яких розробляються інструкції, що визначають вимоги до доступу в систему, а також вимоги контролю за наданням привілеїв.

4. Паролі [83]:

стеження за структурою пароля й терміном його дії, заборона використовувати повторно старі паролі;

встановлення правил зберігання паролів;

зміна паролів, встановлених за замовчуванням;

призначення й використання спеціальних паролів, які сигналізують про обов’язковість введення пароля;

заборона відображення символів пароля при його введенні через інтерфейс користувача;

забезпечення передачі пароля КПІ у зашифрованому вигляді.

Рекомендації щодо підвищення стійкості паролів і поліпшення якості їх запам’ятовування

Застосування рекомендацій дозволить значною мірою поліпшити якість запам’ятовування паролів, не знижуючи при цьому їх довжини. Основні дії [108]:

1. Використання транслітерації – прийом введення символів пароля, при якому символи вводяться в одній розкладці, наприклад, англійській, а саме слово (або його частина) вводиться, дивлячись на іншу розкладку. Наприклад, російською мовою слово "крепость" реально буде виглядати як "rhtgjcnm". Цей прийом дозволить деякою мірою ускладнити використання візуального КВІ або звичайного підглядання при введенні пароля.

2. Впровадження спочатку/у середині/наприкінці пароля символу (більше одного призводить до ускладнення запам’ятовування) зі зміненим регістром, тобто якщо пароль вводиться рядковими символами, то використання в зазначених місцях великого символу (це додаткове натискання клавіші Shift під час введення, це можна зробити непомітно за допомогою мізинця) збільшує його криптостійкість не знижуючи здатності до запам’ятовування. Даний прийом заснований на психологічному факторі людини, при якому досить легко можна запам’ятати символ і його місце розташування, відмінний від усіх вводів інших. Таким чином, введений пароль може виглядати так: "КрепостЬ" або "кавуН".

3. Використання в тих же місцях (див. п. 2) цифр, але не більше двох, тому що більша кількість уже буде помітна при введенні. Цей прийом також ускладнює процес підглядання під час введення пароля. Таким чином, введений пароль може виглядати так: "2крепость" або "кавун78".

4. При введенні осмислених літературних слів (це не раціонально з погляду криптостійкості й можливості атаки за словником) рекомендується підбирати слова, що складаються із букв на клавіатурі, які знаходяться поряд (мається на увазі встановлена розкладка клавіатури – QWERTY). Це дозволить, не володіючи достатньою швидкістю набору, ввести пароль із необхідною швидкістю, що також зменшить імовірність підглядання під час введення пароля. Таким чином, введений пароль може виглядати так: "крепость" або "кавун".

5. Використання зворотного порядку введення осмислених слів – для оволодіння цього прийому необхідні відповідні навички, що може не кожний користувач. Крім того, не варто забувати про подібні можливості в програмах аудиту (злому) парольного захисту, наприклад, SAMInside або L0phtCrack 5 [80]. Таким чином, введений пароль може виглядати так: "ьтсоперк" або "нувак".

6. Використання ASCII-кодів другої половини таблиці (вводиться код, що є тризначною цифрою). Даний прийом ефективний, якщо вводиться пароль, що становить цифровий код достатньої довжини, наприклад, номер стільникового телефону з кодом оператора. Послідовність, що вводиться тоді, буде нерозривною при введенні й, отже, непомітною. Методика вводу: правою рукою на цифровій панелі вводиться цифрова послідовність, а лівою рукою непомітно натискаються відповідні клавіші (Shift+Alt) при вводі альтернативного коду. Таким чином, введений па-

роль може виглядати так "34657**156**457683**210**456", де жирним кольором показані альтернативні коди – 156 і 210. Також цим способом можна одержати достатню довжину пароля.

7. Використання властивості "щоденності" фрази, що приводить до значного збільшення довжини пароля, тобто у якості паролю використовується відома, повсякденна фраза, словосполучення, пропозиція, афоризм, прислів'я, вірші.

8. Використання властивості "незвичайності або неординарності", що є протидією методу соціальної інженерії: коли зломщик, стежачи за власником пароля, складає індивідуальний словник користувача (його звички, слова-паразити, жаргон, сленг, клички тварин, дати, скорочення, абревіатури), що потім буде використовувати для атаки за словником. Тоді, застосовуючи дане правило, користувач використовує як пароль зовсім незвичайне для нього слово, фразу, словосполучення.

Для виявлення подібних джерел можна користуватися так званими програмами твикерами (від англ. tweak) – редакторами схованих настроювань ОС або редакторами реєстру. До речі, використовуючи ці ж джерела, працюють деякі віруси.

5. Формалізувати правила розмежування доступу для кожної частини системи, що має свою специфіку.

6. Розробити правила віддаленого (зовнішнього) доступу користувачів (адміністраторів) у внутрішню систему організації:

використання тільки певного програмно-апаратного забезпечення;

віддалений користувач забезпечує належний захист комп'ютерного устаткування і даних на додаткових робочих вузлах;

організація є власником усієї інтелектуальної власності, використовуваної або створеної у середовищі віддаленого доступу;

співробітники несуть відповідальність за підтримку структурованого робочого середовища, а також виконання всіх інструкцій, що стосуються безпеки віддалених систем (ліцензування програмного забезпечення, створення резервних копій і т. д.).

Правила інформаційної безпеки при використанні ресурсів (Інтернет)

1. Підхід до Інтернет:

визначити питання, які стосуються правил безпеки при використанні зовнішніх ресурсів;

констатувати архітектуру мережі, задачі брандмауера і перетворення мережних адрес;

визначити перелік основних програм, програм забезпечення і протоколів, які можуть пропускатися через шлюз;

визначити відмінності між проксі-сервером і фільтрацією пакетів.

2. Правила адміністрування ресурсів, доступних із зовнішньої мережі:

обов'язкове обслуговування загальнодоступних даних;

порядок оновлення ресурсів;

порядок реагування на порушення ІБ зовнішніми користувачами.

3. Обов'язки користувачів:

інструктаж користувачів для роз'яснення їх обов'язків і відповідальності;

роз'яснення позиції організації щодо того, в якому вигляді співробітники представляють організацію під час їх доступу до різних вузлів мережі Інтернет;

заборона пересилання інформації з обмеженим доступом (необхідний перелік цієї інформації) без спеціально визначених процедур;

визначення правил завантаження та інсталяції ПЗ з мережі Інтернет.

4. Правила роботи в WWW:

рознесення на різні вузли мережі Web-серверів і програм, доступних через Web-сервер;

обов'язкова перевірка сервісних програм і сценаріїв на предмет безпеки і наявності помилок;

супровід і забезпечення захисту засобів, що постачаються ззовні, використовуваних для підтримки Web-послуг;

визначити відповідальних (правила керування) ресурсами Web-вузла;

визначення відповідальності користувачів у мережі Інтернет.

5. Відповідальність за програми:

відповідальні за програми і процеси особи повинні нести відповідальність за інформацію, яка пересилається, а також за її надійність і забезпечення гарантій того, що інформація поширюється тільки серед користувачів, яким надано відповідні повноваження;

правила розробки програм залежать від правил розробки ПЗ;

розширена автентифікація користувачів при зверненні до Інтернету;

6. Визначення ключових положень щодо використання віртуальних приватних мереж.

7. Модеми:

розробити правила, де і як встановлювати модеми;

розробити правила, які дозволять адміністраторам централізований моніторинг і керування модемами;

розробити правила, що передбачають обов'язкову автентифікацію осіб, які отримують доступ до мережі.

8. Застосування інфраструктури відкритого ключа (PKI):

описати правила і процедури використання PKI.

9. Описати інфраструктуру забезпечення електронної торгівлі:

зберігання даних;

ідентифікація і автентифікація;

захист пересилання даних;

методи обробки замовлень.

Правила інформаційної безпеки при використанні електронної пошти

1. Правила використання електронної пошти:

правила повинні вимагати відповідності поштових повідомлень загальноприйнятим морально-етичним нормам, загального відношення до електронної пошти і підпорядкування правилам безпеки.

2. Адміністрування електронної пошти:

визначення керування системою електронної пошти;

встановлення права сканування повідомлень, що проходять через систему електронної пошти. Це сканування може проводитися для пошуку КВ або перевірки змісту повідомлень. Незалежно від типу сканування необхідно сформулювати правило, яким передбачено право проведення організацією сканування;

правила експлуатації електронної пошти можуть включати механізми обмеження розмірів повідомлень, щоб не допустити перевантаження серверів і смуги пропускання мережі;

якщо повідомлення електронної пошти архівуються, необхідно це відзначити в правилі, в якому будуть відбиті основні деталі того, як проводитиметься архівація. У даному правилі також повинні бути позначені терміни зберігання та потенційні винятки з правил.

3. Використання електронної пошти для конфіденційного обміну інформацією:

розпорядження шифрувати повідомлення перед їх пересиланням і "підписувати" їх цифровими підписами;

правила шифрування фактично не відносяться до правил безпеки електронної пошти. Тому до правил безпеки електронної пошти повинно бути включене формулювання, яке адресує користувача до розпоряджень прийнятих в організації правил шифрування.

Антивірусний захист систем консолідованої інформації

1. Визначення принципів побудови системи антивірусного захисту (САЗ):

реалізація єдиної технічної політики під час обґрунтування вибору антивірусних продуктів для різних сегментів мережі;

повнота охоплення САЗ всієї мережі;

безперервність контролю мережі;

централізоване керування АЗ.

2. Формулювання завдань щодо впровадження АЗ:

придбання, установка і своєчасна заміна антивірусних пакетів на серверах і робочих станціях користувачів;

контроль правильності застосування антивірусного ПЗ;

виявлення вірусів у локальній мережі, їх оперативне лікування, видалення заражених об’єктів, локалізація заражених ділянок мережі;

своєчасне сповіщення користувачів про виявлені або можливі віруси, їх ознаки й характеристики;

підключення користувачів до мережі тільки за заявкою з відміткою адміністратора безпеки про установку ліцензійного антивірусного ПЗ;

передачу робочої станції від одного користувача іншому необхідно проводити з переоформленням підключення до мережі;

виявлені віруси доцільно досліджувати на стенді підрозділу ІБ для вироблення рекомендацій щодо їх коректного знешкодження;

у віддалених структурних підрозділах слід призначити позаштатних співробітників, відповідальних за антивірусний захист.

3. Програмно-технічні методи практичної реалізації антивірусного захисту інформації:

використання антивірусних пакетів;

архівація інформації;

резервування інформації;

ведення бази даних про віруси та їх характеристики.

4. Загальні вимоги до використовуваних антивірусних засобів:

сумісність з ОС серверів і робочих станцій;

сумісність з використовуваними програмами;

наявність повного набору антивірусних функцій, необхідних для забезпечення антивірусного контролю й знешкодження усіх відомих вірусів;

частота оновлення антивірусного ПЗ і гарантії постачальників (розробників) щодо його своєчасності.

Правила впровадження програмних засобів

1. Етапи розробки ПЗ:

наявність правил розробки ПЗ гарантує врахування питань безпеки при проектуванні й розробці ПЗ;

визначити обов'язки, які сприяють розробці заходів безпеки і коректному використанню ПЗ;

основні рекомендації розробки ПЗ: розробка специфікацій; контроль і перевірка інформації, що вводиться користувачем; контроль граничних значень даних під час їх пересилання; виключення не документованих можливостей уникнення засобів захисту і особливих привілеїв для розробників;

засоби керування доступом, вбудовані у власне ПЗ, повинні відповідати стандартам та інструкціям на їх застосування;

під час проектування та впровадження ПЗ власної розробки в ньому повинні застосовуватися ідентифікація і авторизація, що базуються на алгоритмах, вбудованих в ОС, БД або в системи сервісного ПЗ;

інші правила, що стосуються процесу розробки ідентифікації та авторизації, стосуються обробки інформації, яка містить паролі.

2. Тестування й документування:

забезпечити захист особистої та запатентованої інформації шляхом обмеження її використання під час тестування ПЗ;

процедура тестування призначена для виявлення усіх можливих проблем і порушень захисту;

заборонено встановлювати ПЗ, якщо воно не пройшло тестування і не було затверджене керівництвом;

наявність документації – це можливість проведення аналізу на предмет виникнення в системі проблем і побічних ефектів, які можуть негативно вплинути на ІБ системи.

3. Заміна версій і керування конфігурацією:

знати конфігурацію системи та її компонентів, завдяки чому адміністратори зможуть доповідати про порушення безпеки та несправні програми, які встановлені у системі;

вимога письмових запитів на внесення до системи змін, які впливають на безпеку;

встановлене ПЗ містить помилки. Проте установка "патчів" від постачальників може призвести до непередбачених результатів. Правила, що регламентують цю сферу, повинні вводити процедури тестування і вимагати встановлення виправлень, які стосуються захисту, до встановлення всього ПЗ;

незалежно від того, наскільки часто тестується ПЗ, може виникнути необхідність вивантажити з працюючої системи встановлене раніше ПЗ або "патчі". У правила керування конфігурацією необхідно включити вимогу як щодо інсталяції, так і щодо "відкату" до попередньої версії.

4. Стороння розробка:

стороннє ПЗ становить потенційну загрозу безпеці – вжити заходи контролю цілісності ПЗ;

вимога сумісності ПЗ із засобами керування безпекою ОС – розробити правила, де вказати, щоб в угодах із сторонніми організаціями містилися умови продажу та поширення розробленого ПЗ.

5. Питання інтелектуальної власності:

незалежно від того, хто займається розробкою, кінцевий результат вважається інтелектуальною власністю організації. Програми повинні розглядатися як цінні ресурси, що належать організації.

Порядок впровадження і контролю виконання політики безпеки

1. Тестування й ефективність правил [72]:

у цьому розділі правила охоплюють процеси збору статистики та складання звітів;

керівництво повинне заохочувати проведення навчання з питань безпеки, щоб кожен співробітник організації розумів правила безпеки та їх вплив на виробничі процеси;

включити положення про звичайні заходи, використовувані для тестування правил на їх ефективність.

2. Публікація правил:

регламентувати публікацію документів і записати вимоги щодо повідомлення про терміни публікації;

вказати, хто відповідатиме за цю роботу.

3. Моніторинг, засоби керування й міри покарання:

визначення прав організації щодо спостереження;

правила керування затверджують право організації на впровадження алгоритмів, які дозволяють вбудувати в систему певні засоби керу-

вання. Крім того, необхідно визначити склад осіб, які займатимуться адмініструванням і тестуванням цих засобів керування;

затвердити розроблені інструкції за призначенням покарань. Вони не повинні викликати питань про те, чи має організація право застосовувати заходи покарання при порушеннях правил безпеки;

правила повинні охоплювати незаконну діяльність, здійснювану внутрішніми користувачами і зовнішніми зловмисниками.

4. Обов'язки адміністраторів:

ці правила охоплюють питання адміністративного узгодження та впровадження, які не входять у сферу адміністративного керування;

визначають порядок розриву трудової угоди з організацією;

встановлюють коло осіб, які несуть відповідальність за своєчасне анулювання права доступу, звільнення ресурсів, виділених користувачу, виявлення в призначених для користувача ресурсах порушень безпеки та інших помилок осіб, а також за архівне зберігання призначених для користувача файлів та інших даних.

5. Міркування щодо реєстрації подій:

перевірка журналів аудиту, які створюються в системі і в програмах;

у журналах фіксуються всі операції, які користувачі виконують у системі або мережі, а також фіксуються всі помилкові та успішні спроби доступу до системи;

правила реєстрації є досить складними, оскільки неможливо скласти загальне формулювання, відповідне для будь-якої конфігурації системи. Напевно, непрактично реєструвати кожну операцію, що виконується в комп'ютерній системі, але необхідно забезпечити підтримку сервісних систем, які обслуговують бази даних;

описати порядок обробки інформації з журналів;

правила оновлення журналів можуть змінюватися залежно від роду діяльності організацій, а також від різновиду журналів.

6. Звітність про порушення безпеки:

звіти про інциденти можуть приходити з декількох джерел. Проблеми із захистом виявляють адміністратори, і для того, щоб користувачі могли фіксувати порушення, вони повинні мати правила, які визначають, як це робити;

встановлюються вимоги до звітності адміністраторів і користувачів;

у правила роботи з відкритими широкодоступними звітами необхідно включити методи розділення інформації, яку інформацію вважати достовірною, а яку перевіряти;

після повідомлення про інцидент збираються відповідні дані, і застосовуються правові санкції, які базуються на цьому повідомленні. Недостатньо просто повідомити про те, що щось відбулося. Якщо під час розслідування інциденту встановлено, що потрібно застосувати заходи покарання, які можуть обмежуватися дисциплінарними заходами або застосуванням заходів, передбачених законодавством, то в правилах повинні бути описані вимоги щодо обробки цих доказів.

7. Міркування, що стосуються дій після вчинення комп'ютерних злочинів: проконсультуватися з відповідними підрозділами правоохоронних органів на предмет вимог за поданням доказів.

Порядок перегляду політики безпеки

1. Періодичний перегляд правил документів:

певних рекомендацій з приводу того, як часто потрібно переглядати правила, не існує. Проте рекомендується, щоб цей термін був у межах від шести місяців до одного року;

включити вимогу щодо створення тимчасової комісії при терміновій необхідності внесення у правила значних змін.

2. Підстави для перегляду:

інформація, зібрана в процесі аналізу;

дані, зібрані в процесі впровадження правил і процедур, створених на базі цих правил;

інформація, зібрана в процесі аналізу ризиків і аудиту.

3. Комісія з перегляду правил:

в ідеалі комісія з перегляду правил повинна складатися з представників усіх зацікавлених сторін, які були задіяні для розробки правил.

Представлена модель оформлення ПІнБ не є суворою. Конкретна ПІнБ організації, природно, буде ширшою і повинна зважати на специфіку функціонування СКІ організації.

9.2. Моделі систем безпеки

Відповідальність за ІБ несе її керівник, що делегує цю відповідальність одному з менеджерів. Звичайно ці функції виконує директор з ІБ (CISO) або директор з безпеки (CSO), іноді директор (CIO) інформаційної служби. Пропонується розроблений автором повний класифікатор типів

(видів) осіб, що приймають рішення (табл. 9.1), відміною особливістю якого є одночасне урахування ієрархічної взаємозалежності існуючої вітчизняної та зарубіжної законодавчої бази на основі де-факто і де-юре ознак, що дозволило отримати відповідності посадам у державному класифікаторі професій [82]. При розробці та використанні ПІнБ [72] необхідно враховувати рекомендації: витрати на забезпечення ІБ не повинні перевищувати вартості об'єкта, що захищається, або величину збитку, що може бути нанесений внаслідок атаки на об'єкт, що захищається; необхідно визначити розмір такого збитку.

Таблиця 9.1

Класифікатор типів (видів) осіб, що приймають рішення

Абревіатура	Повна назва	Опис	Відповідність у державному класифікаторі професій [82]
1	2	3	4
CISO	Chief Information Security Officer	Посадова особа, що відповідає за інформаційну безпеку в межах підприємства	2414 – Професіонали з питань безпеки підприємств, установ та організацій
CAO	Chief Accounting Officer	Співробітник, що відповідає за спостереження за всіма аспектами бухгалтерських процесів в організації	3433 – Бухгалтери та касири-експерти. 1231 20656 – Головний бухгалтер
CAO	Chief Administrative Officer	Співробітник, що відповідає за управління приватними, суспільними або урядовими корпораціями	1210.1 – Генеральний директор (голова, президент, інший керівник) об'єднання підприємств (асоціації, корпорації, концерну, радіокомпанії, телекомпанії, телерадіокомпанії, теле- та радіо-інформаційного агентства та ін.)
CAO	Chief Analytics Officer	Посадова особа, що відповідає за аналіз даних у межах організації	4113 – Оператори із збору даних
CCO	Chief Channel Officer	Посадова особа, що відповідає разом із партнером за весь непрямий дохід в організації	1231 20656 – Головний бухгалтер
CCO	Chief Compliance Officer	Посадова особа, що відповідає за складання договорів, врегулювання проблем у межах організації	2441.2 25359 – Економіст з договірних та претензійних робіт
CCO	Chief Communications Officer	Посада начальника зв'язку й/або радника з суспільних питань в організації	2443.2 – Експерт із суспільно-політичних питань

Продовження табл. 9.1

1	2	3	4
CDO	Chief Data Officer	Корпоративна посадова особа, менеджер на підприємстві, що відповідає за обробку й пошук даних	4113 – Оператори із збору даних
CEO	Chief Executive Officer	Звичайно старша корпоративна посадова особа або адміністратор, що завідує загальним управлінням корпорації, компанії, організації або агентством	1210.1 – Директор (начальник, інший керівник) підприємства
CFO	Chief Financial Officer	Управляє фінансовими процесами на підприємстві	1231 – Директор фінансовий
CIO	Chief Information Officer	Глава інформаційних технологій в організації	2433.2 – Професіонали в галузі інформації та інформаційні аналітики
CMO	Chief Marketing Officer	Посадова особа, що відповідає за продажі в організації	3421 – Брокери (посередники) з купівлі-продажу товарів
GIO	Geospatial Information Officer	Глава інформаційних технологій у цивільних, ділових, державних і військових організаціях	2433.2 – Професіонали в галузі інформації та інформаційні аналітики
CLO	Chief Learning Officer	Старша корпоративна посадова особа, що вивчає управління корпорації або агентства	2447 – Професіонали в сфері управління проектами та програмами
CLO	Chief Legal Officer	Старша корпоративна посадова особа, що відповідає за виконання юридичних справ корпорації або агентства	1231 24157 – Начальник юридичного відділу
CNO	Chief Networking Officer	Посадова особа, що відповідає за мережні зв’язки в організації або підприємстві	3119 21740 – Диспетчер підприємства (району) мереж
CPO	Chief Procurement Officer	Виконавча роль співробітника спрямована на керування поставками для підприємства	1237.1 20936 – Головний фахівець з автоматизованих систем керування
CRO	Chief Risk Officer	Посадова особа, що відповідає за аналіз ризиків на підприємстві	2433 – Професіонали в галузі інформації та інформаційного аналізу
CSO	Chief Strategy Officer	Посадова особа, що відповідає за створення, виконання та підтримку стратегічних ініціатив у корпорації	1475.4 – Менеджер (управитель) з логістики
CTO	Chief Technology Officer	Посадова особа, діяльність якої спрямована на рішення наукових і технічних питань в організації	2414.1 – Науковий співробітник (безпека підприємств, установ та організацій)
CD	Creative Director	Посадова особа на підприємстві рекламної діяльності або художнього виробництва	245 – Професіонали в галузі художньої творчості 1234 21073 – Головний художник (реклама)

Закінчення табл. 9.1

1	2	3	4
ED	Executive Director	Старший менеджер або виконавча посадова особа організації, компанії чи корпорації	14 – Менеджери (управителі) підприємств, установ, організацій та їх підрозділів
MD	Managing Director	Посада, що використовується для президента компанії (об'єднаної компанії)	1210.1 – Генеральний директор (голова, президент, інший керівник) об'єднання підприємств (асоціації, корпорації, концерну, радіокомпанії, телекомпанії, телерадіокомпанії, теле- радіоінформаційного агентства та ін.)

У рамках підходу до ІБ як стану, який обумовлений впливом зовнішнього середовища, слід зазначити ресурсно-функціональну модель (РФМ) [100]. Автори цього підходу ІБ розглядають як "стан найбільш ефективного використання корпоративних ресурсів для запобігання загроз і забезпечення стабільного функціонування підприємства в цей час і в майбутньому" [100, с. 38]. Із цією метою Є. Олейников розглядає сукупність процесів, що протікають в організації, з усіма їхніми характерними рисами й взаємозв'язками, які становлять єдину родинну групу з погляду їхньої функціональної ролі в забезпеченні ІБ й, разом узяті, відіграють важливу роль у забезпеченні ІБ. У РФМ як основні напрямки ІБ розрізняють сім функціональних складових: інтелектуально-кадрову, фінансову, техніко-технологічну, політико-правову, екологічну, інформаційну й силову [100, с. 39].

Окремо необхідно згадати про моделі СІБ, які можна назвати вузькофункціональними. Мова йде про розгляд СІБ з позиції окремого аспекту її діяльності. Так, висловлюється думка, що найважливішим напрямком формування СІБ є створення діючого механізму фінансової безпеки. Обґрунтовується, що облік є однією з основних функцій керування, спрямованою на забезпечення ІБ, і саме облік виключає можливість прямих розкрадань без установлених законом наслідків, створює інформаційні умови для здійснення контролю доцільності й законності використання ресурсів у превентивному, поточному й наступному режимах і сприяє запобіганню реалізації загроз, які знижують економічну стабільність підприємства.

Безумовно, розробка вузькофункціональних моделей необхідна, тому що дозволяє провести всебічні й глибокі дослідження обраного ас-

пекту діяльності підприємства, прикладом чому і є показ конкретних шляхів й способів забезпечення ІБ в тій або іншій сфері його діяльності. Всім вузькофункціональним моделям до забезпечення ІБ властивий один дуже серйозний недолік. Автори цих моделей найчастіше виходять із різного розуміння ІБ. У цьому випадку спроби будь-яким чином об'єднати вузькофункціональні моделі СІБ заздалегідь приречені на невдачу. Відсутність єдиного розуміння ІБ може значно знизити результативність вузькофункціональних моделей.

Аналіз розглянутих підходів до проблеми ІБ дозволяє зробити наступні висновки. ІБ складається з декількох функціональних складових, які для кожного конкретного підприємства можуть мати різні пріоритети залежно від характеру існуючих загроз. Основним фактором, що визначає стан ІБ, є володіння підприємством стійкими конкурентними перевагами. Ці переваги повинні відповідати цілям планування стратегічного управління підприємством.

Модель ECMA. Модель ECMA [190] розроблена 9-ою технічною групою 32-го технічного Комітету (TG9/TC32) ECMA (European Computer Manufacturers Association – Асоціація європейських виробників комп'ютерів). Вона одержала назву TR/46 (Technical Report) та була опублікована у липні 1988 року. Вона становить абстрактну модель, усередині якої визначаються стандарти безпечної взаємодії розподілених систем. Основними висновками цього документа є: стандарти безпеки не повинні залежати від обраної політики ІБ; підсистема безпеки повинна розпізнавати різні області захисту, представлені різними адміністраторами.

Компоненти моделі ECMA (рис. 9.1) створюють три кільця захисту. Перше кільце відокремлює користувачів від СІБ. Сама розподілена система перебуває усередині першого кільця захисту й складається з об'єктів, які є суб'єктами керування безпекою. Друге кільце безпеки оточує кожний з об'єктів, що входять до складу моделі. Це означає, що всі взаємодії об'єктів, що здійснюються через інфраструктуру, контролюються. Третє кільце безпеки оточує внутрішні складові кожного об'єкта (дані й здатність обчислень). Модель дозволяє об'єктам мати своє внутрішнє керування доступом, забезпечуючи об'єкти необхідною інформацією й додатковими послугами.

Ключова концепція моделі безпеки полягає у використанні інформації з обмеженим доступом про повноваження, вона генерується пев-

ними службами безпеки у відповідь на автентифіковані запити до них і потім використовується іншими службами. Інформація про повноваження

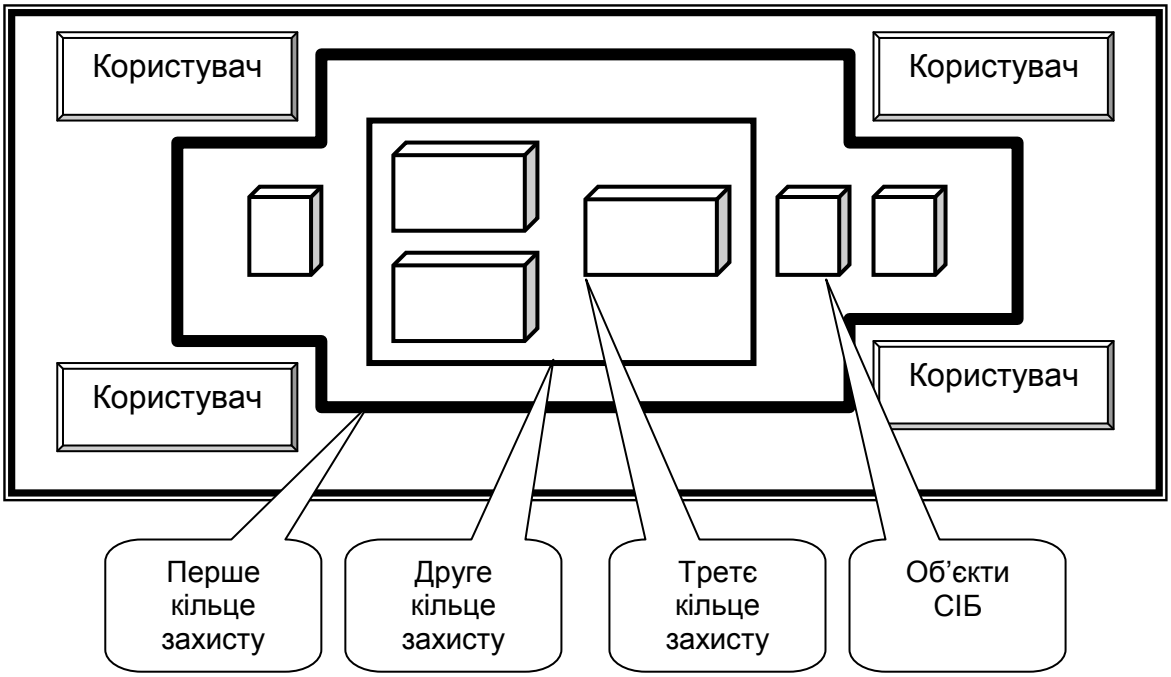


Рис. 9.1. **Компоненти моделі ECMA**

є засіб, за допомогою якого відомості про повноваження (security knowledge) поширюються усередині розподіленої системи. Це означає, що ця інформація повинна бути надійною, а також що її можна легко передавати будь-якому, навіть незахищеному об'єкту. Класи служб ІБ, які передбачені в моделі ECMA, представлені на рис. 9.2.

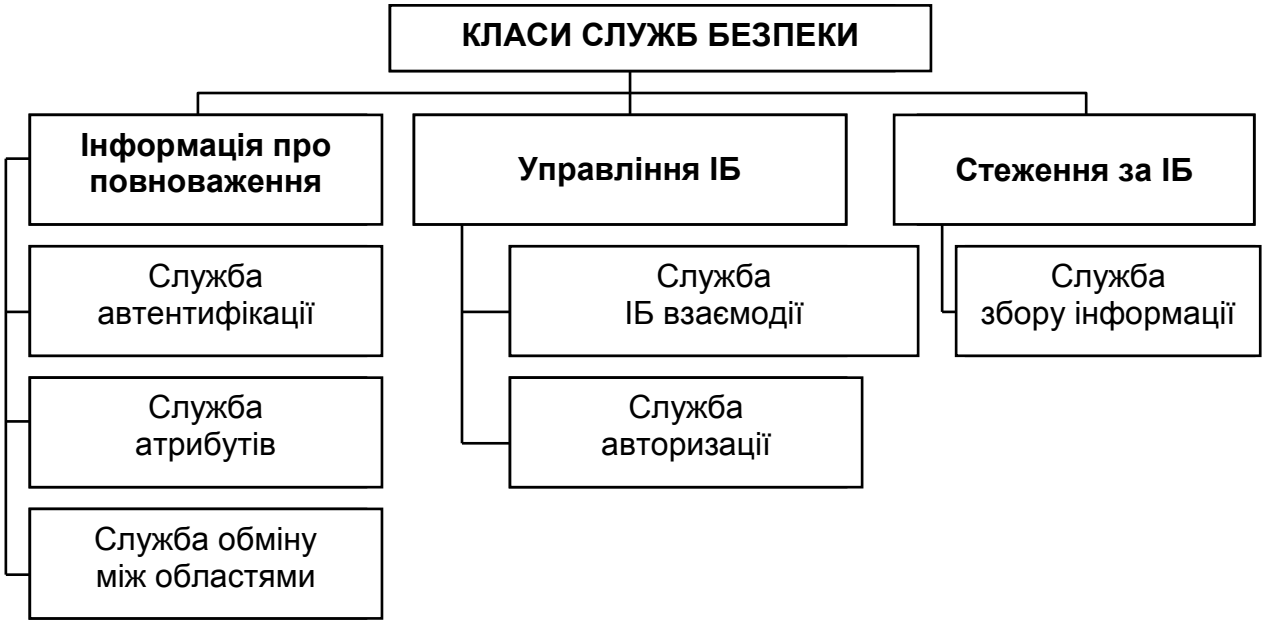


Рис. 9.2. **Класи служб ІБ**

Ключові аспекти симетричної моделі (табл. 9.2) забезпечують розуміння й реалізацію захисту підприємства й управління СІБ.

Симетрична модель СІБ. Дана модель може бути використана як для загальної концепції ІБ, так і для розроблювальної СІБ. Схема вибору основних засобів і способів для побудови СІБ наведена на рис. 9.3.

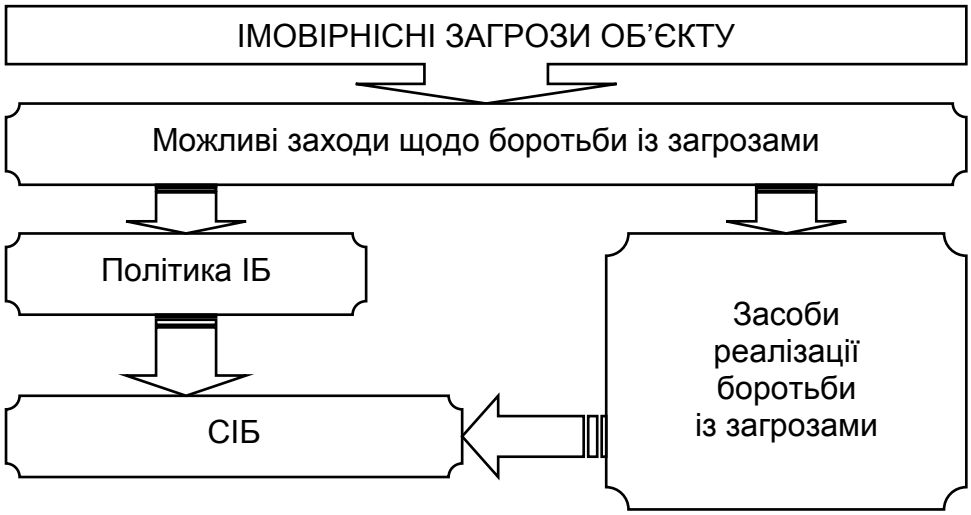


Рис. 9.3. **Схема вибору способів та засобів ІБ**

Реалізується симетрична модель за допомогою технології Intranet.

Загальна модель СІБ. Запропонована автором загальна модель СІБ побудована на основі моделі, визначеної в роботі [66]. З об'єктом, що є складовою частиною СІБ, зв'язана множина дій, у тому числі й несанкціонованих – економічні загрози, фінансові втрати. Між об'єктом (***O***) і загрозою (***P***) існує множина відносин, яка утворює граф, у якому дуга $<o_n, p_n>$ існує тоді й тільки тоді, якщо p_n є засобом доступу до об'єкта o_n (рис. 9.4), який описує модель СІБ в загальному вигляді. Слід зазначити, що зв'язок між p_n і o_n характеризується типом "один до багатьох", тобто одна погроза покриває множину об'єктів, у свою чергу, один об'єкт уразливий від більш ніж однієї загрози. Наявність дуги типу $<p_n, o_n>$ характеризує незахищений об'єкт СІБ.

Метою СІБ є створення своєрідного бар'єру, що охороняє об'єкти від можливих загроз. Для цього вводиться множина S, що включає засоби забезпечення безпеки СІБ. Будь-яке відношення $s_m \in S$ повинне усунути дугу $<p_n, o_n>$ у загальному графі й забезпечити протистояння спробам несанкціонованого доступу або виникнення економічних загроз. Можливість протистояння (опору) СІБ є основною характеристикою елементів $s_m \in S$. Дана множина перетворює дугу $<p_n, o_n>$ у форму:

$$<p_i, s_j> \cup < s_j, o_i>. \qquad (9.1)$$

Таблиця 9.2

Ключові аспекти симетричної моделі СІБ

Користувачі	Доступ до внутрішніх ресурсів	Доступ в Інтернет	Завантаження в мережу	Завантаження з мережі	Електронна пошта
Співробітники в офісі	Обмеження доступу (за необхідністю). Необхідність шифрування. Необхідність запису на носії. Розмежування доступу до НЖМД (тільки з робочих станцій)	Обмеження за IP-адресою	Доступ до всієї інформації компанії. Обмеження за IP-адресою. Обмеження за змістом	Завантаження будь-якої інформації. Загальна заборона завантаження. Обмеження за IP-адресою. Обмеження за змістом	Обмеження за змістом (вхідної й вихідної кореспонденції). Обмеження за IP-адресою (адресата й джерела)
Вилучені робочі місця	Ідентифікація вилученого користувача. Обмеження доступу	Обмеження доступу за IP-адресою	Доступ до всієї інформації компанії. Обмеження за IP-адресою	Обмеження за IP-адресою. Обмеження за змістом	Обмеження за змістом (вхідної й вихідної кореспонденції)
Співробітники поза офісом (в інших офісах компанії)	Автентифікація віддаленого користувача перед здійсненням доступу	Обмеження доступу за IP-адресою	Доступ до всієї інформації компанії. Обмеження за IP-адресою. Обмеження за змістом	Завантаження будь-якої інформації. Загальна заборона завантаження. Обмеження за IP-адресою. Обмеження за змістом	Обмеження за змістом (вхідної й вихідної кореспонденції). Обмеження за IP-адресою (адресата й джерела)
Постачальники, ділові партнери, клієнти	Доступ тільки до спеціально відведених областей для виробників, партнерів і клієнтів	Незастосовне	Завантаження будь-якої інформації. Загальна заборона завантаження. Фільтрація	Завантаження будь-якої інформації. Загальна заборона завантаження. Фільтрація	Обмеження за змістом (вхідної й вихідної кореспонденції). Обмеження за IP-адресою (адресата й джерела)
Потенційні клієнти	При відкритому доступі інтрамережа ізольована. Ідентифікація користувача не потрібна	Незастосовне	Завантаження будь-якої інформації. Загальна заборона завантаження. Фільтрація	Завантаження будь-якої інформації. Загальна заборона завантаження. Фільтрація	Обмеження за змістом (вхідної й вихідної кореспонденції). Обмеження за IP-адресою (адресата й джерела)

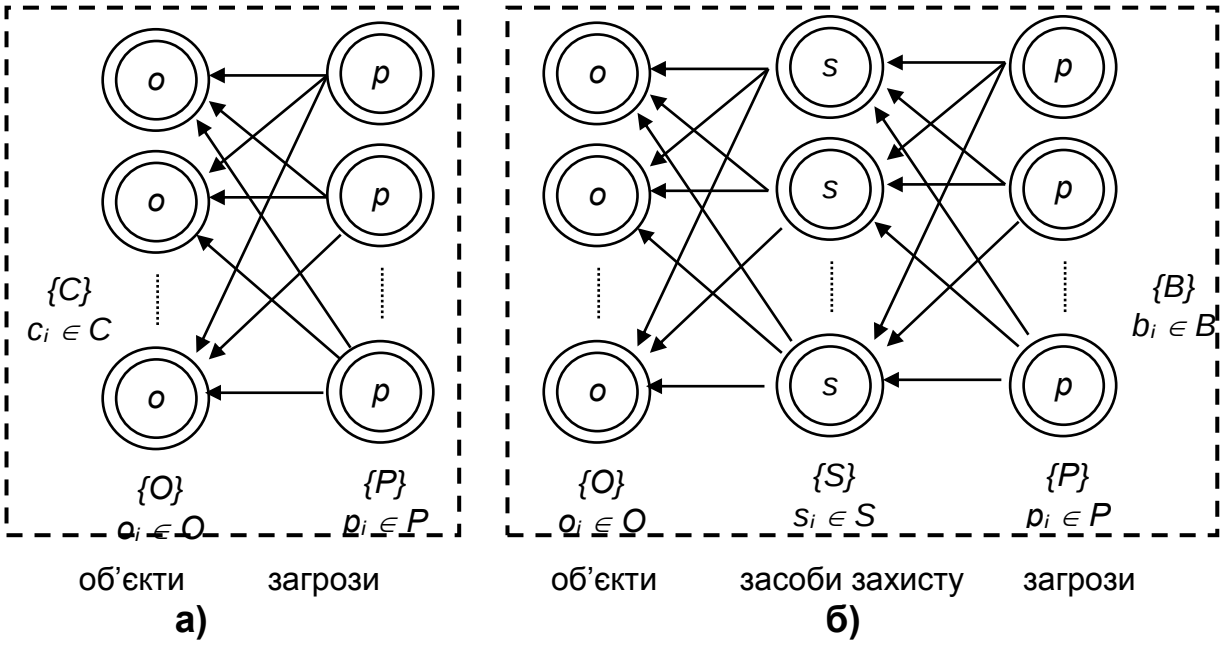


Рис. 9.4. **Загальна модель СІБ: а) без СІБ; б) з використанням СІБ**

Модифікацією даної моделі є модель, що складається із такої множини:

$$S = <O, P, S, C, B>, \qquad (9.2)$$

де O – множина захищених об'єктів ($o_i \in O$);

P – множина загроз ($p_i \in P$);

S – множина засобів захисту в СІБ ($s_m \in S$);

C – множина уразливих місць (відображення PxO на множині $C_i = <p_i, o_i>$ – канали проникнення та витоку інформації);

B – множина фільтрів (відображення CxS або $PxSxO$ на множині $B_n = <p_i, s_j, o_i>$).

У свою чергу елемент множини фільтрів B описується трьома компонентами. Наприклад, дуга b_2 $<p_2, s_2, o_2>$ забезпечує протистояння погрозі p_2 можливості доступу до об'єкта o_2 за допомогою засобу СІБ s_2 (рис. 9.4б) і характеризує ймовірність появи загрози – p, розмір загрози при проникненні до об'єкта – r, ступінь опору погрозі – k.

Таким чином, на основі запропонованої загальної моделі СІБ можливо отримання більш деталізованих моделей.

Моделі СІБ *з повним перекриттям.* Для якої введемо поняття захищеності СІБ – ступінь адекватності реалізованих у ній механізмів захисту інформації з обмеженим доступом ризикам, пов'язаним із здійсненням

погроз ІБ. Під погрозами інформації з обмеженим доступом розуміється можливість порушення властивостей інформації з обмеженим доступом: конфіденційність, цілісність та доступність.

Основою формального опису СІБ вважається модель з повним перекриттям, у якій розглядається взаємодія "області погроз", "області, що захищаються" – ресурси СІБ та "системи захисту" – механізми безпеки СІБ [69]. Тобто, маємо:

$T = \{t_i\}$ – множина погроз безпеки, $O = \{o_j\}$ – множина об'єктів (ресурсів) СЕБП, $M = \{m_k\}$ – множина механізмів безпеки.

Елементи цих множин перебувають між собою в певних відносинах, які властиво й описують СІБ. Для опису СІБ використовується звичайна модель графа (рис. 9.5).

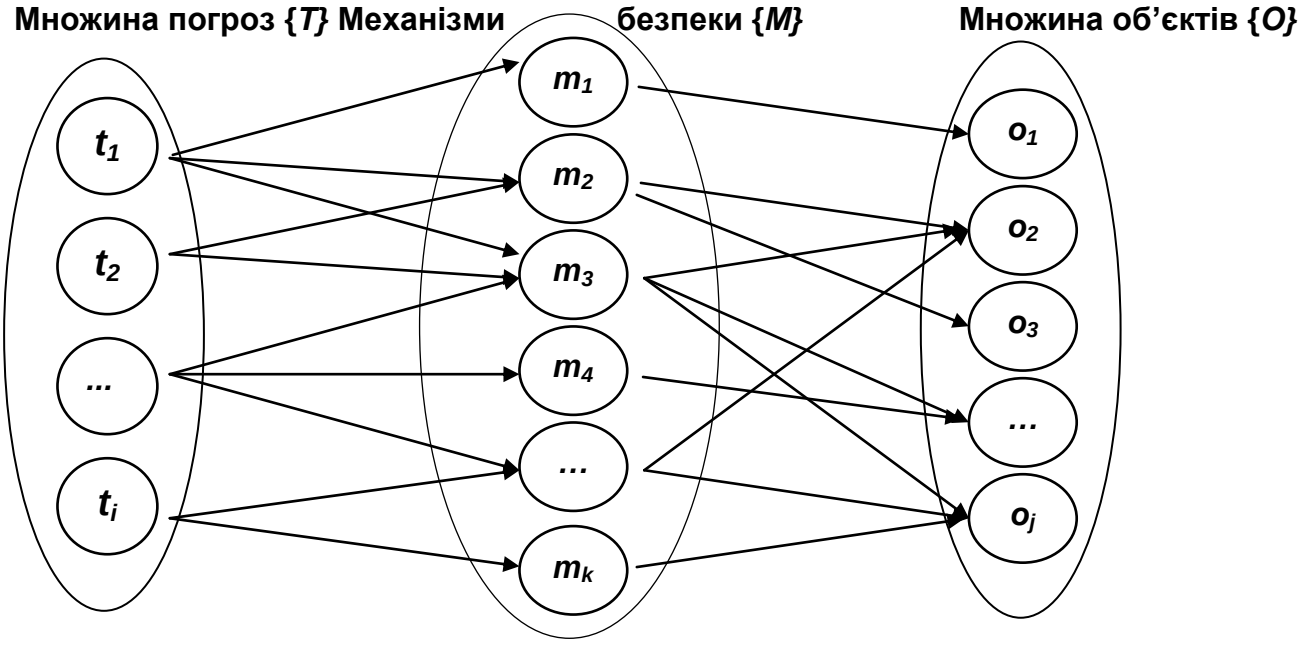


Рис. 9.5. **Модель графа Q_2 СІБ з повним перекриттям**

Множина відносин типу погроза-об'єкт утворює дводольний граф $Q_1\{T, O\}$. Мета побудови полягає у тому, щоб перекрити всі можливі ребра в графі. Це досягається введенням множини $\{M\}$. У результаті отримуємо тридольний граф $Q_2\{T, M, O\}$.

Подальший розвиток моделі вимагає введення множин: $\{V\}$ – множина уразливостей, обумовлена підмножиною декартового добутку $T \times O$: $vr = <t_i, o_j>$. Таким чином, під уразливістю СІБ розуміється можливість здійснення погрози t_i відносно об'єкта o_j (на практиці під уразливістю СЕБП розуміють не саму можливість здійснення погрози безпеки, а ті властивості СІБ, які сприяють успішному здійсненню погрози, або викорис-

товується зловмисником для здійснення погрози); *{B}* – множина фільтрів, обумовлена декартовим добутком $V \times M$: $bl = \langle t_i, o_j, m_k \rangle$, що представляють собою шляхи здійснення погроз безпеки, які перекриті засобами захисту.

У результаті одержуємо модель СІБ, що складається з п'яти множин: Q_3 *{T, O, M, V, B}*, й яка описує СІБ з урахуванням уразливостей (рис. 9.6).

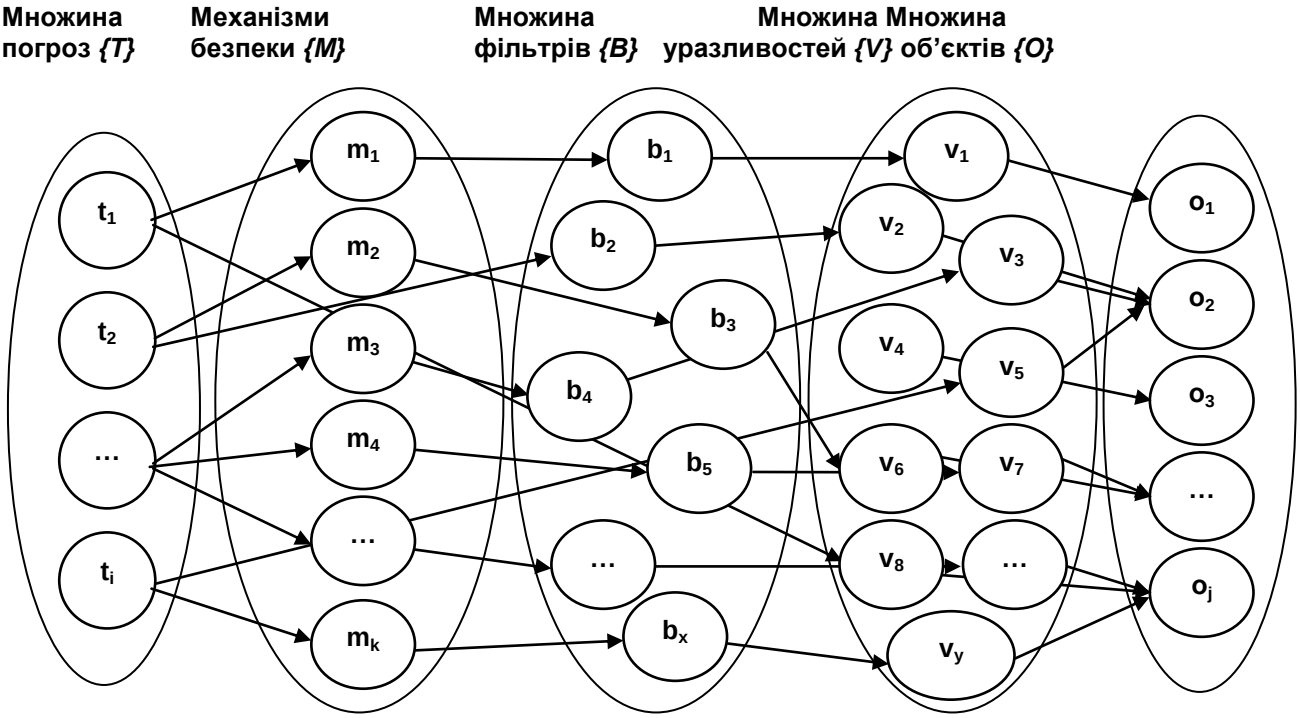


Рис. 9.6. **Модель з повним перекриттям, що містить уразливості**

Концептуальна модель СІБ. СІБ є однією з таких, призначення якої полягає в організації забезпечення нормального функціонування підприємства й запобіганні (усуненні) можливих збитків (втрат, як описано у роботі автора [76]), які можуть відбутися в результаті реалізації різних загроз, а в остаточному підсумку – запобіганні загрози банкрутства підприємства. СІБ становить сукупність (комплекс) заходів і засобів, використання яких регламентується відповідними правовими актами (державними, регіональними, власними).

Найважливішим показником функціонування СІБ (index of functioning of system of economic security, *IFses*) виступає отриманий (досягнутий) рівень ІБ при використанні своїх корпоративних ресурсів. При цьому *IFses* є

комплексним (інтегральним) показником і може бути визначений такою формулою:

$$IF_{ses} = \sum_{i=1}^{n} K_i \cdot v_i, \qquad (9.3)$$

де K_i – частковий функціональний показник (ЧФП) ІБ;

v_i – питома вага ЧФП, причому $\sum v_i = 1$;

n – кількість ЧФП, що враховуються їхня сукупність повинна забезпечити об'єктивність визначення IF_{ses}.

Матрична модель СІБ. Метою дослідження ІБ є формалізація СІБ у вигляді матричної моделі, що дозволить надалі використовувати її для проведення розрахунків економічної ефективності реалізації ПІнБ у зручній і наочній формі.

Для досягнення поставленої мети за основу була використана концептуальна модель СІБ з усіма властивостями і перевагами. Однак для проведення економічних розрахунків параметрів і характеристик дана модель не зовсім зручна. Тому для усунення цього недоліку на основі розробленої "стільникової" концептуальної моделі пропонується матрична модель СІБ [69], що дозволить одержати реальні числові оцінки ефективності її використання у підприємницькій діяльності.

Також був введений основний показник функціонування СІБ – IF_{ses} (9.3), що визначає досягнутий рівень ІБ при використанні корпоративних ресурсів. Причому питома вага ЧФП ІБ розраховується на основі оцінки сукупних збитків за функціональними складовими ІБ.

У результаті була отримана множина, що описується виразом (9.4). Якщо представити дані компоненти у вигляді відповідних розмірностей, то одержимо шестивимірну інформаційну матрицю IM_{ses}. Тоді кількість осередків у матриці буде дорівнювати добутку розмірностей для кожної складової:

$$IM_{ses} = R_B \times R_U \times R_C \times R_R \times R_S \times R_P, \qquad (9.5)$$

де $R_B = 4$ (розмірність множини баз, що забезпечують виконання основних функцій СІБ);

$R_U = 8$ (розмірність множини загроз підприємства);

$R_C = 10$ (розмірність множини цілей функціонування СІБ);

$R_R = 5$ (розмірність множини ресурсів, які використовуються у контурі життєвого циклу СІБ, що запропонований у роботі автора [59]);

R_S = *4* (розмірність множини напрямків або сфер діяльності підприємства, необхідних для обліку в СІБ);

R_P = *6* (розмірність множини втрат у діяльності підприємства, необхідних для обліку в СІБ).

Таким чином, одержимо розмірність $IM_{ses} = 4 \times 8 \times 10 \times 5 \times 4 \times 6 = 38\,400$. Саме стільки можливих описів (станів) підприємства можна одержати на основі "стільникової" концептуальної моделі СІБ [66]. Наприклад, стан моделі СІБ, що описується координатами

$$IM_{ses}\ (b_1 = 0.9;\ u_3 = 0.7;\ c_6 = 0.5;\ r_5 = 0.1;\ s_1 = 0.5;\ p_6 = 0.9), \qquad (9.6)$$

буде мати такий стан: на підприємстві повністю виконуються всі НА законодавчої бази держави; виявлення фактів витоку інформації з обмеженим доступом на підприємствв відбувається із частотою 1 раз/квартал; підприємство не має власного ВК і потреби в наборі персоналу не задовольняються, тому підприємство періодично проводить РППК; лише деякі об'єкти підприємства перебувають під обліком і надійно захищені; підприємство втрачає в середньому до 100 грн за тиждень при існуючих екологічних порушеннях.

Таким чином, при використанні матричної моделі СІБ досить легко одержати формалізоване визначення рівня ІБ у вербальному вигляді. У свою чергу, сумарну кількість можливих станів цілком дозволить урахувати всі можливі варіанти рівнів розвитку часткових показників СІБ. Крім того, "стільникова" модель СІБ може давати якісну оцінку кожної складової окремо.

Маючи подібну інформацію й реальні методики (наведені у роботі автора [82]) використання її на практиці будь-який підприємець зможе якісно й швидко управляти розвитком свого підприємства й забезпечити йому гідний конкурентоспроможний стан на сучасному ринку, а, отже, зможе забезпечити успіх своєї діяльності.

Якщо представити отриману матрицю у просторовому вигляді, то одержимо модель із 6 ступенями (рис. 9.7), на якої показані умовні координати для виразу (9.6).

Якщо проводити періодичний аудит СІБ, то можна в наочному вигляді побачити динаміку "руху" стану СІБ (матричної моделі) в 6-вимірній системі координат "стільникової" моделі СІБ (рис. 9.8).

У виді абстрактності подання в просторовому вигляді, отримані стани на рис. 9.9 представляються у вигляді ліній (зв'язок 2-х точок). Зміни координат станів показані у вигляді траєкторій кутових точок.

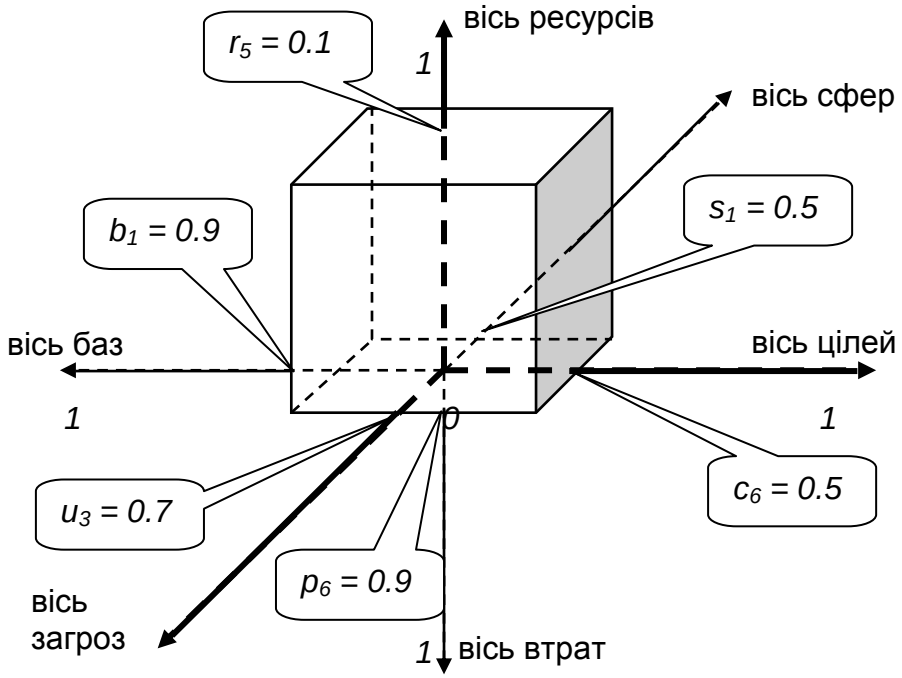


Рис. 9.7. **Відображення матричної моделі СІБ у 6-вимірній системі координат**

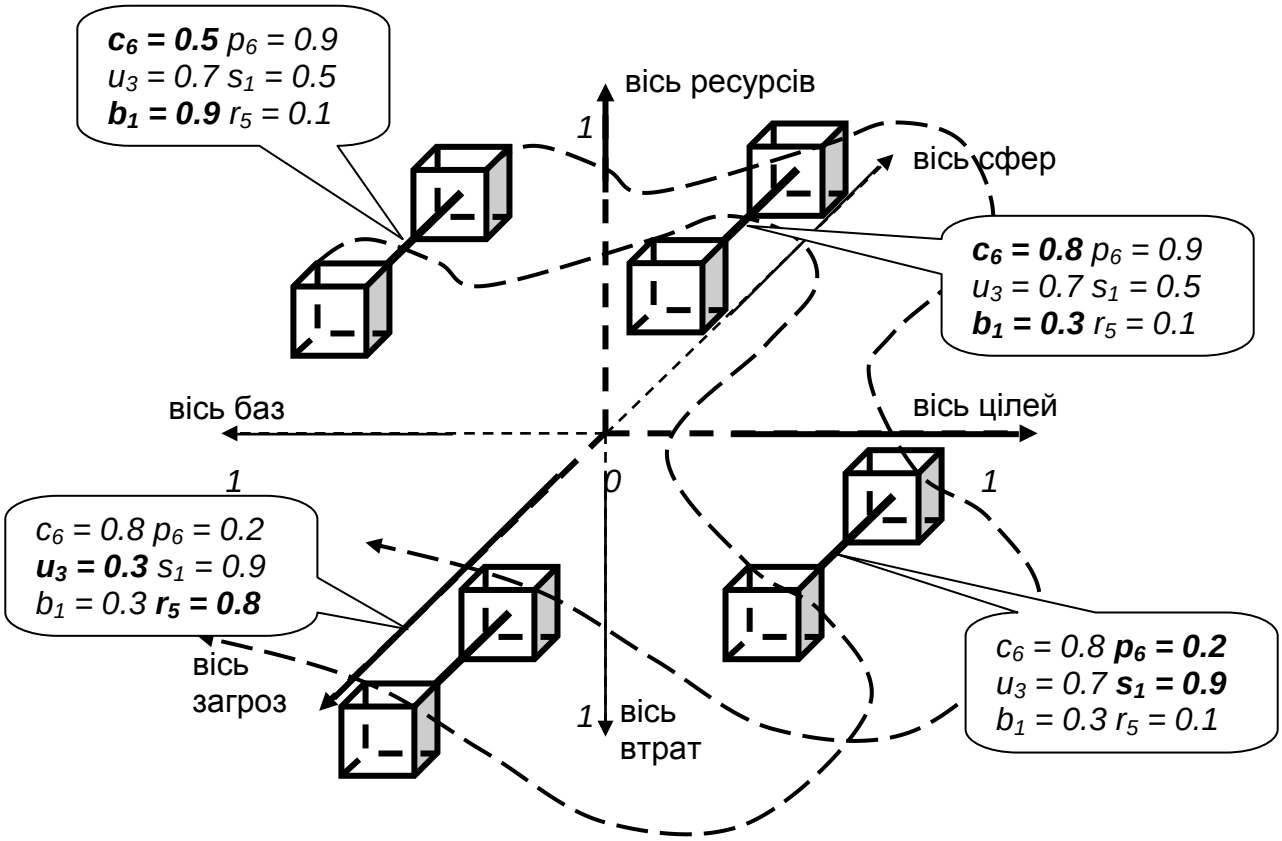


Рис. 9.8. **Динаміка "руху" (наведено пунктирною лінією) моделі СІБ в 6-вимірній системі координат**

Як відомо, у будь-якій матриці всі її елементи повинні бути пронумеровані. Аналогічно в матриці IMses всі елементи (осередку) мають свій номер з 6-ма координатами, які й визначать в остаточному підсумку стан СІБ. Дане подання в 6-вимірній системі координат варто розглядати як деяку абстракцію, не використовуючи основні правила геометрії у якості прикладу матриці IMses (табл. 9.3).

Таблиця 9.3

Приклад розміщення елемента матриці IM_{ses} (стану СІБ)

База	Погрози	Ресурси	$r_5 = 0.1$								$r_5 = 0.5$			
		Втрати	$p_6 = 0.1$				$p_6 = 0.9$				$p_6 = 0.7$			
		Сфери	$s_1 = 0.9$	$s_1 = 0.7$	$s_1 = 0.5$	$s_1 = 0.1$	$s_1 = 0.9$	$s_1 = 0.7$	$s_1 = 0.5$	$s_1 = 0.1$	$s_1 = 0.9$	$s_1 = 0.7$	$s_1 = 0.5$	$s_1 = 0.1$
$b_1 = 0.9$	$u_3 = 0.9$	$c_6 = 0.9$												
		$c_6 = 0.7$												
		$c_6 = 0.5$												
		$c_6 = 0.1$												
	$u_3 = 0.7$	$c_6 = 0.9$												
		$c_6 = 0.7$												
		$c_6 = 0.5$												
		$c_6 = 0.1$												
	$u_3 = 0.5$	$c_6 = 0.9$												
		$c_6 = 0.7$												
		$c_6 = 0.5$												
		$c_6 = 0.1$												
	$u_3 = 0.1$	$c_6 = 0.9$												
		$c_6 = 0.7$												
		$c_6 = 0.5$												
		$c_6 = 0.1$												

При цьому кожне знакомісце відповідає показнику однієї з розглянутих множин: IM_{ses} *(*b_1 *= 0.9; X; X; X; X; X)* – повністю виконуються всі нормативні акти на підприємстві; IM_{ses} *(X;* u_3 *= 0.7; X; X; X; X)* – виявлення фактів незнання інформації відбувається із частотою 1 раз/квартал; IM_{ses} *(X; X;* c_6 *= 0.5; X; X; X)* – підприємство періодично проводить рекрутинг персоналу й підвищення їхньої кваліфікації; IM_{ses} *(X; X; X;* r_5 *= 0.1; X; X)* – підприємство не має власного відділу кадрів, потреби в наборі персоналу не задовольняються; IM_{ses} *(X; X; X; X;* s_1 *= 0.5; X)* – деякі об'єкти підприємства перебувають під обліком і надійно захищені; IM_{ses} *(X; X; X; X; X;* p_6 *= 0.9)* – підпри-

ємство втрачає в середньому до 100 грн/тиждень (штрафи).

Таким чином, запропонована автором матрична модель СІБ має такі властивості:

1. Зв'язність: відстеження твердих зв'язків між окремими елементами матриці.

2. Аудитивність: можливість використання при первинному аудиті ІБ.

3. Технологічність: множина всіх осередків матриці дає повний технологічний опис СІБ.

4. Варіативність: отриману матричну модель легко можна підбудувати під існуючі стандарти.

5. Застосовність: запропонована модель при відповідній методиці дозволить у динаміці оцінити ефективність існуючої (розроблювальної) СІБ.

6. Використовуючи значення елементів матриці СІБ можна розробити реальні практичні рекомендації із забезпечення ІБ.

9.3. Методика розробки політики безпеки

Загальні відомості. Політика інформаційної безпеки (ПІнБ) є юридичним документом (поряд з уставом організації), прийнятим на підприємстві й затвердженому директором або радою директорів із відповідними юридичними реквізитами (підписом і печаткою). Розробляє ПІнБ адміністратор, хоча це не є його прямим обов'язком, і узгоджується з юристом (у плані коректності й відповідності законодавству) і може в окремих випадках із начальником відділу ІБ підприємства (не обов'язково) [72].

Загальним принципом ПІнБ на підприємстві є заборона всіх видів доступу, дій і операцій, які не дозволені явно в розробленій ПІнБ. Тобто, якщо немає спеціального дозволу на проведення конкретних дій або використання конкретних мережних ресурсів, то такі дії, або таке використання заборонені, а особи, які їх здійснюють, підлягають покаранню.

Звичайно, ПІнБ складається із двох основних частин:

1. Політика для роботи в окремій мережі.
2. Політика для роботи в міжмережному середовищі.

Щодо *реалізації ПІнБ* визначають межі відповідальності й звітності, описаної в наступних розділах. ПІнБ визначає відповідальних посадових осіб за реалізацію ПІнБ, до яких вона застосовна.

Область дії ПІнБ застосовна до всіх підрозділів підприємства її офісів, а також до всіх спонсорів і ділових партнерів. Підрозділам рекоменду-

ється уточнити загальні рекомендації в тій мірі, у якій вони застосовні до них, але доповнення до політики не повинні конфліктувати з основними рекомендаціями ПІнБ. У випадку суперечки щодо інтерпретації або реалізації локальної політики стосовно загального ПІнБ, останнє слово – за відділом безпеки підприємства. Відповідальність за виконання ПІнБ покладає на начальника служби безпеки й адміністратора підприємства й/або на інших осіб верхньої ланки керування. Уточнення й інтерпретації ПІнБ можуть бути отримані у відділі безпеки у випадках очевидного конфлікту між локальними вимогами й різними тлумаченнями положень основних ПІнБ.

Реалізація ПІнБ. Кожна посадова особа й службовець підприємства, що адмініструє або використовує мережні й інші ресурси, відповідає за суворе дотримання розробленої ПІнБ. Кожний користувач зобов'язаний повідомляти про підозрювані або реальні уразливі місця (загрози) у безпеці системи своєму безпосередньому керівнику (менеджерові) або адміністраторові. У підприємства є своя група залагоджування інцидентів із комп'ютерною безпекою (ГЗІКБ), що повинна повідомляти керівництво в обов'язковому порядку про основні інциденти, за яких відбулися компрометація, неправильне використання або псування інформаційних цінностей підприємства. Підрозділам (відділам) рекомендується організовувати свої локальні ГЗІКБ для більше швидкого виявлення уразливих місць у захисті та їхнього усунення. Хоча співробітники, що входять до ГЗІКБ, мають свої основні посадові обов'язки, питання безпеки мають пріоритет стосовно них. Керівники підрозділів повинні призначати своїх співробітників до складу ГЗІКБ при виникненні інциденту, і звільняти від основних обов'язків до кінця розслідування.

Опис політики. У цій частині ПІнБ зазначаються положення й критерії, які визначають її тією мірою, якою вона застосовна до кожного об'єкта й суб'єкта на підприємстві. Частина, що ставиться до мереж, включає критерії, які повинні бути виконані для Інтернет із погляду безпеки.

Мережі. Інтернет складається з мереж, тому ПІнБ рівною мірою застосовується до всіх мережних компонентів. Мережа, що не є частиною Інтернету, не має засобу захисту, повинна дотримувати вимог внутрішньої мережний ПІнБ. Така мережа не містить точки ризику і є захищеною.

Інтереси підприємства. Мережні ресурси підприємства існують лише для того, щоб підтримувати її діяльність. У деяких випадках важко провести риску між інтересами підприємства (службовими інтересами) та іншими інтересами. Система конференцій і електронної пошти Інтернет є

прикладами змішання інтересів підприємства й особистих інтересів співробітників щодо використання цих ресурсів. Підприємство розуміє, що спроби використання обмежень типу "тільки в інтересах підприємства" у цих випадках безглузді. Тому необхідно дати рекомендації, а не суворі вимоги щодо інформаційних ресурсів, які служать для вирішення завдань, що стоять не тільки перед підприємством. *Керівники відділів мають право ухвалити рішення щодо допустимості використання мережних ресурсів співробітниками для вирішення завдань, відмінних від службових, у тому випадку, якщо при цьому підвищується ефективність роботи даного співробітника.* З іншого боку менеджери повинні перешкоджати некоректному використанню мережних і інших ресурсів як для особистих цілей, так і для цілей відпочинку й розваги співробітників.

Принцип "знай тільки те, що ти повинен знати для роботи". Доступ до інформаційних цінностей підприємства не буде здійснений, якщо не виникне необхідності в такій інформації. Це означає, що критична інформація повинна бути захищена таким чином, щоб вона була **невідома** основній масі співробітників.

Розробка ПІнБ ведеться **тільки** після виходу відповідного наказу на підприємстві, де регламентуються права й можливості адміністратора на етапі розробки. При цьому в наказі на розробку ПІнБ повинен указуватися рівень доступу адміністратора до робочих місць користувачів і в інші приміщення, а також доступ до різних категорій інформації, наприклад, у режимі перегляду файлів і папок. Зверніть увагу, що доступ забезпечується до категорій інформації, а не до її змісту. У середньому на побудову ПІнБ на досить великому підприємстві повинно виділятися до 3-х місяців.

Увесь процес побудови ПІнБ можна розділити на 3 етапи:

1. Аналіз даних, інформації, цілей реалізації.
2. Розробка ПІнБ, результатом якої є юридичний документ.
3. Упровадження, зокрема, доведення обов’язків посадових осіб (під підпис), реєстрація у відділі кадрів та ін.

ПІнБ повинна реалізовуватися в не більше ніж трьох екземплярах, які відповідно зберігаються в юриста (копія), адміністратора й директора (копія й, до того ж, необов’язкова).

На першому етапі на кожному робочому місці користувача пропонується збирати таку інформацію:

1. Місце розташування або топологічна прив’язка вузлів мережі до схеми приміщення.

2. Характеристики приміщень, залів, будинків, поверхів і т. д.

3. Технологічні норми й нормативи щодо розміщення робочого місця користувача, наприклад, відстань монітора від протилежного монітора або користувача й т. д.

4. Параметри й характеристики ПК.

5. Список користувачів, що працюють на ПК і їхні права доступу.

6. Категорії інформації, використовуваної на робочому місці, що в підсумку повинна бути кваліфікована із прив'язкою до організаційно-штатної структури підприємства.

7. Типи груп користувачів, передбачуваних для використання в мережі, які обґрунтовуються й регламентуються в ПІнБ із обліком на подальше використання й розширення. При цьому адміністратору дозволяється додавання нових і зміна існуючих типів груп, пов'язаних із реорганізацією компанії.

Уся термінологія в ПІнБ повинна бути описана заздалегідь грамотно з юридичної й технічної точки зору. У ПІнБ має бути регламентована в окремому пункті її доля, наприклад, у випадку звільнення адміністратора ПІнБ втрачати свою юридичну чинність, оскільки адміністратор є її розроблювачем.

Обов'язки посадових осіб, що охоплюють усі сфери діяльності співробітника, регламентуються в ПІнБ в окремих розділах для кожної категорії. Тут указуються права, обов'язки, перелік заборонених операцій і дій, а також можливі види санкцій, застосовуваних до співробітника. При цьому перелік останніх указується в ПІнБ окремою статтею, з узгодженням керівництва. Наприклад, це може бути список штрафних санкцій у вигляді утримання коштів, залежно від міри порушення, а також вказівки на відповідні нормативні законодавчі акти для більш серйозних порушень.

Таким чином, політика мережної безпеки на підприємстві розподіляє відповідальність за її реалізацію й підтримку між конкретними посадовими особами. Вона визначає обов'язки кожного службовця компанії при використанні мережних і інших ресурсів і необхідності повідомляти про уразливі місця в системі безпеки. Вона також установлює, що загальною політикою є – **заборонено все, що явно не дозволено**. Тобто, якщо діяльність або вид доступу не можуть бути знайдені або визначені в цьому документі, то вони заборонені.

За доробку ПІнБ відповідає особа, що займається розробкою даного документа, у міру того, як потреба в безпеці й технології мережної взаємодії змінюються. Директиви, що втримуються в ПІнБ, повинні бути завжди інтерпретовані як наказ директора підприємства.

Методика побудови ПІнБ [72]

Побудову ПІнБ можна реалізувати таким алгоритмом.

1. На першому кроці необхідно скласти ОШС підприємства на підставі даних, наданих відділом кадрів, з узгодженням у керівництва. Дана ОШС буде основою для розробки логічної структури. ОШС наочніше за все встановити у вигляді схеми (Сх1) із зазначенням спрямованості підпорядкованості, наприклад (рис. 8.2).

2. На підставі Сх1 будується *перша* матриця інформаційних потоків ($М_{ип}$) і вузлів електронної обробки, що прив'язується до топологічної схеми мережі (табл. 9.4).

Таблиця 9.4

Матриця інформаційних потоків ($М_{ип}$) і вузлів електронної обробки

№ вузла / № вузла	**Вузол № 1**	**Вузол № 2**	**…….**	**Вузол № n**
Вузол № 1	Обробка документів	…….	…….	Доповідь начальникові
Вузол № 2	…….	…….	…….	…….
…….	…….	Обробка документів	…….	…….
Вузол № n	Доповідь начальникові	…….	…….	…….

3. На підставі матриці $М_{ип}$ робиться *друга* матриця, що описує топологічний зв'язок ($М_{тс}$) об'єктів і суб'єктів (фізичне з'єднання, реальне розташування вузлів, вікон, дверей, розташування робочих місць, габарити). Виноситься в додаток із грифом. При цьому вказується все використовуване мережне комунікаційне устаткування (рис. 9.9).

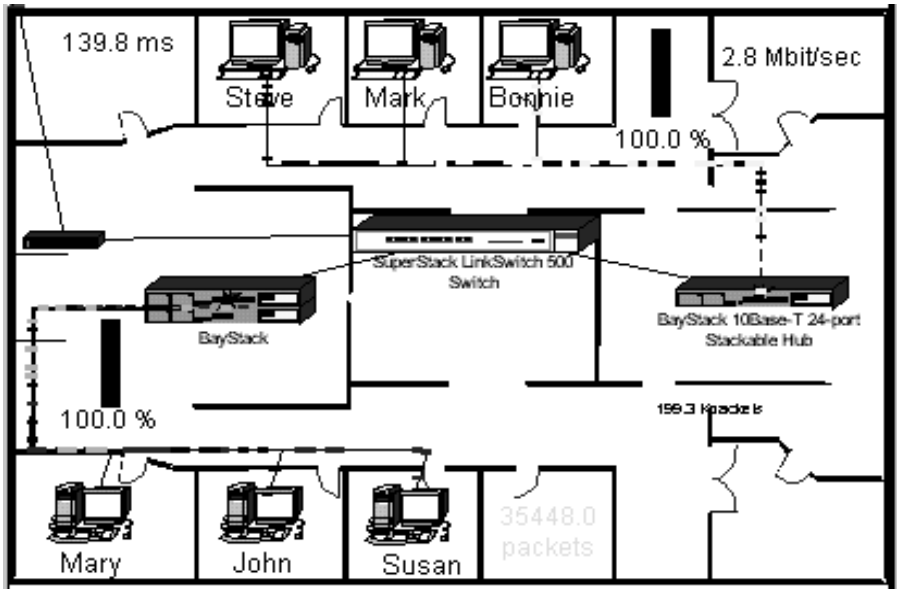


Рис. 9.9. **Матриця топологічного зв'язку**

4. *Третя* матриця створюється на 1-му етапі й називається матриця категорування типів інформації – $М_{ки}$. Це двовимірна матриця, де по одній осі вказуються всі типи інформації (комерційна, службова й ін.), по іншій – об'єкти, співробітники (табл. 9.5).

Таблиця 9.5

Матриця категорування типів інформації

Користувач / Категорія інформації	**Іванов С. В.**	**Петров С. В.**	**…….**	**Кавун С. В.**
Службова	+	-	+	+
Комерційна	-	-	-	+
…….	…….	+	-	-
Ел. пошта	+	-	-	+

5. На матриці $М_{тс}$ із використанням даних матриці $М_{ки}$ вказуються напрямки й обсяги переданої категорованої інформації.

6. Потім формується *четверта* матриця – матриця приналежності завдання ($М_п$) до відповідної категорії користувачів (табл. 9.6).

Таблиця 9.6

Матриця приналежності завдання ($М_п$) до відповідної категорії користувачів

Категорії завдань	**Категорії користувачів**						
	I	**II**	**III**		**I**	**II**	**III**
	Директор	**Заст. директора**	**Навчальна частина**	**Менеджери**	**Адміністратори**	**ІТ-викладачі**	**Студенти**
1	2	3	4	5	6	7	8
Складання договорів		✓					
Висновок договорів	✓			✓			
Контроль договорів	✓						
Адміністрування					✓	✓	
Закупівля й установка спеціалізованого ПЗ		✓			✓		
Розробка й заповнення навчальної документації й матеріалів			✓	✓			
Контроль за заповненням навчальної документації й матеріалів		✓					

Закінчення табл. 9.6

1	2	3	4	5	6	7	8
Підготовка звітної документації			✓	✓			
Контроль звітної документації	✓	✓					
Проведення калькуляцій і записів			✓	✓			
Контроль калькуляцій і записів		✓			✓		
Проведення занять						✓	
Виконання практичних завдань							✓

5. Далі формуємо перелік категорій співробітників і типових завдань (відправлення електронної пошти, створення документів) у вигляді *п'ятих* і *шостих* незалежних матриць – $М_{кс}$ і $М_{тз}$ (табл. 9.7).

Таблиця 9.7

Матриці $М_{кс}$ і $М_{тз}$

Матриця $М_{кс}$
Категорії співробітників
Користувач
Адміністратор
.....
Менеджер

Матриця $М_{тз}$
Перелік типових завдань
Складання звіту
Уведення даних
.....
Друк

6. Для кожної категорії користувачів підприємства визначаються такі параметри й характеристики:

а) права доступу й інші права за узгодженням з юристом і профспілкою;

б) посадові обов'язки за узгодженням з юристом і керівництвом підприємства.

в) за узгодженням із керівництвом визначається рівень застосовуваних до користувачів санкцій, перелік яких заздалегідь визначений у *сьомій* матриці – $М_с$ (табл. 9.8).

Таблиця 9.8

Перелік санкцій

№ п/п	Вид порушення	Тип санкції
1	Несанкціоноване копіювання або поширення інформації	Штраф у розмірі до 1 000 грн
…	……	……
n	Неправильне використання паролів	Штраф у розмірі до 500 грн

7. Окремим списком також уводиться перелік заохочень у вигляді *восьмої* матриці ($М_{пщ}$) за аналогією.

8. Окремим списком у вигляді *дев'ятої* матриці вводиться перелік сервісів у мережі – $М_{ср}$. Під кожний тип сервісу докладно описується його організація, переваги й недоліки у вигляді можливостей, мета використання (табл. 9.9).

Таблиця 9.9

Перелік сервісів у мережі

№ п/п	Тип сервісу	Опис
1	Електронна пошта	Засіб обміну повідомленнями з будь-яким вузлом у будь-якій мережі, реалізується спеціальним сервером і управляється адміністратором, для використання надається адреса
…	……...	……
n	Архівування	Процес збереження даних з використанням стиснення для тривалого зберігання й резервування, використовується в основному для запобігання втрати даних

9. *Десята* матриця $М_{су}$ – відповідність типів сервісу на вузлах мережі.

10. Окремим документом із твердженням створюється список користувачів із числа співробітників із зазначенням їхніх робочих місць, посади, часу роботи на комп'ютері у вигляді *одинадцятої* матриці. На підставі матриць $М_{кс}$ і $М_{ср}$ докладно (із посиланням на тип покарання або рівень відповідальності) описуються обов'язки користувача на робочому місці при роботі з тим або іншим сервісом із зазначенням рівня безпеки, перелік яких визначається в матриці $М_{уб}$. Рівні ризику при цьому описуються детально (табл. 9.10).

11. Далі визначається організація діяльності користувача на робочих місцях. При цьому використовують або висхідний опис – від рядового користувача до директора, або спадний – навпаки.

Таблиця 9.10

Рівні ризику

№ п/п	Рівні безпеки	Опис
1	Низький	
…	……	
n	Особливий	

Таким чином, пропонована методика дозволить адміністраторам і начальникам відділів безпеки підвищити рівень розробки й ефективність використання політики безпеки компанії для забезпечення цілісності й надійності різних категорій інформації й самої системи в цілому.

9.4. Методи оцінки втрат

Припустимо, що виникла необхідність у розробці та використанні політики ІБ [72] в організації. Тому необхідно враховувати такі рекомендації:

1) витрати на забезпечення ІБ не повинні перевищувати вартості об’єкта, що захищається, або величину збитку, що може бути нанесений внаслідок атаки на об’єкт, що захищається;

2) необхідно визначити розмір такого збитку [76].

На підставі досліджень авторів пропонується модифікована методика оцінки нанесеного збитку [76], що деталізована до реальних показників. При цьому використовуються такі положення:

1. Законодавчо в Україні встановлений 40-годинний робочий тиждень (ст. 50 Кодексу законів про працю України); на місяць – 24 робочих днів або 192 години; за рік – 46±1 робочий тиждень або 1 840±40 годин (ст. 75 Кодексу законів про працю України).

2. Атаки (зовнішні або внутрішні) ведуться в основному на один або кілька вузлів у комп’ютерній мережі (КМ), але однаково в підсумку страждають кінцеві вузли КМ.

3. Час, який затрачується на відновлення серверу, в 3 рази більший відповідного часу, що відводиться на відновлення робочої станції (РС).

4. Час, що затрачується для роботи з вузлом, який виступає мережним устаткуванням дорівнює 0, оскільки для останнього виконується звичайна заміна. А ремонт і відновлення виконуються після проведення всіх відбудовних робіт із РС і серверами (основне завдання – приведення КМ у працездатний стан за мінімальний час).

Нехай маємо такі вихідні дані:

1. Кількість РС, які піддалися атаці – N.
2. Кількість серверів, які піддалися атаці – S.
3. Час бездіяльності і-го вузла (сервера або РС) внаслідок атаки, $t_i^{Б}$ (годин); у складові цього часу входять: тривалість впливу атакуючого на КМ (більшість сучасних атак мають тривалість до декількох хвилин), тривалість простою вузла в результаті наслідків атаки до настання можливості проведення реабілітаційних дій.
4. Час відновлення і-го вузла (сервера або РС) після атаки, $t_i^{В}$ (годин), залежить від багатьох факторів і може включати такі дії: перевстановлення ОС, наприклад, з "нуля", з образу, "поверх", установка й настроювання драйверів системи (відсутній, якщо перевстановлення виконується з образу), налаштування ОС (відсутній, якщо перевстановлення виконується з образу), установка необхідного ПЗ (відсутній, якщо перевстановлення виконується з образа).
5. Час, що затрачається на відновлення втраченої інформації на і-му вузлі (сервері або РС), $t_i^{ВІ}$ (годин); якщо відновлення інформації в принципі неможливо, то $t_i^{ВІ} \to \infty$; залежить від багатьох факторів і може включати такі дії: визначення (пошук) обсягу інформації для відновлення, пошук дублікатів даної інформації, перезапис інформації в системі, використання спеціальних програмних засобів для відновлення інформації.

Графічно послідовність часів на і-му вузлі з моменту початку проведення атаки виглядає як показано на рис. 9.10.

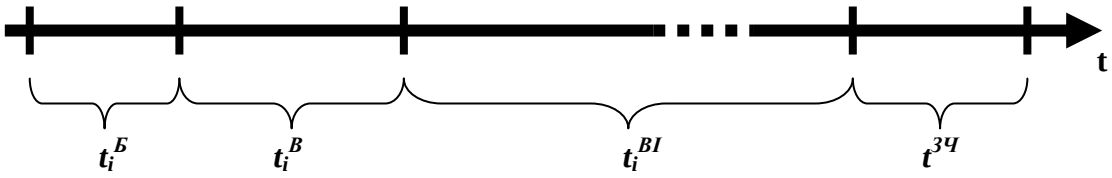


Рис. 9.10. **Діаграма послідовності часів і-го вузла**

6. Середня зарплата адміністратора (оскільки саме адміністратор виконує всі операції з виявлення атак і усунення їхніх наслідків) або фахівців з ІБ, що беруть участь у процесі відновлення, $z_i^{СІБ}$ (грн на місяць).
7. Середня зарплата співробітника атакованого вузла, $z_i^{С}$ (грн на місяць).
8. Економічний ефект від діяльності атакованого і-го вузла з урахуванням віддачі співробітників, що працюють на цьому вузлі, b_i (грн за рік). Тут також варто відрізняти економічний ефект від роботи РС і сер-

вера. У середньому економічний ефект роботи сервера в 2 рази вище ефекту від роботи РС.

9. Час, який затрачається на заміну мережного устаткування або запасних частин, $t^{ЗЧ}$ (годин). Для і-го вузла час $t^{ЗЧ}$ може дорівнювати 0, якщо цей вузол не має потреби ні в якому мережному устаткуванні або запасних частинах для заміни.

10. Середня вартість виконуваних робіт із заміни мережного устаткування або запасних частин, $C_{ЗЧ}$ (грн за годину).

11. Сумарні грошові витрати на ремонт і відновлення мережного устаткування або запасних частин, $Z_{РВ}$ (грн); виконується після проведення всіх попередніх заходів і тривалість, при цьому, не має значення.

У підсумку одержуємо такі вирази.

1. $S + N = O^{ПР}$, де $O^{ПР}$ – загальна кількість атакованих вузлів на підприємстві.

2. Сумарний час простою (бездіяльності) КМ із $O^{ПР}$ вузлів за весь період – $T_{КС}$ (годин) складе

$$T_{КС} = \sum_{i=1}^{O^{ПР}} t_i^{Б}. \qquad (9.7)$$

1. Сумарний час відновлення КМ із $O^{ПР}$ вузлів – $T_{В}$ (годин)

$$T_{В} = \sum_{i=1}^{N} t_i^{В} + 3\sum_{j=1}^{S} t_j^{В}, \qquad (9.8)$$

де $t_j^{В}$ – час відновлення j-го сервера.

2. Сумарний час відновлення загубленої інформації на $O^{ПР}$ вузлах – $T_{ВІ}$ (годин) складе

$$T_{ВІ} = \sum_{i=1}^{O^{ПР}} t_i^{ВІ}. \qquad (9.9)$$

3. Сумарні грошові витрати всіх K фахівців з ІБ за годину, задіяних в усуненні наслідків атаки – $Z_{СІБ}$. Крім того, у цьому процесі можуть брати участь і X зовнішніх експертів, оплата яких в 2 – 5 разів вище оплати штатних фахівців. Усі фахівці з ІБ і експерти працюють одночасно, тому що визначальним фактором є мінімізація часу повернення працездатно-

го стану КМ, отже, облік грошових витрат на їхню роботу повинен також виконуватися одночасно:

$$\sum (T_{КС} + T_{В} + T_{ВІ} + t^{ЗЧ}) = T \rightarrow \min, \qquad (9.10)$$

тоді

$$Z_{СІБ} = \frac{1}{192}\left(\sum_{i=1}^{K} z_i^{СІБ} + (2 \div 5) \cdot \sum_{j=1}^{X} z_j^{СІБ} \right). \qquad (9.11)$$

4. Сумарні витрати на заробітну плату всіх М співробітників за годину, що працюють (тому що вони працюють не одночасно, а послідовно) за атакованим вузлом – Z_C. Як правило, вважається, що за одним вузлом працює один співробітник (у більшості випадків).

$$M = \left[\frac{T}{192} \right] + 1,$$

$$Z_C = \frac{1}{T} \cdot \sum_{i=1}^{M} z_i^C. \qquad (9.12)$$

Можна, звичайно, звести до нуля грошові витрати (зарплату) для них. У цьому випадку повинна бути використана погодинна оплата співробітників.

5. Сумарний економічний ефект від діяльності всіх атакованих вузлів – $Z_{ЕВ}$ за час Т складе

$$Z_{ЕВ} = \frac{1}{1840}\left(\sum_{i=1}^{N} b_i + 2 \cdot \sum_{j=1}^{S} b_j \right) \cdot T \ , \qquad (9.13)$$

де b_j – економічний ефект від діяльності атакованого j-го сервера.

6. Сумарні грошові витрати на заміну мережного устаткування або запасних частин – $Z_{ЗЧ}$ складуть

$$Z_{ЗЧ} = C_{ЗЧ} \cdot t^{ЗЧ}. \qquad (9.14)$$

7. Формули 9.10 – 9.13 визначають проміжні грошові витрати, що виникають в організації в результаті атаки за час Т, обумовлений виразами 9.7 – 9.9.

8. Таким чином, сумарні грошові витрати простою КМ організації (втрати, збиток) у результаті атаки – Z_Σ за весь період часу Т складуть

$$Z_\Sigma = Z_{ЕВ} + Z_{ЗЧ} + (Z_{СІБ} + Z_C + Z_{РВ})\ T. \qquad (9.14)$$

Нагадаємо, що дані розрахунки наведені для однієї атаки. При здійсненні Y (маємо на увазі, що атаки однакові за наслідками, інакше розрахунки повинні вестися для кожної атаки окремо) атак зі своїми коефіцієнтами складності L_i для сумарних грошових витрат простою КМ організації одержимо таке вираження

$$Z = \sum_{i=1}^{Y} L_i \cdot Z_{\Sigma}^{i} \ . \qquad (9.15)$$

Коефіцієнти складності $\boldsymbol{L_i}$ визначаються фахівцями з ІБ експертним шляхом.

Приклад

Організація із чисельністю співробітників – 50 (середня організація). Кількість РС, що піддалися атаці – N = 11 (два відділи, два сегменти). Кількість серверів, що піддалися атаці – S = 2 (один центральний і один допоміжний сервер – друку, поштовий, файловий або резервний). Час бездіяльності і-го вузла (сервера або РС) внаслідок атаки, $t_i^{Б}$ = 5 годин. Час відновлення і-го вузла (сервера або РС) після атаки, $t_i^{В}$ = 16 годин (2 робочих дня). Час, що затрачується на відновлення втраченої інформації на і-му вузлі (сервері або РС), $t_i^{ВІ}$ = 28 годин (3,5 робочих дня). Середня зарплата адміністратора $z_i^{СІБ}$ = 1 500 грн. Кількість фахівців, що брали участь у відновленні К = 2 (адміністратор і його помічник). Кількість зовнішніх експертів Х = 0 (відновлення здійснювалося власними силами). Середня зарплата співробітника атакованого вузла, $z_i^{С}$ = 1 200 грн. Середня економічна вигода від діяльності атакованого і-го вузла з урахуванням віддачі співробітників, що працюють на цьому вузлі, b_i = 5 000 грн. Час, який витрачається на заміну мережного устаткування або запасних частин, $t^{ЗЧ}$ = 1 година (оскільки це тільки заміна). Середня вартість виконуваних робіт із заміни мережного устаткування або запасних частин, $C_{ЗЧ}$ = 120 грн (це оплата праці фахівці сторонніх фірм [105]). Вартість ремонту й відновлення мережного устаткування або запасних частин, $Z_{РВ}$ = 0 грн (після атаки все устаткування або працювало, або його просто замінили на нове – зробили "апгрейд"). Атаки здійснюються однотипні, тому коефіцієнти складності однакові – приймаємо L = 1. Кількість атак за рік, Y = 7. Всі атаки за характером наслідків однакові.

Рішення

1. Загальна кількість атакованих вузлів на підприємстві, $О^{ПР}$ = 13.
2. Сумарний час простою (бездіяльності) КМ (9.7), $T_{КС}$ = 65 годин.

3. Сумарний час відновлення КМ (9.8), $T_В$ = 272 години.

4. Сумарний час відновлення загубленої інформації (9.9), $T_{ВІ}$ = 364 години.

5. Сумарний час, що відводиться на повне обслуговування і-го вузла (9.10), Т = 702 години.

6. Сумарні грошові витрати на оплату послуг фахівців з ІБ за годину, задіяних в усуненні наслідків атаки (9.11), $Z_{СІБ}$ = 15,625 грн.

7. Кількість співробітників, що працюють за атакованим вузлом, М = 4.

8. Сумарні витрати на заробітну плату за годину співробітників, що працюють за атакованим вузлом (9.12), $Z_С$ = 6,84 грн.

9. Сумарний економічний ефект за час Т від діяльності всіх атакованих вузлів (9.13), $Z_{ЕВ}$ = 28 614,13 грн.

10. Сумарні грошові витрати на заміну мережного устаткування або запасних частин (9.14), $Z_{ЗЧ}$ = 120 грн.

11. Сумарні грошові витрати за час **Т**, викликані простоєм КМ підприємства (втрати) у результаті однієї атаки (9.15), Z_{Σ} = 44 504,56 грн.

12. Сумарні грошові витрати простою КМ організації (втрати) у результаті всіх атак (9.15) – при цьому оскільки атаки однотипні, тому $Z = Z^{i}_{\Sigma}$, Z = 311 531,92 грн.

У підсумку організація може втратити навіть третину млн грн у результаті мережних атак на її ресурси протягом року.

Таким чином, пропонована методика допоможе оцінити реальні грошові витрати, що виникають внаслідок кількаразових атак на ресурси фірми, а також підкаже, які засоби ІБ необхідно використовувати, виходячи з вартості розрахованих витрат.

9.5. Методи оцінки ризиків

Методи оцінки ризиків на основі методики фірми Digital Security

Гриф – інструмент для аналізу захищеності ресурсів інформаційної системи компанії й ефективного керування ризиками [63].

Гриф. Модель інформаційних потоків. Загальний опис [65]

Аналіз ризиків ІБ здійснюється за допомогою побудови моделі СКІ компанії. Розглядаючи засоби захисту ресурсів з цінною інформацією, взаємозв'язок ресурсів між собою, вплив прав доступу груп користувачів,

організаційні міри, модель досліджує захищеність кожного виду інформації. У результаті роботи алгоритму програма представляє дані:

1. Інвентаризація.
2. Значення ризику для кожного цінного ресурсу компанії.
3. Перелік всіх уразливостей, які стали причиною отриманого значення ризику.
4. Значення ризику для ресурсів після завдання контрзаходів (залишковий ризик).
5. Ефективність контрзаходів.
6. Рекомендації експертів.

Перед заповненням програми **Гриф** необхідно провести інвентаризацію цінних ресурсів і інформації компанії, тобто визначити всю цінну інформацію й ресурси, на яких вона зберігається.

Далі власники інформації або відповідальні особи (як правило, начальники відділів, у яких ведеться обробка інформації) повинні визначити збиток, що зазнає підприємство при здійсненні загроз конфіденційності, цілісності й доступності даної інформації. Якщо власнику інформації складно оцінити збиток інформації в грошах, програма дозволяє заносити збиток у рівнях (кількість і оцінку рівнів власник вибирає самостійно (у діапазоні від 2 до 100), але для всіх видів інформації в СКІ підприємства кількість і оцінка рівнів повинні бути однакові).

Відзначимо, що в програму **Гриф** заносяться тільки ресурси, на яких обробляється цінна інформація, тобто інформація, для якої можна оцінити збиток при реалізації загроз.

Далі фахівець відділу ІТ (адміністратор системи) надає дані про групи користувачів, які мають доступ до інформації, особливості надання доступу користувачів до ресурсів підприємства (права доступу, вид доступу, мережне устаткування) і засоби захисту, установлені в СКІ.

Фахівці відділу ІБ надають дані про витрати на ІБ.

Співробітникові, що заповнює програму, потрібно внести такі дані, що показані в табл. 9.11.

Основні поняття й допущення моделі:

ресурс – фізичний ресурс, на якому розташовується цінна інформація (сервер, робоча станція, мобільний комп'ютер і т. д.);

мережна група – група, у яку входять взаємозалежні ресурси;

відділ – структурний підрозділ компанії;

бізнес-процеси – виробничі процеси, у яких обробляється цінна інформація;

Таблиця 9.11

Приклади даних для внесення у програму

Дані, які заносяться в програму	Співробітник, відповідальний за надання даних
Види цінної інформації	Власник інформації (ВІ) (або начальник відділу, у якому здійснюється обробка інформації)
Збиток для кожного виду цінної інформації із трьох видів загроз	ВІ (або начальник відділу, у якому здійснюється обробка інформації)
Бізнес-процеси, у яких обробляється інформація	ВІ (або начальник відділу, у якому здійснюється обробка інформації)
Ресурси, на яких зберігається цінна інформація	Фахівець служби ІТ
Мережні групи, у яких перебувають ресурси системи (тобто фізичні зв'язки ресурсів один із одним)	Фахівець служби ІТ
Відділи, до яких ставляться ресурси	Як правило, збігаються з організаційною структурою підприємства
Групи користувачів, що мають доступ до цінної інформації	Фахівець служби ІТ
Клас групи користувачів	Фахівець служби ІТ
Доступ групи користувачів до інформації	Фахівець служби ІТ
Характеристики доступу групи користувачів до інформації (вид і права)	Фахівець служби ІТ
Засоби захисту, установлені в СКІ	Фахівець служби ІТ
Витрати на ІБ	Фахівець служби ІБ

група користувачів – група користувачів, що має однаковий клас і засоби захисту. Суб'єкт, що здійснює доступ до інформації;

клас групи користувачів – особлива характеристика групи, що показує, як здійснюється доступ до інформації;

основні класи груп користувачів:

анонімні Інтернет-користувачі;

авторизовані Інтернет-користувачі;

звичайні користувачі, що здійснюють локальний і вилучений доступ до інформації;

системні адміністратори й офіцери безпеки (так звані суперкористувачі), тобто користувачі, що мають виключні права;

користувачі, що здійснюють доступ до інформації з офісу компанії через Інтернет;

користувачі, що здійснюють доступ до інформації з офісу підприємства по модему;

мобільні Інтернет-користувачі;

засоби захисту робочого місця групи користувачів – засоби захисту клієнтського місця користувача, тобто ресурсу, з якого користувач здійснює доступ до інформації;

характеристики групи користувачів – під характеристиками групи користувачів розуміються види доступу групи користувачів (локальний або вилучений доступ) і права, дозволені групі користувачів при доступу до інформації (читання, запис або видалення);

засоби захисту – засоби захисту ресурсу, на якому розташована (або обробляється) інформація й засоби захисту самої інформації, тобто застосовувані до конкретного виду інформації, а не до всього ресурсу;

ефективність засобу захисту – кількісна характеристика засобу захисту, що визначає ступінь його впливу на СКІ, тобто наскільки сильний засіб впливає на захищеність інформації й робочого місця групи користувачів. Визначається на основі експертних оцінок;

коефіцієнт локальної захищеності (КЛЗ) інформації на ресурсі. Розраховується, якщо до інформації здійснюється тільки локальний доступ. У цьому випадку клієнтське місце групи користувачів і ресурс, на якому зберігається інформація, збігаються; тому захищеність групи користувачів окремо оцінювати не потрібно;

коефіцієнт вилученої захищеності (КВЗ) інформації на ресурсі. Розраховується, коли до інформації здійснюється вилучений доступ; тобто по суті це сумарний коефіцієнт засобів захисту об’єкта;

КЛЗ робочого місця групи користувачів. Розраховується, коли група користувачів здійснює вилучений доступ до інформації, тобто це сумарний коефіцієнт захисту суб’єкта або клієнтського місця групи користувачів. Даний коефіцієнт неможливо визначити для груп анонімних і авторизованих Інтернет-користувачів;

спадкування коефіцієнтів захищеності. Якщо на ресурсі розташовані кілька видів інформації, причому до деяких з них здійснюється доступ через Інтернет (групами анонімних, авторизованих або мобільних Інтернет-користувачів), то загрози, що виходять від цих груп користувачів можуть вплинути й на інші види інформації. Отже, це необхідно врахувати. Якщо на одному з ресурсів, що перебуває в мережній групі, зберігається інформація, до якої здійснюють доступ зазначені групи користувачів, то це враховується аналогічно для всіх видів інформації, що зберігаються на всіх ресурсах, що входять до мережної групи. Механізм спадкування буде докладно описаний далі;

базовий час простою ресурсу (без застосування ЗЗІ) – час, протягом якого доступ до інформації ресурсу неможливий (відмова в обслуговуванні). Визначається в годинах за рік на основі експертних оцінок без обліку впливу на інформацію засобів захисту. Базовий час простою залежить від груп користувачів, що мають доступ до ресурсу: час простою збільшується, якщо до ресурсу мають доступ Інтернет-користувачі;

додатковий час простою ресурсу – час простою, протягом якого доступ до інформації ресурсу неможливий, обумовлене неадекватною роботою програмного або апаратного забезпечення ресурсу. Задається користувачем. Указується в годинах за рік (виняток: час простою не може задаватися для твердої копії);

мережний пристрій – пристрій, за допомогою якого здійснюється зв'язок між ресурсами мережі. Наприклад, комутатор, маршрутизатор, концентратор, модем, точка доступу;

час простою мережного пристрою – час, протягом якого доступ, здійснюваний за допомогою мережного пристрою, до інформації ресурсу неможливий через відмову в обслуговуванні мережного пристрою;

максимальний критичний час простою (T_{max}) – значення часу простою, що є критичним для підприємства. Тобто збиток, нанесений компанії при простоюванні ресурсу протягом критичного часу простою, максимальний. При простоюванні ресурсу протягом часу, що перевищує критичний збиток, нанесений підприємству, не збільшується;

контрзахід – дія, яку необхідно виконати для закриття уразливості;

ризик – імовірний збиток, що зазнає організація при реалізації загроз ІБ, що залежить від захищеності системи;

ризик після завдання контрзаходів – значення ризику, переліченого з урахуванням завдання контрзаходів (закриття уразливостей);

ефективність комплексу контрзаходів – оцінка, наскільки знизився рівень ризику після завдання комплексу контрзаходів стосовно первісного рівня ризику.

Введення в модель

Для того, щоб оцінити ризик інформації, необхідно проаналізувати захищеність і архітектуру побудови СКІ.

Власникові СКІ потрібно спочатку описати архітектуру своєї мережі:

усі ресурси, на яких зберігається цінна інформація;

мережні групи, у яких перебувають ресурси системи (тобто фізичні зв'язки ресурсів один з одним);

відділи, до яких відносяться ресурси;

види цінної інформації;

збиток для кожного виду цінної інформації із трьох видів загроз;

бізнес-процеси, у яких обробляється інформація;

групи користувачів, що мають доступ до цінної інформації;

клас групи користувачів;

доступ групи користувачів до інформації;

характеристики цього доступу (вид і права);

засоби захисту інформації;

засоби захисту робочого місця групи користувачів.

Виходячи з введених даних, можна побудувати повну модель СКІ компанії, на основі якої буде проведений аналіз захищеності кожного виду інформації на ресурсі.

Принцип роботи алгоритму

Отже, пройшовши перший етап (опис необхідних для моделі даних), перейдемо безпосередньо до роботи алгоритму моделі.

Ризик оцінюється окремо по кожному зв’язку "група користувачів – інформація", тобто модель розглядає взаємозв’язок "суб’єкт – об’єкт", з огляду на всі їхній характеристики. Ризик реалізації загрози ІБ для кожного виду інформації розраховується за трьома основними загрозами: конфіденційність, цілісність і доступність. Власник інформації задає збиток окремо за трьома загрозами; це простіше й зрозуміліше, тому що оцінити збиток у цілому не завжди можливо.

Розглянемо принцип роботи моделі послідовно для одного зв’язку "інформація – група користувачів" (для інших вважаємо аналогічно).

Розрахунок ризиків за загрозами конфіденційність і цілісність

Розрахунок ризиків для загроз конфіденційність і цілісність (алгоритми розрахунку для погроз цілісності й конфіденційності схожі, тому їх об’єднали):

1. Визначаємо вид доступу групи користувачів до інформації. Від цього буде залежати кількість засобів захисту, тому що для локального й вилученого доступу застосовуються різні ЗЗІ.

2. Визначаємо права доступу групи користувачів до інформації. Це важливо для цілісності, тому що при доступі "тільки читання" цілісність інформації порушити не можна, і для доступності. Певні права доступу впливають на засоби захисту інформації.

3. Імовірність реалізації загрози залежить від класу групи користувачів. Наприклад, анонімні Інтернет-користувачі становлять найбільшу загрозу для цінної інформації підприємства, тобто, якщо дана група має доступ до інформації, ризик реалізації погрози збільшується. Також залежно від класу групи користувачів змінюються їх ЗЗІ. Наприклад, для авторизованих і анонімних Інтернет-користувачів ми не можемо визначити засобу захисту їхнього робочого місця.

4. Особливим видом засобу захисту є антивірусне ПЗ. В умовах сучасного функціонування СКІ зберігання й обробки інформації шкідливе ПЗ становить найнебезпечнішу й руйнівну загрозу. Знаючи силу впливу КВ, відсутність антивірусного ПЗ на ресурсі (або клієнтському місці користувача) необхідно брати до уваги окремо. Якщо на ресурсі не встановлений антивірус, то ймовірність реалізації загроз конфіденційності, цілісності й доступності різко зростає. Дана модель це враховує.

5. Тепер у нас є всі необхідні знання, щоб визначити ЗЗІ й місце групи користувачів. Просумувавши ваги ЗЗІ, одержимо сумарний коефіцієнт. Для загрози цілісність ураховує специфічні ЗЗІ – засоби резервування й контролю цілісності інформації. Якщо до ресурсу здійснюється локальний і вилучений доступ, то на даному етапі будуть визначені три коефіцієнти: КЛЗ інформації на ресурсі, КВЗ ЗІ на ресурсі й КЛЗ робочого місця групи користувачів. З отриманих коефіцієнтів вибираємо мінімальний. Чим менше коефіцієнт захищеності, тим слабкіше захист, тобто важливо врахувати найменш захищене (найбільш уразливе) місце в СКІ.

6. На цьому етапі набуває чинності поняття спадкування коефіцієнтів захищеності й базових ймовірностей. Наприклад, на ресурсі, що входить у мережну групу, утримується інформація, до якої здійснюється доступ груп користувачів (анонімних, авторизованих або мобільних) з Інтернет. Для цього зв’язку "інформація – група Інтернет-користувачів" розраховується тільки КВЗ інформації на ресурсі, тому що оцінити захищеність груп користувачів не можна (для групи мобільних Інтернет-користувачів КВЗ групи користувачів розраховується окремо). Тепер цей КВЗ необхідно зрівняти з коефіцієнтами захищеності, отриманими для нашого зв’язку "інформація – група користувачів". Це дуже важливий момент. Таким чином, ми враховуємо вплив інших ресурсів системи на наш ресурс і інформацію. У реальній СКІ всі ресурси взаємозалежні між собою, здійснюють один на одного вплив. Тобто зловмисник, проникнувши на один ресурс СКІ (наприклад, одержавши доступ до інформації ресур-

су), може без проблем одержати доступ до ресурсів, фізично зв'язаним зі зламаним. Значною перевагою даної моделі є те, що вона враховує взаємозв'язки між ресурсами СКІ.

7. Окремо враховується наявність криптографічного захисту даних при вилученому доступі. Якщо користувачі можуть одержати вилучений доступ до цінних даних, не використовуючи систему шифрування, це може значно вплинути на цілісність і конфіденційність даних.

8. На останньому етапі перед одержанням підсумкового коефіцієнта захищеності зв'язку "інформація – група користувачів" аналізуємо кількість людей у групі користувачів і наявність у групи користувачів виходу в Інтернет. Усі ці параметри позначаються на захищеності інформації.

9. Отже, пройшовши по всьому алгоритму, ми одержали кінцевий, підсумковий коефіцієнт захищеності для нашого зв'язування "інформація – група користувачів".

10. Далі отриманий підсумковий коефіцієнт потрібно помножити на базову ймовірність реалізації загрози ІБ. Базова ймовірність визначається на основі методу експертних оцінок. Група експертів, виходячи із класів груп користувачів, що одержують доступ до ресурсу, видів і прав їхнього доступу до інформації, розраховує базову ймовірність для кожної інформації. Власник СКІ може задати цей параметр самостійно. Перемноживши базову ймовірність і підсумковий коефіцієнт захищеності, одержимо підсумкову ймовірність реалізації загрози. Нагадаємо, що для кожної із трьох загроз ІБ ми окремо розраховуємо ймовірність реалізації.

11. На завершальному етапі значення отриманої підсумкової ймовірності накладаємо на збиток від реалізації загрози й одержуємо ризик загрози ІБ для зв'язку "вид інформації – група користувачів".

12. Щоб одержати ризик для виду інформації (з урахуванням усіх груп користувачів, що мають до неї доступ), необхідно спочатку просумувати підсумкові ймовірності реалізації загрози за такою формулою:

$$P_{inf} = 1 - \prod_{i=1}^{n} (1 - P_{ug,n}).$$

А потім отриману підсумкову ймовірність для інформації множимо на збиток від реалізації загрози, одержуючи, таким чином, ризик від реалізації загрози для даної інформації.

13. Щоб одержати ризик для ресурсу (з урахуванням всіх видів інформації, збереженої й оброблюваної на ресурсі), необхідно просумувати ризики за всіма видами інформації.

Розрахунок ризиків за загрозою відмови в обслуговуванні

Якщо для цілісності й конфіденційності ймовірність реалізації загрози розраховується у відсотках, то для доступності аналогом імовірності є час простою ресурсу, що містить інформацію. Однак ризик за загрозою відмова в обслуговуванні однаково вважається для зв'язування "інформація – група користувачів", тому що існує ряд параметрів, які впливають не на ресурс у цілому, а на окремий вид інформації. Отже:

1. Визначаємо базовий час простою для інформації.
2. Далі необхідно розрахувати коефіцієнт захищеності зв'язування "інформація – групи користувача". Для загрози відмова в обслуговуванні коефіцієнт захищеності визначається, з огляду на права доступу групи користувачів до інформації й засобів резервування.
3. Так само, як для загроз порушення конфіденційності й доступності, наявність антивірусного ПЗ є особливим ЗЗІ й враховується окремо.
4. Накладаючи коефіцієнт захищеності на час простою інформації, одержимо час простою інформації, з огляду на ЗЗІ. Він розраховується в годинах простою за рік.
5. Специфічний параметр для зв'язування "інформація – група користувачів" – час простою мережного устаткування. Доступ до ресурсу може здійснюватися різними групами користувачів, використовуючи різне мережне устаткування. Для мережного устаткування час простою задає власник СКІ. Час простою мережного устаткування підсумовується часами простою інформації, отриманими у результаті роботи алгоритму. Таким чином, ми одержуємо підсумковий час простою для зв'язку "інформація – група користувачів".
6. Значення часу простою для інформації (**T_{inf}**), з огляду на всі групи користувачів, що мають до неї доступ, обчислюється за такою формулою:

$$T_{inf} = (1 - \prod_{i=1}^{n}(1 - \frac{T_{ug,n}}{T_{max}})) \times T_{max},$$

де T_{max} – максимальний критичний час простою;

$T_{ug,n}$ – час простою для зв'язку "інформація – група користувача".

7. Збиток для загрози відмови в обслуговуванні задається в годинах. Перемноживши підсумковий час простою й збиток від реалізації загрози, одержимо ризик реалізації загрози відмови в обслуговуванні для зв'язку "інформація – група користувачів".

Завдання контрзаходів

У новій версії алгоритму користувач має можливість задавати контрзаходи. Для розрахунку ефективності введеного контрзаходу (Кз) необхідно пройти послідовно по всьому алгоритму з урахуванням заданого контрзаходу. Тобто на виході користувач одержує значення двох ризиків – ризику без обліку контрзаходу (R_{old}) і ризик з урахуванням заданого контрзаходу (R_{new}) (або з обліком того, що уразливість закрита).

Ефективність введення контрзаходу розраховується за формулою:

$$E = \frac{R_{old} - R_{new}}{R_{old}}.$$

У результаті користувач системи одержує такі дані:

ризик реалізації за трьома базовими загрозами для виду інформації;
ризик реалізації за трьома базовими загрозами для ресурсу;
ризик реалізації сумарний за всіма загрозами для ресурсу;
ризик реалізації за трьома базовими загрозами для СКІ;
ризик реалізації за всіма загрозами для СКІ;
ризик реалізації за всіма загрозами для СКІ після завдання Кз;
ефективність контрзаходу;
ефективність комплексу Кз.

Приклади розрахунку ризиків

Приклад розрахунку ризиків СКІ на основі моделі інформаційних потоків. Вихідні дані

Наприклад, СКІ підприємства складається із двох ресурсів: сервера (сервером у даному прикладі будемо вважати ПК, на якому декілька папок відкриті для віддаленого доступу) й РС, які перебувають в одній мережній групі, тобто фізично пов'язані між собою. На сервері зберігаються наступні види інформації: бухгалтерський звіт і база клієнтів підприємства. На РС розташована база даних найменувань товарів підприємства з описом. До сервера локальний доступ має група користувачів (до першої інформації – бухгалтерський звіт): головний бухгалтер.

До сервера вилучений доступ мають групи користувачів (до другої інформації – база клієнтів компанії):

бухгалтер (з робочої станції);

фінансовий директор (через глобальну мережу Інтернет).

До РС локальний доступ має група користувачів (до бази даних найменувань товарів підприємства з описом): бухгалтер.

За правилами роботи моделі бухгалтер при вилученому доступі до сервера є групою звичайних користувачів, а фінансовий директор – групою авторизованих користувачів. Причому, бухгалтер має вилучений доступ до сервера через комутатор. ЗЗІ сервера наведені в табл. 9.12. ЗЗІ першої інформації (бухгалтерський звіт) наведені в табл. 9.13.

Таблиця 9.12

Засоби захисту сервера

Засіб захисту	Вага ЗЗІ
Засоби фізичного захисту	
Контроль доступу в приміщення, де розташований ресурс (фізична охорона, двері із замком, спеціальний пропускний режим у приміщення)	25
Засоби локального захисту	
Відсутність дисководів і USB портів	10
Засоби корпоративного мережного захисту	
Міжмережний екран	10
Обманна система	2
Система антивірусного захисту на сервері	10
Засоби резервування й контролю цілісності	
Апаратна система контролю цілісності	20

Таблиця 9.13

Засоби захисту першої інформації

Засіб захисту	Вага ЗЗІ
Засоби локального захисту	
Засоби криптографічного захисту (криптозахист даних на ПК)	20
Засоби резервування й контролю цілісності	
Резервне копіювання	10
Програмна система контролю цілісності	10

ЗЗІ другої інформації (база клієнтів компанії): ЗЗІ немає. ЗЗІ РС наведені в табл. 9.14.

ЗЗІ (база даних найменувань товарів підприємства з їхнім описом) наведені в табл. 9.15. ЗЗІ клієнтського місця групи користувачів: ЗЗІ клієнтського місця бухгалтера (група звичайних користувачів) наведені в табл. 9.16.

Таблиця 9.14

ЗЗІ РС

Засіб захисту	Вага ЗЗІ
Засоби фізичного захисту	
Контроль доступу в приміщення, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	
Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність дисководів і USB портів	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3
Система криптозахисту електронної пошти	10

Таблиця 9.15

ЗЗІ

Засіб захисту	Вага ЗЗІ
Засоби резервування й контролю цілісності	
Резервне копіювання	10
Програмна система контролю цілісності	10

Таблиця 9.16

ЗЗІ клієнтського місця групи користувачів

Засіб захисту	Вага ЗЗІ
Засоби фізичного захисту	
Контроль доступу в приміщення, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	
Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність дисководів і USB портів	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3
Система криптозахисту електронної пошти	10

Засоби захисту клієнтського місця головного бухгалтера (група звичайних користувачів) наведені в табл. 9.17.

Таблиця 9.17

ЗЗІ клієнтського місця головного бухгалтера

Засіб захисту	Вага ЗЗІ
Засоби фізичного захисту	
Контроль доступу в приміщення, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	
Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність дисководів і USB портів	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3
Система криптозахисту електронної пошти	10

Вид і права доступу груп користувачів до інформації, наявність з'єднання через VPN, кількість чоловіків у групі наведені в табл. 9.18.

Таблиця 9.18

Вид і права доступу груп користувачів до інформації

Категорія	Вид доступу	Права доступу	Наявність VPN-з'єднання	Кількість чоловік у групі
Головний бухгалтер/ бухгалтерська звітність	Локальний	Читання, запис, видалення	Немає	1
Бухгалтер/база клієнтів підприємства (П)	Вилучений	Читання	Є	1
Фінансовий директор/ база клієнтів П	Вилучений	Читання, запис	Є	1
Бухгалтер/база даних найменувань товарів П	Локальний	Читання, запис, видалення	Немає	1

ЗЗІклієнтського місця фінансового директора (група авторизованих Інтернет-користувачів): ЗЗІ клієнтського місця груп авторизованих Інтернет-користувачів неможливо оцінити, тому що невідомо, звідки будуть здійснювати доступ користувачі цієї групи. Наявність у групи користувачів виходу в Інтернет наведені в табл. 9.19.

Збиток підприємства від реалізації загроз ІБ наведені в табл. 9.20.

Отже, сервер і РС підприємства перебувають в одній групі, тобто фізично з'єднані між собою, необхідно поширити найменший коефіцієнт захисту й найбільшу базову ймовірність групи Інтернет-користувачів на всі інформації на всіх ресурсах, що входять у мережну групу.

Таблиця 9.19

Наявність у групи користувачів виходу в Інтернет

Категорія	Доступ в Інтернет
Головний бухгалтер	Є
Бухгалтер	Немає
Фінансовий директор	Не аналізується

Таблиця 9.20

Збиток підприємства від реалізації загроз ІБ

Категорія	Конфіденційність (у. о. за рік)	Цілісність (у. о. за рік)	Доступність (у. о. за годину)
Бухгалтерська звітність	100 у. о.	100 у. о.	1 у. о.
База клієнтів П	100 у. о.	100 у. о.	1 у. о.
База даних найменувань товарів П	100 у. о.	100 у. о.	1 у. о.

Приклад розрахунку ризиків за загрозою конфіденційності

1. Коефіцієнти захищеності:

При локальному доступі до інформації на ресурсі необхідно знайти КЛЗ *інформації*, що складається із суми ваг засобів фізичного й локального захисту.

При вилученому доступі розраховуємо КЛЗ *робочого місця групи користувачів, що мають доступ до інформації*, (сума ваг засобів фізичного, локальної й персонального мережного захисту) і *вилученої захищеності інформації на ресурсі* (сума ваг засобів корпоративного мережного захисту). У подальших розрахунках бере участь найменший коефіцієнт.

При локальному й вилученому доступі знаходимо всі три коефіцієнти, з яких також вибираємо найменший.

Розрахунок ризиків за загрозою конфіденційності

Коефіцієнти захищеності наведені в табл. 9.21.

Облік наявності доступу за допомогою VPN

При локальному доступі наявність VPN не аналізується. При вилученому доступі, при використанні VPN до найменшого коефіцієнта захищеності додається вага VPN-шлюзу. Якщо при вилученому доступі VPN-з’єднання не використовується для груп Інтернет-користувачі, в підсумковий коефіцієнт захищеності множиться на 4, для груп звичайних користувачів (не Інтернет-користувачів) – залишається незмінним, як наведено в табл. 9.22.

Таблиця 9.21

Коефіцієнти захищеності

Категорія	КЛЗ інформації	КВЗ інформації	КЛЗ робочого місця групи користувачів	Найменший коефіцієнт
Головний бухгалтер/ бухгалтерська звітність	55	–	–	55
Бухгалтер/база клієнтів підприємства	–	22	43	22
Фінансовий директор/ база клієнтів П	–	22	–	22
Бухгалтер/база даних найменувань товарів П	30	–	–	30

Таблиця 9.22

Значення коефіцієнтів захищеності

Категорія	Найменший коефіцієнт	Вага VPN-з'єднання	Результуючий коефіцієнт
Головний бухгалтер/ бухгалтерська звітність	55	–	55
Бухгалтер/база клієнтів П	22	20	42
Фінансовий директор/база клієнтів П	22	20	42
Бухгалтер/БД найменувань товарів П	30	–	30

1. Облік кількості людей у групі й наявність у групи користувачів доступу до Інтернету наведений в табл. 9.23.

2. Якщо до інформації має доступ група користувачів, що перевищує 50 осіб, то це відповідно збільшує підсумковий коефіцієнт.

3. Якщо група користувачів має доступ до Інтернету, то це збільшує підсумковий коефіцієнт в 2 рази. Приклад розрахунку підсумкового коефіцієнта: $K = (1 \times 2) / 55 = 0{,}036$.

4. Підсумкова ймовірність.

Щоб одержати підсумкову ймовірність, необхідно визначити базову ймовірність і помножити її на підсумковий коефіцієнт (табл. 9.24).

Таблиця 9.23

Облік кількості людей у групі

Категорія	Результуючий коефіцієнт	Кількість людей у групі користувачів	Наявність у групи користувачів доступу до Інтернет	Підсумковий коефіцієнт
Головний бухгалтер/ бухгалтерська звітність	55	1	2	0,036
Бухгалтер/база клієнтів	42	1	1	0,024
Фінансовий директор/ база клієнтів П	42	1	–	0,024
Бухгалтер/база даних найменувань товарів П	30	1	1	0,033

Таблиця 9.24

Базова ймовірність і підсумковий коефіцієнт

Категорія	Базова ймовірність	Підсумкова базова ймовірність	Підсумковий коефіцієнт	Проміжна ймовірність	Підсумкова ймовірність
Головний бухгалтер/ бухгалтерська звітність	0,35	0,7	0,036	0,0252	0,0252
Бухгалтер/база клієнтів П	0,35	0,7	0,024	0,0168	0,0331
Фінансовий директор/ база клієнтів П	0,7	0,7	0,024	0,0168	
Бухгалтер/БД найменувань товарів П	0,35	0,7	0,033	0,0231	0,0231

Тобто до інформації на ресурсі, що перебуває у мережній групі, мають доступ група Інтернет-користувачів, їхня базова ймовірність поширюється на всю інформацію.

Підсумкова ймовірність для другої інформації, до якої мають доступ кілька груп користувачів, розраховуємо за формулою:

$$P_{inf} = 1 - \prod_{i=1}^{n} (1 - P_{ug,n}).$$

3. Ризик за загрозою конфіденційності наведено в табл. 9.25.

Приклад розрахунку ризиків за загрозою цілісності

1. Перший пункт обчислюється аналогічно розрахунку за загрозою конфіденційності.

2. Облік засобів резервування й контролю цілісності – в табл. 9.26.

Таблиця 9.25

Ризик за загрозою конфіденційності

Категорія	Підсумкова ймовірність	Збиток від реалізації загрози	Ризик
Бухгалтерська звітність	0,0252	100	2,52
База клієнтів П	0,0331	100	3,31
База даних найменувань товарів П	0,0231	100	2,31

Таблиця 9.26

Облік засобів резервування й контролю цілісності

Категорія	Найменший коефіцієнт	Вага VPN-з'єднання	Ваги засобів резервування й контролю цілісності	Результуючий коефіцієнт
Головний бухгалтер/ бухгалтерська звітність	55	–	40	95
Бухгалтер/база клієнтів підприємства	22	20	20	62
Фінансовий директор/ база клієнтів П	22	20	20	62
Бухгалтер/база даних найменувань товарів П	30	–	20	50

3. Облік наявності резервного копіювання, кількості людин у групі користувачів і наявності в групи користувачів доступу до Інтернету наведений в табл. 9.27.

4. Аналогічно розрахунку за загрозою конфіденційності одержимо підсумкову ймовірність наведену в табл. 9.28.

Наявність резервного копіювання враховується у такий спосіб: якщо в інформації на ресурсі здійснюється резервне копіювання, то вага резервного копіювання (10) додається до коефіцієнта захищеності. Якщо в інформації на ресурсі резервне копіювання не здійснюється, і групі користувачів, що має доступ до інформації, дозволені запис або видалення, то підсумковий коефіцієнт збільшується в 4 рази.

Приклад розрахунку ризиків за загрозою відмови в обслуговуванні

Розрахунок ризиків за загрозою доступності

1. Розрахунок коефіцієнта захищеності за загрозою доступності.

При розрахунку ризиків за загрозою доступності аналізуються засоби резервування: кластер, резервне копіювання й резервний канал

(табл. 9.29). Вплив резервного каналу враховується у тому випадку, якщо група звичайних користувачів (не Інтернет-користувачів) має тільки вилучений доступ до інформації на ресурсі (табл. 9.30).

Таблиця 9.27

Облік наявності резервного копіювання, кількості людей у групі користувачів

Категорія	Результуючий коефіцієнт	Наявність резервного копіювання	Кількість людей у групі користувачів	Наявність у групи користувачів доступу до Інтернет	Підсумковий коефіцієнт
Головний бухгалтер/ бухгалтерська звітність	95	1	1	2	0,021
Бухгалтер/база клієнтів П	62	1	1	1	0,016
Фінансовий директор/ база клієнтів П	62	4	1	–	0,065
Бухгалтер/БД найменувань товарів П	50	1	1	1	0,02

Таблиця 9.28

Підсумкова ймовірність

Категорія	Базова ймовірність	Підсумкова базова ймовірність	Підсумковий коефіцієнт	Проміжна ймовірність	Підсумкова ймовірність
Головний бухгалтер/ бухгалтерська звітність	0,25	0,7	0,021	0,0147	0,0147
Бухгалтер/база клієнтів П	0,1	0,7	0,016	0,0112	0,05619
Фінансовий директор/ база клієнтів П	0,7	0,7	0,065	0,0455	
Бухгалтер/база даних найменувань товарів П	0,25	0,7	0,02	0,014	0,014

1. Ризик за загрозою цілісності наведений в табл. 9.29.

Таблиця 9.29

Ризик за загрозою цілісності

Категорія	Підсумкова ймовірність	Збиток від реалізації загрози	Ризик
Бухгалтерська звітність	0,0147	100	1,47
База клієнтів П	0,05619	100	5,61
БД найменувань товарів П	0,014	100	1,4

Таблиця 9.30

Засоби резервування: кластер, резервне копіювання й резервний канал

Засіб	Кластер		Резервне копіювання		Резервний канал	
	є	немає	є	немає	є	немає
Запис і Видалення	20	Const	4	збільшується в 5 разів	5	Const
Видалення	20	Const	4	збільшується в 4 рази	5	Const
Запис	20	Const	4	збільшується в 4 рази	5	Const
Читання	40	Const	4	збільшується в 2 рази	5	Const

Таблиця 9.31

Вплив резервного каналу

Категорія	Коефіцієнт захищеності	Наявність у групи користувачів доступу до Інтернет	Підсумковий коефіцієнт
Головний бухгалтер/ бухгалтерська звітність	0,25	2	0,5
Бухгалтер/база клієнтів П	2	1	2
Фінансовий директор/ база клієнтів П	4	–	4
Бухгалтер/база даних найменувань товарів П	0,25	1	0,25

2. Розрахунок підсумкового часу простою наведений в табл. 9.32.

При розрахунку ризиків за загрозою доступності базові часи простою успадковуються тільки в межах ресурсу. Час простою мережного устаткування додається до підсумкового часу простою.

Якщо підсумковий час простою перевищує максимально критичне (280 годин за рік за базовими налаштуваннями), він прирівнюється до максимально критичного часу простою.

3. Розрахунок ризиків наведений у табл. 9.33.

Основні поняття й допущення моделі

Ризик – імовірний збиток, що зазнає компанія при здійсненні загроз ІБ.

Базові загрози ІБ – порушення конфіденційності, порушення цілісності й відмова в обслуговуванні.

Таблиця 9.32

Розрахунок підсумкового часу простою

Категорія	Базовий час простою	Підсумковий базовий час простою	Час простою мережного устаткування	Підсумковий коефіцієнт	Проміжний час простою	Підсумковий час простою
Головний бухгалтер/ бухгалтерська звітність	40	70	–	0,5	35	35
Бухгалтер/база клієнтів П	40	70	10	2	140	280
Фінансовий директор/ база клієнтів П	70	70	–	4	280	
Бухгалтер/БД найменувань товарів П	40	40	–	0,25	10	10

Таблиця 9.33

Розрахунок ризиків

Категорія	Підсумковий час простою	Збиток від реалізації загрози	Ризик
Бухгалтерська звітність	35	1	35
База клієнтів П	280	1	280
БД найменувань товарів П	10	1	10

Ресурс – контейнер, призначений для зберігання інформації, підданий загрозам ІБ (сервер, робоча станція, переносний комп'ютер). Властивостями ресурсу є: перелік загроз, що впливають на нього, і критичність ресурсу.

Критичність ресурсу (АС) – ступінь значимості ресурсу для СКІ, тобто наскільки реалізація загроз ІБ на ресурс вплине на роботу СКІ. Задається в рівнях (кількість рівнів може бути в діапазоні від 2 до 100) або в грошах. Залежно від обраного режиму роботи може складатися із критичності ресурсу з конфіденційності, цілісності й доступності (Ас, АСі, АСа).

Критичність реалізації загрози (ER) – ступінь впливу реалізації загрози на ресурс, тобто наскільки реалізація загрози вплине на роботу ресурсу. Задається у відсотках. Складається із критичності реалізації загрози щодо конфіденційності, цілісності й доступності (ERc, ERi, ERa).

Імовірність реалізації загрози через дану уразливість протягом року (P(V)) – ступінь можливості реалізації загрози через дану уразливість у тих або інших умовах. Вказується у відсотках.

Максимальний критичний час простою (T_{max}) – значення часу простою, що є критичним для компанії. Тобто збиток, нанесений підприємству при простоюванні ресурсу протягом критичного часу простою, максимальний. При простоюванні ресурсу протягом часу, що перевищує критичний збиток, завданий підприємству, не збільшується.

З погляду базових загроз ІБ існує два режими роботи алгоритму:

одна базова загроза (сумарна);

три базові загрози.

З точки зору одиниць виміру критичності й ризику ресурсу існують два режими роботи алгоритму:

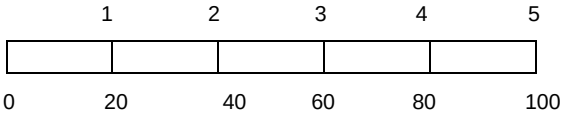
у грошових одиницях;

у рівнях (відсотках).

Принципи розділення шкали на рівні

При роботі з алгоритмом використовується шкала від 0 до 100 %. Максимальне число рівнів – 100, тобто шкалу можна розбити на 100 рівнів. При розбивці шкали на менше число рівнів кожен рівень займає певний інтервал на шкалі. Причому, можливі два варіанти поділу: рівномірний та логарифмічний. Наприклад, для 5 рівнів:

Рівномірний:



1 рівень – 20 %;

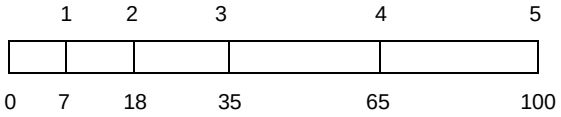
2 рівень – 40 %;

3 рівень – 60 %;

4 рівень – 80 %;

5 рівень – 100 %.

Логарифмічний:



1 рівень – 7 %;

2 рівень – 18 %;

3 рівень – 35 %;

4 рівень – 62 %;

5 рівень – 100 %.

Розрахунок ризиків за загрозою ІБ

1. На першому етапі розраховуємо рівень загрози за уразливістю Th на основі критичності й імовірності реалізації загрози через дану уразливість. Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс із урахуванням імовірності її реалізації.

1.1. Для режиму з однією базовою загрозою:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100},$$

де ER – критичність реалізації загрози (вказується в %);

P(V) – імовірність реалізації загрози через дану уразливість (вказується в %).

Одержуємо значення рівня загрози за уразливістю в інтервалі від 0 до 1.

1.2. Для режиму із трьома базовими загрозами:

$$Th_c = \frac{ER_c}{100} \times \frac{P(V)_c}{100},\ Tn_i = \frac{ER_i}{100} \times \frac{P(V)_i}{100},\ Th_a = \frac{ER_a}{100} \times \frac{P(V)_a}{100},$$

де ER_c, ER_i, ER_a – критичність реалізації загрози конфіденційності, цілісності або доступності (вказується в %);

$P(V)_c$, $P(V)_i$, $P(V)_a$ – імовірність реалізації загрози конфіденційності, цілісності або доступності через дану уразливість (вказується у %).

Одержуємо значення рівня загрози за уразливістю в інтервалі від 0 до 1.

2. Щоб розрахувати рівень загрози за всіма уразливостями CTh, через які можлива реалізація даної загрози на ресурсі, просумуємо отримані рівні загроз через конкретні уразливості.

2.1. Для режиму з однією базовою загрозою:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i),$$

де Th – рівень загрози через уразливість.

Значення CTh одержимо в інтервалі від 0 до 1.

2.2. Для режиму із трьома базовими загрозами:

$$CTh_c = 1 - \prod_{j=1}^{n} (1 - Th_{c,j}),\ CTh_i = 1 - \prod_{j=1}^{n} (1 - Th_{i,j}),$$

$$CTh_a = 1 - \prod_{j=1}^{n} (1 - Th_{a,j}),$$

де Th_c, Th_i, Th_a – рівень загрози конфіденційності, цілісності або доступності з уразливості.

Значення CTh одержимо в інтервалі від 0 до 1.

2.2. Для режиму із трьома базовими загрозами:

$$CTh_c = 1 - \prod_{j=1}^{n}(1 - Th_{c,j}), \quad CTh_i = 1 - \prod_{j=1}^{n}(1 - Th_{i,j}),$$

$$CTh_a = 1 - \prod_{j=1}^{n}(1 - Th_{a,j}),$$

де Th_c, Th_i,Th_a – рівень загрози конфіденційності, цілісності або доступності з уразливості.

Значення CTh одержимо в інтервалі від 0 до 1.

3. Аналогічно розраховуємо загальний рівень загроз за ресурсом CTh (з огляду на всі погрози, що діють на ресурс):

3.1. Для режиму з однією базовою загрозою:

$$CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i),$$

де CTh – рівень загрози за всіма уразливостями.

Значення загального рівня загрози одержимо в інтервалі від 0 до 1.

3.2. Для режиму із трьома базовими загрозами:

$$CThR_c = 1 - \prod_{j=1}^{n}(1 - CTh_{c,j}), \quad CThR_i = 1 - \prod_{j=1}^{n}(1 - CTh_{i,j}),$$

$$CThR_a = 1 - \prod_{j=1}^{n}(1 - CTh_{a,j}),$$

де CTh_c, CTh_i, CTh_a – рівень загрози конфіденційності, цілісності або доступності за всіма загрозами.

Значення загального рівня загрози одержимо в інтервалі від 0 до 1.

4. Ризик з ресурсу R розраховується таким чином:

4.1. Для режиму з однією базовою загрозою:

$$R = CThR \times D,$$

де D – критичність ресурсу (задається в грошах або рівнях);

CTh – загальний рівень загроз з ресурсу.

Якщо ризик задається в рівнях, то як значення критичності беремо оцінку рівня. Наприклад, для трьох рівномірних рівнів, що наведені в табл. 9.34.

Таблиця 9.34

Приклад оцінки рівнів

Назва рівня	Оцінка рівня, %
1	33,33
2	66,66
3	100

У випадку загрози доступність (відмова в обслуговуванні) критичність ресурсу за рік обчислюється за такою формулою:

$$D_{а/рік} = D_{а/годину} \times T_{max}$$

де $D_{а/рік}$ – критичність ресурсу за загрозою доступності за рік;

$D_{а/годину}$ – критичність ресурсу за загрозою доступності за годину;

T_{max} – максимальний критичний час простою ресурсу за рік.

Для інших загроз критичність ресурсу задається за рік.

4.2. Для режиму із трьома базовими загрозами:

$$R_c = CThR_c \times D_c,\ R_i = CThR_i \times D_i,\ R_a = CThR_a \times D_a,$$

$$R_{\sum} = \left(1 - \left(\left(1 - \frac{R_c}{100}\right) \cdot \left(1 - \frac{R_i}{100}\right) \cdot \left(1 - \frac{R_a}{100}\right)\right)\right) \cdot 100,$$

де D_c, D_i, D_a – критичність ресурсу за погрозою конфіденційність, цілісність або доступність. Задається в грошах або рівнях;

$CThR_c$, $CThR_i$, $CThR_a$ – загальний рівень загроз конфіденційність, цілісність або доступність за ресурсом;

$R_{\sum}$ – сумарний ризик за трьома загрозами.

Таким чином, одержимо значення ризику з ресурсу в рівнях (заданих користувачем) або грошах.

5. Ризик для СКІ CR розраховується за формулою:

5.1. Для режиму з однією базовою загрозою:

5.1.1. Для режиму роботи в грошах:

$$CR = \sum_{i=1}^{n} R_i,$$

де R – ризик за ресурсом.

5.1.2. Для режиму роботи в рівнях:

$$CR = \left(1 - \prod_{i=1}^{n}\left(1 - \frac{R_i}{100}\right)\right) \cdot 100,$$

де R – ризик за ресурсом.

5.2. Для режиму роботи із трьома загрозами:

5.2.1. Для режиму роботи в грошах:

$$CR_c = \sum_{j=1}^{n} R_{c,j},\ CR_i = \sum_{j=1}^{n} R_{i,j},\ CR_a = \sum_{j=1}^{n} R_{a,j},$$

$$CR_\Sigma = CR_c + CR_i + CR_a,$$

де CR_c, CR_i, CR_a – ризик за системою за загрозами конфіденційності, цілісності або доступності;

CR_Σ – ризик за системою сумарно за трьома видами загроз.

5.2.2. Для режиму роботи в рівнях:

$$CR_c = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{c,j}}{100}\right)\right) \cdot 100, \qquad CR_i = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{i,j}}{100}\right)\right) \cdot 100,$$

$$CR_a = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{a,j}}{100}\right)\right) \times 100,$$

$$CR_\Sigma = \left(1 - \left(\left(1 - \frac{CR_c}{100}\right) \cdot \left(1 - \frac{CR_i}{100}\right) \cdot \left(1 - \frac{CR_a}{100}\right)\right)\right) \cdot 100,$$

де CR_c, CR_i, CR_a – ризик за системою за загрозами конфіденційності, цілісності або доступності;

CR_Σ – ризик за системою сумарно за трьома видами загроз.

9.6. Служба інформаційної безпеки. Організація її аудиту

Цілі та призначення аудиту

До основних цілей аудиту ІБ можна віднести такі:

одержання об’єктивної й незалежної оцінки поточного стану захищеності інформаційних ресурсів;

одержання максимальної віддачі від засобів, що інвестуються у створення системи ІБ [71];

оцінка можливого збитку від несанкціонованих дій [76];
розробка вимог до побудови системи захисту інформації;
визначення зон відповідальності співробітників підрозділів;
розрахунок необхідних ресурсів [107];
розробка порядку й послідовності впровадження системи ІБ.

Аудит може проводиться у таких варіантах:

комплексний аудит – перед створенням системи ІБ;

точковий – формування вимог до проведення модернізації СЗІ;

періодичний – зовнішня регламентна перевірка рівня захищеності СКІ;

перевірочний – експертиза й оцінка використовуваних або планованих до використання систем і рішень.

Етапи проведення аудиту

Процес аудиту СКІ можна представити у вигляді своєрідних елементів (рис. 9.11), де на одній чаші розглядаються системи безпеки доступу, на іншій – контроль бізнес-процесів, а як опора служить технічна інфраструктура, що, у свою чергу, заснована на прийнятих методах авторизації, конфігурації системи, а також на політиках і процедурах, прийнятих в організації.

Роботи з аудиту безпеки СКІ містять у собі ряд послідовних етапів (рис. 9.12), які в цілому відповідають етапам проведення комплексного аудиту СКІ, що містить у собі:

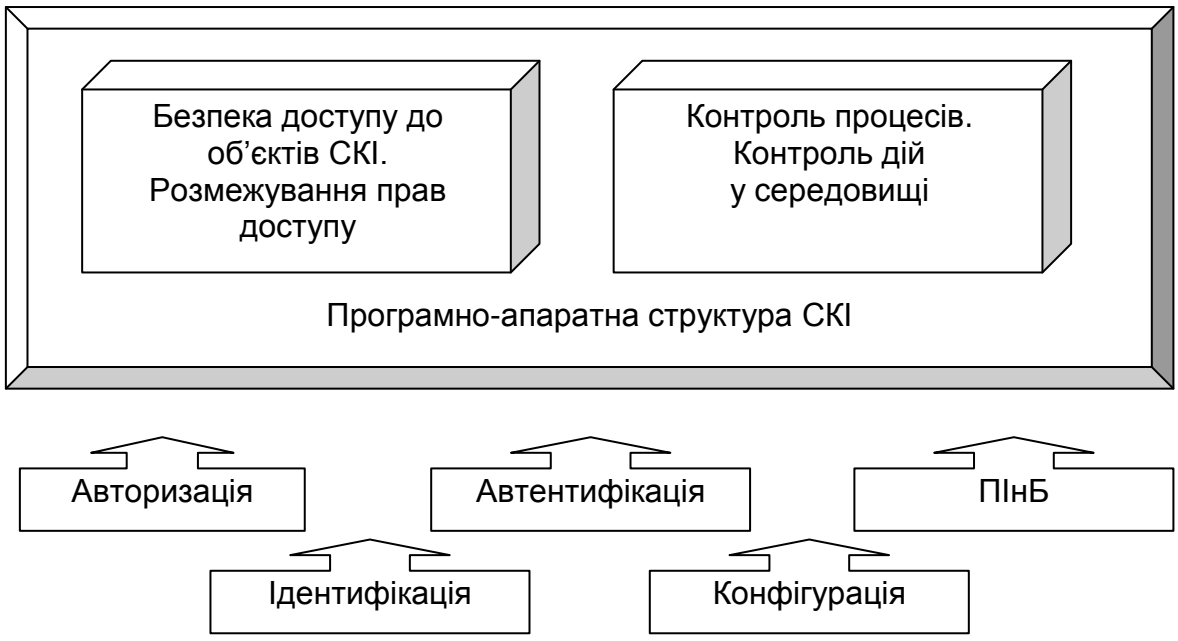


Рис. 9.11. **Елементи процесу проведення аудиту СКІ**

Рис. 9.12. **Етапи проведення аудита ІБ** [108]

1) комплексне обстеження – включає збір інформації про використовувані інформаційні ресурси – системне ПЗ, локальні мережі й телекомунікації, прикладні системи, а також аналіз існуючих організаційно-правових процесів. За результатами обстеження формується (уточнюється) перелік критичних ресурсів і розробляється перелік загроз для даних ресурсів;

2) проведення оцінки захищеності – включає роботи з виявлення уразливостей технічних засобів, аналізу технологічної захищеності, а також адекватності організаційних процедур. На основі виявлених недоліків проводиться оцінка ризиків, що включає основні способи подолання системи захисту, ступінь критичності й можливість реалізації;

3) атестація системи – включає заходи щодо обстеження (оцінки) існуючих мір і заходів щодо захисту інформації, оцінки їхньої адекватності, а також відповідність вимогам провідних стандартів;

4) за результатами аудиту розробляється план виправлення виявлених недоліків. Завдання планування полягає у визначенні пріоритетів виправлення виявлених недоліків, розробки черговості й методології їхнього усунення. Додатково передбачається розробка концептуальних і

процедурних документів, таких, як Концепція ІБ, Загальні вимоги й рекомендації із захисту інформації, ПІнБ та ін.

Залежно від цілей і способу проведення аудиту ІБ, ініціатором цього заходу, як уже було зазначено , є зацікавлена сторона. Найбільше часто ініціатором аудита є організація в особі його керівництва.

Як правило на етапі обстеження вирішуються такі, організаційні питання:

права й обов'язки аудитора чітко визначаються й документально закріплюються в його посадових інструкціях, а також у положенні про внутрішній *(зовнішній)* аудит;

аудитором підготовляється й узгоджується з керівництвом план проведення аудиту ІБ.

На етапі обстеження також визначаються межі проведення обстеження. Межі проведення обстеження зазвичай визначаються такими термінами:

список обстежуваних фізичних, програмних та інформаційних ресурсів;

площадки *(приміщення)*, що потрапляють у межі обстеження;

основні види загроз безпеки, розглянуті при проведенні аудиту;

організаційні *(законодавчі, адміністративні й процедурні)*, фізичні, програмно-технічні та інші аспекти забезпечення безпеки, які необхідно врахувати в ході проведення обстеження, їх пріоритети *(у якому обсязі вони повинні бути враховані)*.

Далі треба провести збір інформації аудиту, що є найбільш складним і тривалим. Це, як правило, пов'язано з відсутністю необхідної документації на інформаційну систему й з необхідністю щільної взаємодії аудитора з багатьма посадовими особами організації.

Компетентні висновки щодо стану справ у компанії з ІБ можуть бути зроблені аудитором тільки за умови наявності всіх необхідних вихідних даних для аналізу. Одержання інформації про організацію, функціонування й поточний стан СКІ здійснюється аудитором у ході спеціально організованих інтерв'ю з відповідальними особами компанії, шляхом вивчення технічної й організаційно-розпорядницької документації, а також дослідження СКІ із використанням спеціалізованого програмного інструментарію.

Забезпечення ІБ організації – це комплексний процес, що вимагає чіткої організації й дисципліни. Він повинен починатися з визначення ролей і розподілу відповідальності серед посадових осіб, що займаються ІБ. Тому перший пункт аудиторського обстеження починається з одер-

жання інформації про організаційну структуру користувачів СКІ і обслуговуючих підрозділів. У зв'язку з цим аудиторові потрібна документація, що стосується схеми організаційної структури СКІ. Звичайно, у ході інтерв'ю аудитор задає опитуваним питання, що стосуються використання інформації, яка циркулює усередині СКІ.

Призначення й принципи функціонування СКІ багато в чому визначають існуючі ризики й вимоги безпеки, пропоновані до системи. Тому на наступному етапі аудитора цікавить інформація про призначення й функціонування СКІ. На даному етапі аудитор може використовувати документацію, що містить такі дані: опис автоматизованих функцій; схема інформаційних потоків; опис структури комплексу технічних засобів СКІ; опис структури ПЗ; опис структури інформаційного забезпечення; опис технічних завдань використовуваних додатків.

Далі аудитору потрібна більш детальна інформація про структуру СКІ. Це дозволяє з'ясувати, яким чином здійснюється розподіл механізмів безпеки за структурними елементами та рівнями функціонування СКІ.

Підготовка значної частини документації на СКІ, звичайно, здійснюється вже в процесі проведення аудиту. Коли всі необхідні дані з СКІ, включаючи документацію, підготовлені, можна перейти до наступного етапу – їх аналізу.

Використовувані аудиторами методи аналізу даних визначаються обраними підходами до проведення аудиту, які можуть істотно розрізнятися. Але загалом можна виділити 3 підходи [99].

Перший підхід, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної СКІ індивідуальний набір вимог безпеки, яка найбільшою мірою враховує особливості даної СКІ, середовища її функціонування й існуючі в даному середовищі загрози безпеки. Даний підхід є найбільш трудомістким і вимагає найвищої кваліфікації аудитора. На якість результатів аудита, у цьому випадку, значно впливає використовувана методологія аналізу й керування ризиками та її застосовність до даного типу СКІ.

Якщо для проведення аудиту безпеки обраний даний підхід, то на етапі аналізу даних аудиту зазвичай виконуються такі групи завдань:

1. Аналіз ресурсів СКІ, включаючи інформаційні ресурси, програмні й технічні засоби, а також людські ресурси.
2. Аналіз груп завдань, розв'язуваних системою, і бізнес-процесів.

3. Побудова *(неформальної)* моделі ресурсів СКІ, що визначає взаємозв'язок між інформаційними, програмними, технічними й людськими ресурсами, їх взаємне розташування й способи взаємодії.

4. Оцінка критичності інформаційних ресурсів.

5. Визначення найбільш імовірних загроз безпеки щодо ресурсів СКІ і уразливостей захисту, що роблять можливим здійснення цих загроз.

6. Оцінка ймовірності здійснення загроз, величини уразливостей і збитку, який наноситься організації у випадку успішного здійснення загроз.

7. Визначення величини ризиків для кожної трійки: загроза – група ресурсів – уразливість.

Перерахований набір завдань є досить загальним. Для їх рішення можуть використовуватися різні формальні й неформальні, кількісні та якісні, ручні й автоматизовані методики аналізу ризиків. Суть підходу від цього не змінюється.

Оцінка ризиків може даватися з використанням різних як якісних, так і кількісних шкал. Головне, щоб існуючі ризики були правильно ідентифіковані й ранжирувані відповідно до ступеня їх критичності для організації. На основі такого аналізу може бути розроблена система першочергових заходів щодо зменшення величини ризиків до прийнятного рівня.

Другий підхід, більш практичний, опирається на використання стандартів ІБ. Стандарти визначають базовий набір вимог безпеки для широкого класу СКІ, що формується у результаті узагальнення світової практики. Стандарти можуть визначати різні набори вимог безпеки, залежно від рівня захищеності СКІ, що потрібно забезпечити, її приналежності *(комерційна організація, або державна установа)*, а також призначення *(фінанси, промисловості, зв'язок і т. п.)*. Від аудитора в цьому випадку потрібно правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити для даної СКІ. Через свою простоту *(стандартний набір вимог для проведення аудиту вже заздалегідь визначений стандартом)* і надійності, описаний підхід найпоширеніший на практиці *(особливо при проведенні зовнішнього аудиту)*. Цей підхід дозволяє при мінімальних витратах ресурсів робити обґрунтовані висновки про стан СКІ.

У випадку проведення аудиту безпеки згідно з даним підходом, аудитор оцінює застосовність вимог стандарту до обстежуваного СКІ і її відповідність вимогам стандарту. Ґрунтуючись на даних про відповідність різних областей функціонування СКІ вимогам стандарту, визначається, які вимоги безпеки в системі не реалізовані. Виходячи із цього, роблять-

ся висновки про відповідність обстежуваної СКІ вимогам прийнятого на підприємстві стандарту й даються рекомендації з реалізації в системі механізмів безпеки, що дозволяють забезпечити таку відповідність.

Третій підхід, найбільш ефективний, припускає комбінування перших двох. Базовий набір вимог безпеки, пропонованих до СКІ, визначається обраним стандартом. Додаткові вимоги, які у максимальному ступені враховуючі особливості функціонування даної СКІ, формуються на основі аналізу ризиків. Цей підхід є набагато простішим першого, тому що більша частина вимог безпеки вже визначена стандартом, і, в той же час, він позбавлений недоліку другого підходу, що полягає у тому, що вимоги стандарту можуть не враховувати специфіки обстежуваної СКІ.

Організація технічного захисту інформації

Захист від апаратних збоїв

Для захисту від апаратних збоїв необхідно мати надійне устаткування. От кілька порад:

1. Якщо дозволяють засоби, то придбайте й використовуйте блоки безперебійного живлення (UPS).

2. Ніколи не здобувайте (а якщо він у вас є, то відмовтеся від використання) кеш-контролер (особливо фірми Tekram).

3. Ніколи не здобувайте (а якщо він у вас є, то відмовтеся від використання) BackPack (жорсткий диск, що працює через паралельний порт) – надзвичайно ненадійний пристрій.

4. Заземліть свій ПК. Гарним заземленням може послужити металева арматура будинку (але не батареї опалення).

5. Ніколи не довіряйте ремонт (складання, підключення додаткових пристроїв, "апгрейд") некваліфікованим особам.

6. Покупку ПК і комплектуючих робіть тільки в надійних і перевірених фірмах.

Захист від програмних збоїв

Для захисту від програмних збоїв необхідно мати деякий мінімум знань, бажано з вузу. Наприклад, можна запропонувати пройти навчання в Харківському національному економічному університеті. І хоча це не профільний технічний ВНЗ, на сьогодні тут пропонують дуже гарну підготовку в даних областях. А вже отримані знання можна застосовувати для підвищення ступеня захищеності від програмних збоїв на основі таких рекомендацій.

1. Користуйтеся надійними ОС або якими доведеться, але самостійно підвищуйте їхній ступінь надійності – прислухайтеся до перевіреної думки, як що це можливо.

2. Ніколи не використовуйте програми кешування дисків smartdrv.exe або подібні – завжди видаляйте їх з файлів автозавантаження, а також config.sys і autoexec.bat та інші подібні програми (до апаратних кеш-контролерів це так само відноситься) – Norton Speed Drive, Rocket. Як правило, більшість збоїв жорстких дисків відбувається саме через них. Та й особливої необхідності в них зараз уже немає, тому що сучасні накопичувачі на жорсткому магнітному диску (НЖМД) мають високі швидкості роботи.

3. Установлюйте мінімум додатків. При установці користуйтеся правилом пішого туриста, що весь багаж несе на власній спині: "Бери із собою не те, що може знадобитись, а те, без чого не можна обійтися". ОС із установленим більшим числом додатків стає "важче".

4. Установлюйте по можливості більший обсяг оперативного запам’ятовуючого пристрою (ОЗП). Правильна ознака недостачі ОЗП – різка зміна роботи й звертання до НЖМД без видимих причин, а це приводить до його зношування. На жорсткому диску ОС виділяє місце для файла підкачування (swap file), куди записуються проміжні дані, що не вміщаються в ОП.

5. Проводьте періодичне "збирання" – знищення зайвих даних на НЖМД. Є два сценарії "збирання": м’який і твердий. За "м’яким" сценарієм видаляються всі додатки, які не використовуються, а також непотрібні файли. Твердий сценарій передбачає форматування диска й нову установку ОС і додатків. Багато користувачів проводять "збирання" за "твердим" сценарієм й зазначають значні поліпшення. Відбувається це тому, що Windows запам’ятовує безліч змін конфігурації, що згодом призводить до її "засмічення".

6. Тримайте одночасно запущеними тільки необхідний мінімум додатків. Наприклад, якщо потрібно прямо перенести об’єкт із однієї програми в іншу. Непотрібні додатки не мінімізуйте (споживати ресурсів від цього вони менше не стануть), а закривайте.

7. Якщо програмна проблема виникла й регулярно повторюється, то варто згадати Олександра Македонського і його спосіб "розв’язання" гордіївого вузла, і провести "чищення" диска за "твердим" сценарієм. Ча-

су в середньому витрачається менше, а користі – набагато більше. Якщо проблема залишається, то з'ясуйте, який додаток її породжує.

8. Намагайтеся уникати бета-версій. Користувач бета-версії, мало того що безкоштовно працює бета-тестером, так ще й нічого не одержує за ризик користування програмою, свідомо утримуючи помилки. У міру виходу офіційних версій не встановлюйте їх відразу, а дочекайтеся виходу ремонтних комплектів.

9. Регулярно запускайте програми діагностики. Іноді вони є корисними.

10. Регулярно виконуйте дефрагментацію НЖМД. Наявність вільного безперервного дискового простору прискорює роботу віртуальної пам'яті. Крім того, сучасні програми дефрагментації дозволяють трохи підвищити швидкість запуску додатків за рахунок їх оптимального й безперервного розміщення на диску.

11. І, нарешті, найголовніше – виконуйте періодичне резервне копіювання (архівування) усіх важливих даних. Причому бажано мати не менш двох копій (різних дат) з вашими важливими даними – пам'ятайте: скупий платить двічі, а то й тричі!

Помилки в ПЗ й відновлення програм

Програми створюються людьми, а людям властиво помилятися. Комп'ютерні зломщики буквально змагаються в пошуку "дір" у системах і програмах, які дозволяють зробити що-небудь недозволене, наприклад, одержати НСД до інформації. Виробники ПЗ постійно працюють над поліпшенням своїх продуктів, випускають нові версії й "латки" ("патчі", patches) до старих версій. Також існують "маленькі" проміжні відновлення – hot fixes [80].

Захист від шкідливих комп'ютерних факторів

Наше нинішнє життя немислиме без ПК, але при роботі з ним необхідно враховувати ряд рекомендацій, які допоможуть зберегти ваше здоров'я.

1. Мінімальна відстань між екраном і оператором ПК повинна бути близько 50 см, але не менш 30 см.

2. Як монітор ПК найкраще використовувати нові кольорові рідиннокришталеві дисплеї.

3. Ідеальним (з погляду безпеки для здоров'я) є комп'ютер типу "Notebook".

4. Якщо ви користуєтеся звичайним монітором на електронно-променевої трубці (ЕПТ), то в обов'язковому порядку необхідно використовувати захисні окуляри. Хоча сучасні монітори й мають високий клас

безпеки, названий ТСО, автор цих рядків, наприклад, користується подібними окулярами.

5. Верх екрана повинен бути приблизно на рівні горизонтальної лінії, проведеної від очей до екрана під прямим кутом.

6. Під час роботи положення кистей рук повинне бути горизонтальним, передпліччя розігнуті в ліктьових суглобах під кутом 90 градусів, спина пряма. Руки повинні мати опору на столі. Для підстав кистей рук дуже допомагають гелеві підложки у ковдрах для миші.

7. Під час нормальної роботи голова не повинна бути сильно нахилена, щоб не турбували головні болі й болі в шиї.

8. Клавіатура повинна розташовуватися не ближче 10 см від краю стола. При тривалій роботі із клавіатурою небажано, щоб кисті й передпліччя опиралися на кут стола.

9. Бажано, щоб комп'ютер був заземлений.

10. При тривалій роботі із ПК важливі своєчасний відпочинок і розминка. Рекомендується такий режим: 45 хвилин безперервної роботи, 15-хвилинний відпочинок з обов'язковою гімнастикою, у тому числі й для очей.

11. Під час роботи з монітором не слід сидіти "як стовп", необхідно періодично змінювати позу, рухати плечима, моргати очами або закривати їх на кілька секунд. Дихати треба вільно.

12. Через 10 хвилин роботи корисно на 5 – 10 секунд відвести очі убік від екрана.

13. Варто обмежити час інтенсивної роботи із ПК; не більше 4 годин на день – таке обмеження передбачено законодавством України.

14. Робочі місця із ПК повинні певним чином установлюватися відносно світлоотворів.

Схеми розміщення робочих місць із ПК повинні враховувати відстані між робочими столами з моніторами (у напрямку тилу поверхні одного монітора й екрана іншого монітора), що повинне бути не менше 2,0 м, а відстань між бічними поверхнями моніторів – не менше 1,2 м.

Конструкція робочого стола повинна забезпечувати оптимальне розміщення на робочій поверхні встаткування з урахуванням його кількості й конструктивних особливостей, характеру виконуваної роботи. При цьому допускається використання робочих столів різних конструкцій, що відповідають сучасним вимогам ергономіки.

Конструкція робочого стільця (крісла) повинна забезпечувати підтримку раціональної робочої пози при роботі на ПК, дозволяти змінювати

позу з метою зниження статичної напруги м’язів шийно-плечової області й спини для попередження розвитку стомлення.

Робочий стілець (крісло) повинен бути підйомно-поворотним і регульованим по висоті й кутам нахилу сидіння й спинки, а також відстані спинки від переднього краю сидіння, при цьому регулювання кожного параметра повинна бути незалежної, легко здійснюваної й мати надійну фіксацію.

Поверхня сидіння, спинки й інших елементів стільця (крісла) повинна бути напівм’якою, з нековзним, що не електризується й повітропроникним покриттям, що забезпечує легке очищення від забруднень.

Для багатьох людей ПК давно став не тільки незамінним другом і помічником, але й робочим місцем, за яким вони повинні просиджувати декілька годин щодня. Відомо, що комп’ютер може негативно впливати на психіку дітей і підлітків. Існують, однак, прості рекомендації, виконуючи які (у деяких місцях повторимося), можна звести до мінімуму несприятливий вплив ПК на здоров’я. От деякі з них.

1. Якщо ви змушені проводити тривалий час, працюючи за ПК, намагайтеся знайти діапазон комфортних для вас положень – комфортну "зону". Часто міняти положення в цьому діапазоні помітно краще й корисніше, ніж проводити цілий день в одній позі. Намагайтеся частіше міняти положення, іноді вставати для виконання іншої роботи – одним словом, давати собі хоч короткий відпочинок. Особливо уважними будьте в другій половині дня. Якщо ваш стілець або крісло регулюється по положенню, частіше користуйтеся цією корисною функцією.

2. Якщо від довгого сидіння за ПК або наприкінці напруженого дня у вас починає боліти спина, спробуйте покласти на стілець клин з пінопласту або іншого матеріалу так, щоб задня частина його піднімалася на 7 рівнів, а передня плавно сходила до площини стільця: коліна повинні перебувати нижче стегон. Час від часу витягайте спину, широко розвівши руки над головою. Розслабити шию й плечі можна, зводячи лопатки, одночасно піднімаючи їх нагору. Приходячи додому після роботи, розстеліть на ліжку клейонку й накрийте її вологим гарячим рушником з декількома краплями лавандового масла. Лягаєте на це голою спиною й укутайтеся вовняною ковдрою. І взагалі, намагайтеся берегти спину й особливо хребет.

3. Коли ви працюєте за ПК, намагайтеся, щоб ваші ноги увесь час прилягали до підлоги ступнями, а не тільки "нісками". Якщо ви використовуєте підставку під ноги, переконаєтеся, що вона досить велика, щоб ви могли частіше міняти положення ніг. Уникайте обмеження простору

для ніг, наприклад, установлення системного блоку під стіл, де він буде вам заважати. Сидячи, намагайтеся розподілити вагу тіла рівномірно – використовуйте спинку стільця, а не подавайтеся всім тілом уперед.

4. Коли ви працюєте за комп'ютером, багато друкуєте, намагайтеся, щоб передпліччя, зап'ястя й кисть перебували на одному рівні, на одній лінії. Не слід опиратися долонями або зап'ястями на клавіатуру або площину стола під час роботи. Особливо небажано опиратися зап'ястям на поверхні, що утворюють прямий кут, наприклад на самий край стола. Намагайтеся, щоб лікті перебували на тім же рівні, що займає на клавіатурі середній ряд клавіш (містить латинські букви G, H).

5. Довго працюючи за комп'ютером, намагайтеся убезпечити очі. Частіше влаштовуйте відпочинок: недовго подивіться вдалину. Обов'язково стежите за тим, щоб екран монітора і ваші окуляри завжди залишалися чистими. Однією з найчастіших причин дискомфорту в очах є висихання слизової оболонки. Намагайтеся частіше моргати – це захистить очі від висихання й позбавить від дискомфорту.

6. Якщо у вас швидко втомлюються очі, закрийте їх долонями так, щоб пальці схрестилися на чолі. Прикрийте віка й рухайте очними яблуками поперемінно то вліво, то вправо протягом 2 – 3 хвилин. Ранком і ввечері на закриті очі на 15 – 20 хвилин можна покласти два чайних пакетики, попередньо заварених окропом і охолоджених, або лляні серветки, змочені в настої ромашки. Намагайтеся частіше давати очам відпочинок, уникайте різкого переходу від темряви до світла й занадто яскравого висвітлення. При виборі шпалер для будинку віддавайте перевагу зеленому, салатному й блакитному кольорам. Буваючи на вулиці, затримуйте погляд на траві й деревах.

7. Якщо ви багато працюєте за комп'ютером, ретельно підберіть положення монітора. Він завжди повинен розташовуватися прямо перед вами. Витягніть руку вперед – екран повинен розташовуватися приблизно на відстані "кісточок" пальців, у той же час текст на екрані повинен бути ясно видний. Розташовуючи монітор по висоті, намагайтеся, щоб верхній рядок тесту розташовувався трохи нижче рівня очей. Площина монітора повинна йти паралельно площині вашого тіла.

8. Працюючи за комп'ютером, намагайтеся розташувати мишу й клавіатуру так, щоб ними було зручно користуватися. Клавіатура повинна перебувати прямо перед вами – так, щоб не довелося нікуди повертатися. Миша або трекбол повинні розташовуватися безпосередньо пра-

воруч або ліворуч від клавіатури (залежно від того, правша ви або лівша), обов'язково на одному рівні з нею.

9. Зняти напругу, стомлення і втому можна, виконавши прості вправи. Покладіть руки на шию й давіть вперед, почуваючи напругу в плечах. Зусилля чергуйте з відпочинком. Потім сплетіть пальці долонь і витягніть руки максимально вперед. Відпочиньте. Позбутися утоми очей можна, надавлюючи протягом трьох секунд пальцями на крапки, розташовані між переніссям і внутрішніми куточками очей. Головний біль можна полегшити круговим масажем скронь і натисненням крапок уздовж брів. Спробуйте також занурювати руки по лікоть у холодну воду. А перед сном потримаєте в прохолодній воді : наберіть небагато в долоні й затримайте на очах.

10. Організація інформаційної безпеки комп'ютерних мереж

10.1. Стандарти інформаційної безпеки

Стандарт ІБ – "Orange Book"

"Orange Book" або Жовтогаряча книга (ЖК) прийнятий як стандарт в 1983 р. МО США (Department of Defense – DoD). Повна назва документа "Department of Defense Trusted Computer System Evaluation Criteria" **–** Критерії ІБ комп'ютерних систем. Згідно з ЖК всі захищені комп'ютерні системи діляться на сім класів – від D1 (мінімальний захист, фактично відсутність усякого захисту) до A1 [190].

ОК призначається для такої мети:

1. Надати виробникам стандарт, що встановлює, якими засобами ІБ варто оснащувати свої нові й плановані продукти, щоб поставляти на ринок доступні системи, що задовольняють вимоги гарантованої захищеності (маючи на увазі, насамперед, захист від розкриття даних) при використанні й обробці цінної інформації.

2. Надати DoD метрику для військового приймання й оцінки захищеності електронних засобів обміну даними, призначених для обробки службової й іншої цінної інформації.

3. Забезпечити базу для дослідження вимог до вибору захищених систем.

Стандарт розглядає два типи оцінки:

без обліку середовища, у якій працює техніка;

у конкретному середовищі (ця процедура називається атестуванням).

Основні елементи ПІнБ

Згідно з ЖК, ПІнБ повинна містити в собі такі елементи:

1. Довільне керування доступом.
2. ІБ повторного використання об’єктів.
3. Мітки ІБ.
4. Примусове керування доступом.

Довільне керування доступом – це метод обмеження доступу до об’єктів, заснований на обліку особистості суб’єкта або групи, у яку суб’єкт входить. Довільність керування полягає у тому, що деяка особа (власник об’єкта) може за своїм розсудом давати іншим суб’єктам або відбирати в них права доступу до об’єкта.

Вимоги до ПІнБ

Вимоги до ПІнБ системи підрозділяються відповідно до основних її напрямів, що передбачаються ЖК (табл. 10.1).

Таблиця 10.1

Опис класів ІБ

Властивість	Опис
1	2
Клас D1	
Мінімальний захист	Клас зарезервований для тих систем, які були піддані оцінюванню, але в які не вдалося досягти виконання вимог більше високих класів оцінок. Всі ОС, не задовольняючим вимогам вищих класів
Клас C1 в ОС підтримується вибірне (дискреційне) розмежування доступу. Користувач перед початком праці з системою повинен підтвердити свою дійсність (автентифікуватися)	
Довільне керування доступом	Надійна система повинна управляти доступом іменованих користувачів до іменованих об’єктів. Механізм керування (права для власника/групи/інших, списки керування доступом) повинен дозволяти користувачам специфікувати поділ файлів між індивідами й/або групами
Ідентифікація й автентифікація	Користувачі повинні ідентифікувати себе, перш ніж виконувати які-небудь інші дії, контрольовані надійною системою. Для автентифікації повинен використовуватися який-небудь захисний механізм, наприклад, паролі. Автентифікаційна інформація повинна бути захищена від НСД

Продовження табл. 10.1

1	2
Операційна гарантованість	Система повинна підтримувати область для власного виконання, захищену від зовнішніх впливів (зокрема, від зміни команд і/або даних) і від спроб спостереження за ходом роботи. Ресурси, контрольовані базою, можуть становити певну підмножину всіх суб'єктів і об'єктів системи
Цілісність системи	Повинні бути в наявності апаратні й/або програмні засоби, що дозволяють періодично перевіряти коректність функціонування апаратних і мікропрограмних компонентів системи
Тестування	Захисні механізми повинні бути протестовані на предмет відповідності їхнього поводження системної документації. Тестування повинне підтвердити, що в неавторизованого користувача немає очевидних способів обійти або зруйнувати засобу захисту системи
Керівництво користувача по засобам ІБ	Окремий фрагмент документації (глава, том) повинен описувати захисні механізми, надавані СКІ, і їхня взаємодія між собою, містити рекомендації з їх використання
Керівництво адміністратора по засобам ІБ	Керівництво повинне містити відомості про функції й привілеї, якими управляє системний адміністратор за допомогою механізмів ІБ
Тестова документація	Розроблювач системи повинен представити експертній раді документ, що містить план тестів, процедури прогону тестів і результати тестів
Опис архітектури	Повинні бути описані підходи до ІБ, використовувані виробником, і застосування цих підходів при реалізації системи. Якщо база складається з декількох модулів, повинен бути описаний інтерфейс між ними
Клас С2 усі суб'єкти й об'єкти ОС мають унікальні ідентифікатори. Усі дії всіх суб'єктів доступу, не дозволені явно, заборонені. Події, потенційно небезпечні для підтримки захищеності ОС, реєструються у спеціальному журналі (журналі аудита), працювати з яким можуть тільки привілейовані користувачі. Уся інформація, що видаляється з ОП ПК або із зовнішніх носіїв інформації, видаляється фізично й не може бути надалі доступна жодному суб'єкту доступу	
Довільне керування доступом	Права доступу повинні гранулюватися з точністю до користувача. Механізм керування повинен обмежувати поширення прав доступу – тільки авторизований користувач може надавати права доступу іншим користувачам. Усі об'єкти повинні піддаватися контролю доступу

Продовження табл. 10.1

1	2
Повторне використання об’єктів	При виділенні збереженого об’єкта з пулу ресурсів надійної системи необхідно ліквідувати всі сліди попередніх використань
Ідентифікація й автентифікація	Кожний користувач системи повинен унікальним образом ідентифікуватися. Кожна дія, яка регіструється, повинна асоціюватися з конкретним користувачем
Аудит	Надійна система повинна створювати, підтримувати й захищати журнал реєстраційної інформації доступу до об’єктів, контрольованим системою. Повинна бути можливість реєстрації таких подій: використання механізму ідентифікації й автентифікації; внесення об’єктів в адресний простір користувача (наприклад, відкриття файла, запуск програми); видалення об’єктів; дії системних операторів, системних адміністраторів, адміністраторів ІБ; інші події, що зачіпають ІБ. Кожний реєстраційний запис повинен включати такі поля: дата, тип і час події; ідентифікатор користувача; результат дії (успіх або невдача). Для подій ідентифікації/автентифікації реєструється ідентифікатор пристрою (термінала). Для дій з об’єктами реєструються імена об’єктів. Системний адміністратор може вибирати набір подій, які регіструються для кожного користувача
Операційна гарантованість	Система повинна ізолювати ресурси, що захищаються згідно з вимогами контролю доступу й підзвітності
Тестування	До С1 тестування повинне підтвердити відсутність очевидних недоліків у механізмах ізоляції ресурсів і захисту реєстраційної інформації
Керівництво адміністратора із засобів ІБ	Повинні описуватися процедури обробки реєстраційної інформації й керування файлами з такою інформацією, а також структура записів для кожного типу подій
Клас В1 підтримується повноважне (мандатне) розмежування доступу до об’єктів ОС. Підтримується маркування експортованої інформації	
Мітки ІБ	Надійна ОС повинна управляти мітками ІБ, асоційованими з кожним суб’єктом і збереженим об’єктом. Мітки є основою функціонування механізму примусового керування доступом. При імпорті непоміченої інформації відповідний рівень таємності повинен запитуватися в авторизованого користувача й всі такі дії варто протоколювати

Продовження табл. 10.1

1	2
Цілісність міток ІБ	Мітки повинні адекватно відбивати рівні таємності суб'єктів і об'єктів. При експорті інформації мітки повинні перетворюватися в точне й яке однозначно трактується зовнішнє подання, що супроводжує дані. Кожний пристрій уведення/виводу (у тому числі комунікаційний канал) повинен трактуватися як однорівневий або багаторівневий. Усі зміни трактування й асоційованих рівнів таємності повинні протоколюватися
Примусове керування доступом	Надійна система повинна забезпечити проведення в життя примусового керування доступом всіх суб'єктів до всіх збережених об'єктів. Суб'єктам і об'єктам повинні бути привласнені влучні ІБ, що є комбінацією впорядкованих рівнів таємності, а також категорій. Мітки є основою примусового керування доступом. Надійна СКІ повинна підтримувати, принаймні, два рівні таємності. Суб'єкт може читати об'єкт, якщо його (суб'єкта) мітка ІБ домінує над міткою ІБ об'єкта, тобто рівень таємності суб'єкта не менше рівня таємності об'єкта й усіх категорій об'єкта входять у мітку ІБ суб'єкта. Суб'єкт може записувати в об'єкт дані, якщо мітка ІБ об'єкта домінує над міткою суб'єкта. Надійна система повинна контролювати ідентифікаційну й автентифікаційну інформацію. При створенні нових суб'єктів (наприклад, процесів) їхньої мітки ІБ не повинні домінувати над міткою їхнього користувача
Ідентифікація й автентифікація	На додаток до С2 надійна система повинна підтримувати мітки ІБ користувачів
Аудит	На додаток до С2 повинні реєструватися операції видачі на печатку й асоційовані зовнішні подання міток ІБ. При операціях з об'єктами, крім імен, реєструються їхні мітки ІБ. Набір подій, що регістрируються може розрізнятися залежно від рівня таємності об'єктів
Верифікація специфікацій архітектури	Повинна існувати неформальна або формальна модель ПІнБ, підтримувана надійною системою. Модель повинна відповідати основним посилкам ПІнБ протягом життєвого циклу системи
Опис архітектури	До С1 повинен бути представлений неформальний або формальний опис моделі ПІнБ, проведеної в життя надійною СКІ. Необхідна наявність аргументів на користь достатності вибраної моделі для реалізації ПІнБ. Повинні бути описані захисні механізми бази і їхнє місце в моделі

Продовження табл. 10.1

1	2
Керівництво адміністратора по засобах ІБ	До С2 керівництво повинне описувати функції оператора й адміністратора, що зачіпають ІБ, у тому числі дії щодо зміни характеристик користувачів. Представляються рекомендації з погодженого й ефективного використання засобів ІБ, їхній взаємодії один з одним, по безпечній генерації нових версій надійної системи
Операційна гарантованість	До С2 надійна система повинна забезпечувати взаємну ізоляцію процесів шляхом поділу їх адресних просторів
Тестування	До С2 група фахівців, що повністю розуміють конкретну реалізацію надійної системи, повинна піддати опис архітектури, вихідні й об'єктні коди ретельному аналізу й тестуванню. Мета повинна полягати у виявленні всіх дефектів архітектури й реалізації, що дозволяють суб'єктові без належної авторизації читати, змінювати, видаляти інформацію або приводити систему в стан, коли вона перестає обслуговувати запити інших суб'єктів. Усі виявлені недоліки повинні бути виправлені або нейтралізовані, після чого система піддається повторному тестуванню, щоб переконатися у відсутності недоліків
Клас В2 Підсистема захисту ОС реалізує формально певну й чітко документовану модель ІБ. Здійснюється контроль схованих каналів витоку інформації. Інтерфейс підсистеми захисту чітко й формально визначені, її архітектура й реалізація повністю документовані. Висуваються більше тверді вимоги до ідентифікації, автентифікації й розмежуванню доступу	
Мітки ІБ	На додаток до В1 повинні позначатися всі ресурси системи, прямо або побічно доступні суб'єктам
Цілісність міток ІБ	На додаток до В1 надійна СКІ повинна негайно сповіщати термінального користувача про зміну його мітки ІБ. Користувач може запросити інформацію про свою мітку. Надійна система повинна підтримувати присвоювання всім підключеним фізичним пристроям мінімального й максимального рівня таємності. Ці рівні повинні використовуватися при проведенні в життя обмежень, що накладаються фізичною конфігурацією системи
Примусове керування доступом	На додаток до В1 всі ресурси системи (у тому числі ПЗУ, пристрою уведення/виводу) повинні мати мітки ІБ і служити об'єктами примусового керування доступом
Аудит	На додаток до В1 повинна бути можливість реєструвати події, пов'язані з організацією таємних каналів з пам'яттю

Продовження табл. 10.1

1	2
Надання надійного шляху	Надійна система повинна підтримувати надійний комунікаційний шлях до себе для користувача, що виконує операції початкової ідентифікації й автентифікації. Ініціатива виходить винятково від користувача
Операційна гарантованість	На додаток до В1 надійна СКІ внутрішньо структурована на добре певні, відносно незалежні модулі. Надійна система ефективно використовує наявне устаткування для відділення елементів, критично важливих з погляду ІБ, від інших компонентів СКІ. Модулі системи проектуються з урахуванням принципу мінімізації привілеїв. Для захисту логічно роздільних збережених об'єктів використовуються АЗ (сегментація). Повинен бути визначений користувальницький інтерфейс до СКІ й всі елементи бази
Цілісність системи: аналіз схованих КПІ	Системний архітектор ретельно аналізує можливості щодо організації схованих каналів з пам'яттю й оцінити максимальну пропускну здатність кожного з них
Надійне адміністрування	Система повинна підтримувати поділ функцій оператора й адміністратора
Тестування	На додаток до В1 повинна бути продемонстрована відносна стійкість надійної системи до спроб проникнення
Верифікація специфікацій архітектури	На додаток до В1 модель ПІнБ повинна бути формальною. Для надійної системи повинні існувати описові специфікації верхнього рівня, точно й повно визначальний її інтерфейс
Конфігураційне керування (КК)	У процесі розробки й супроводу надійної ОС повинна використовуватися система КК, що забезпечує контроль за змінами в специфікаціях верхнього рівня, інших архітектурних даних, реалізаційної документації, вихідних текстах, версії об'єктного коду, що працює, тестових даних і документації. КК повинне забезпечувати відповідність один одному аспектів поточної версії ОС. Повинні надаватися засоби генерації нових версій системи за вихідними текстами і засобами для порівняння версій
Керівництво адміністратора по засобах ІБ	На додаток до В1 повинні бути зазначені модулі надійної системи, що містять механізми перевірки обігів. Повинна бути описана процедура безпечної генерації нової версії системи після внесення змін у вихідні тексти
Тестова документація	До С1 тести повинні підтверджувати дієвість заходів щодо зменшення пропускної здатності таємних КПІ

Продовження табл. 10.1

1	2
Опис архітектури	До В1 модель ПІнБ повинна бути формальною й доказовою. Повинно бути показано, що описові специфікації верхнього рівня точно відбивають інтерфейс надійної ОС. Повинно бути показано, як система реалізує концепцію монітора обігів, чому вона стійка до спроб відстеження її роботи, чому її не можна обійти й чому вона реалізована коректно. Повинна бути описана структура ОС, щоб полегшити її тестування й перевірку дотримання принципу мінімізації привілеїв. Документація повинна містити результати аналізу таємних КПІ й опис мір протоколювання, що допомагають виявляти канали з пам'яттю
Клас В3	
Довільне керування доступом	На додаток до С2 повинні обов'язково використовуватися списки керування доступом (ACL) із вказівкою дозволених режимів. Повинна бути можливість явної вказівки користувачів або їхніх груп, доступ яких до об'єкта заборонений
Надання надійного шляху	На додаток до В2 надійний комунікаційний шлях може формуватися за запитом, що виходить як від користувача, так і від самої системи. Надійний шлях може використовуватися для початкової ідентифікації й автентифікації, для зміни поточної мітки ІБ користувача й т. п. Спілкування надійним шляхом повинне бути логічно відділене й ізольоване від інших інформаційних потоків
Аудит	На додаток до В2 повинна бути можливість реєстрації появи або нагромадження подій, що несуть погрозу ПІнБ системи. Адміністратор ІБ повинен негайно сповіщатися про спроби порушення ПІнБ, а система, у випадку продовження спроб, повинна припиняти їх найменш хворобливим способом
Операційна гарантованість	На додаток до В2 надійна СКІ повинна бути спроектована й структурована таким чином, щоб використовувати повний і концептуально простий захисний механізм із точно певною семантикою. Цей механізм повинен відігравати центральну роль у внутрішній структуризації СКІ. База повинна активно використовувати поділ по рівнях, абстракцію й інкапсуляцію даних. Значні інженерні зусилля повинні бути спрямовані на зменшення складності СКІ й на винесення з її модулів, що не є критично важливими

Продовження табл. 10.1

1	2
Цілісність системи: аналіз схованих КПІ	На додаток до В2 аналогічна процедура повинна бути пророблена для тимчасових каналів зв'язку
Надійне адміністрування	До В2 повинна бути специфікована роль адміністратора ІБ. Дістати права адміністратора ІБ можна тільки після виконання явних дій, які протоколюються. Не належні до захисту дії адміністратора ІБ повинні бути обмежені
Надійне відновлення	Повинні існувати процедури й/або механізми, що дозволяють зробити відновлення після збою або іншого порушення роботи без ослаблення захисту
Тестування	На додаток до В2 повинна бути продемонстрована стійкість надійної системи до спроб проникнення. Не повинно бути виявлено архітектурних недоліків. Допускається виявлення лише невеликого числа поправних недоліків реалізації. Повинна існувати обґрунтована впевненість, що деякі недоліки залишилися не виявленими
Верифікація специфікацій архітектури	На додаток до В2 повинні бути наведені переконливі аргументи відповідності між специфікаціями й моделлю
Керівництво адміністратора із засобів ІБ	До В2 повинна бути описана процедура, що забезпечує ІБ початкового запуску системи й поновлення її роботи
Опис архітектури	На додаток до В2 повинне бути неформально продемонстрована відповідність між описовими специфікаціями верхнього рівня й реалізацією надійної системи
Клас А1	
Цілісність системи: аналіз схованих КПІ	До В3 для аналізу повинні використовуватися формальні методи
Тестування	На додаток до В3 тестування повинне продемонструвати, що реалізація надійної системи відповідає формальним специфікаціям верхнього рівня. Основу тестування засобів захисту від проникнення в систему повинне становити ручне або інше відображення специфікацій на вихідні тексти
Верифікація специфікацій архітектури	Представляються формальні специфікації верхнього рівня, що ставляться до апаратного й/або мікропрограмним елементам, що становлять інтерфейс надійної ОС. Комбінація формальних і неформальних методів підтверджує відповідність між специфікаціями й моделлю. Використовуються сучасні методи формальної специфікації й верифікації систем. Ручне або інше відображення формальних специфікацій на вихідні тексти повинне підтвердити коректність реалізації надійної ОС

Закінчення табл. 10.1

1	2
Конфігураційне керування	Механізм конфігураційного керування поширюється на весь життєвий цикл і всі компоненти системи, що мають відношення до забезпечення ІБ, включаючи специфікації й документацію. Для захисту еталонної копії матеріалів, що використовуються для генерації надійної системи, використовується комбінація фізичних, адміністративних і технічних мір
Надійне поширення	Підтримується цілісність відповідності між еталонними даними, що описують поточну версію системи, і еталонною копією текстів цієї версії. Повинні існувати процедури, що підтверджують відповідність між клієнтами апаратними й програмними компонентами й еталонною копією
Тестова документація	До B2 повинна бути описана відповідність між формальними специфікаціями верхнього рівня й вихідних текстів
Опис архітектури	На додаток до B3 повинна бути неформально продемонстрована відповідність між формальними специфікаціями верхнього рівня й реалізацією надійної системи

З відомих ОС вимоги класу С2 задовольняють багато версій UNIX, Windows NT, OS/400, VAX/VMS і IBM MVS з пакетом RACF. ОС для ПК, що задовольняють вимоги більш високих класів захисту, не існує. Це пояснюється, з одного боку, великою ресурсоємністю підсистем захисту, що задовольняють вимоги класу В1 і вище, і з іншого боку – труднощами забезпечення нормального функціонування розповсюдженого ПЗ в таких ОС. Якщо вимоги класу С2 дозволяють застосовувати в захищеної ОС ПЗ, розроблене для інших програмних середовищ (наприклад, у Windows NT можна запускати Microsoft Office для Windows 95), то вимоги більш високих класів захисту настільки тверді, що помітно заважають функціонуванню прикладних програм, розроблених без обліку цих вимог. Наприклад, текстовий редактор Microsoft Word, будучи запущений в ОС, що задовольняє вимогам класу В1, буде некоректно функціонувати при одночасному відкритті документів з різним грифом таємності.

У цей час існує більше 20 ОС для комп’ютерів класу "мейнфрейм" і "суперЕОМ", що задовольняють вимогам класу В1, і, принаймні, одна ОС (Bell Multics), що задовольняє вимогам класу В2.

Теорема 1.1. Збільшити ступінь захищеності або підвищити клас захисту системи, визначеної за більш низьким класом, можна за допомогою зовнішніх засобів.

Доказ. Розглянемо ситуацію збільшення рівня захищеності від класу С1 до класу С2.

Візьмемо до уваги, що всі вимоги класу С1 виконані.

1. Унікальність ідентифікаторів об’єктів і суб’єктів забезпечується використанням унікальних символьних імен (отже, й ідентифікаторів), файлів, груп, користувачів або кодів для кожного окремого об’єкта/суб’єкта.

2. Заборона всіх дій для всіх суб’єктів забезпечується призначенням групі користувачів права заборони всіх операцій, і тільки необхідні явно дозволяються в ПІнБ ОС.

3. Реєстрація потенційно небезпечних подій в ОС забезпечується трьома журналами (системним, безпеки й додатків), керування якими здійснюється через ПІнБ, крім того, можна використовувати зовнішні реєстратори "третіх" фірм, безліч яких на сьогодні досить велика – доступ до них, природно, також регламентується через ПІнБ ОС.

4. Видалення інформації забезпечується спеціальними програмами, які називають "шредери", знижувачі або вайпери зовнішніх фірм-розробників (наприклад, WipeInfo з пакета утиліт Norton Utilities).

Таким чином, ми виконали всі вимоги класу ІБ С2. Аналогічним образом можна довести можливість приведення рівня захищеності системи до наступних вищих класів ІБ.

За більш ніж 25 років, що пройшли із часу розробки вимог ЖК, багато які з них уже застаріли. З’явився цілий ряд нових вимог до ІБ СКІ, які не відображені в ЖК. Це пов’язане з тим, що за цей час був відкритий цілий ряд раніше невідомих погроз ІБ СКІ.

До основних недоліків ЖК відносяться такі:

зовсім не розглядаються криптографічні засоби ЗІ [198];

практично не розглядаються питання, пов’язані із забезпеченням захисту системи від атак, спрямованих на тимчасовий вивід системи з ладу (атаки типу "відмова в обслуговуванні – DoS");

не приділяється належної уваги питанням захисту від негативних впливів програмних закладок і КВ;

недостатньо докладно розглядаються питання взаємодії декількох екземплярів захищених систем у локальній або глобальній СКІ;

вимоги до засобів захисту від витоку конфіденційної інформації із захищеної системи орієнтовані на зберігання конфіденційної інформації в БД і не придатні для захисту електронного документообігу.

Керівні документи Держтехкомісії Росії

У 1992 році Держтехкомісія при Президенті Російської Федерації опублікувала п’ять керівних документів, присвячених питанням захисту СКІ [87; 178]. Розглянемо найважливіші з них: "Засоби обчислювальної техніки. Захист від НСД до інформації. Показники захищеності від НСД до інформації" і "Автоматизовані системи. Захист від НСД до інформації. Класифікація автоматизованих систем і вимоги до захисту інформації".

У першому документі розглядаються вимоги до забезпечення захищеності окремих програмно-апаратних елементів захищених СКІ. Під ЗОТ розуміються не тільки апаратні засоби, але й "сукупність програмних і технічних елементів систем обробки даних, здатних функціонувати самостійно або в складі інших систем". Установлено сім класів захищеності ЗОТ. Найнижчі вимоги пред’являються до класу 7, найвищі – до класу 1. Вимоги цих класів в основному відповідають аналогічним вимогам ЖК, при цьому клас 7 відповідає класу D1 ЖК, клас 6 — класу C1, ... , клас 1 – класу A1. З найбільш істотних відмінностей слід зазначити такі:

починаючи із класу 5 уводяться вимоги, пов’язані з підтримкою цілісності комплексу засобів захисту ОС, які підсилюються в класах 4 і 3;

у класі 5 вимоги до процедур ідентифікації й автентифікації користувачів трохи менш сильні, чим у відповідному йому класі C2 ЖК;

починаючи із класу 4 вимоги до заборони повторного використання вилученої інформації більш сильні, ніж у ЖК.

Другий документ, що стосується АС, вводить стандарти захищеності не окремих програмно-апаратних засобів захисту, а всієї СКІ, що захищається у цілому. Система стандартів цього документа істотно відрізняється від аналогічної системи стандартів ЖК. Усі АС розділяються на три групи, у кожній з яких вводиться своя ієрархія класів захисту. Усього вводиться дев’ять класів захисту, вимоги яких у застосуванні до ОС викладаються нижче.

Група 3. Однокористувальницькі системи.

Клас 3Б. Перевірка дійсності користувача при вході в систему. Реєстрація входу і виходу користувачів із системи. Облік використовуваних зовнішніх носіїв інформації.

Клас 3А. Виконуються усі вимоги класу 3Б. Реєстрація друку документів. Фізичне очищення областей оперативної і зовнішньої пам'яті.

Група 2. Багатокористувальницькі системи, у яких користувачі мають однакові повноваження доступу до всієї інформації.

Клас 2Б. Перевірка дійсності користувача при вході в систему. Реєстрація входу і виходу користувачів із системи. Облік використовуваних зовнішніх носіїв інформації.

Клас 2А. Виконуються усі вимоги класу 2Б. Вибірне розмежування доступу. Реєстрація подій, потенційно небезпечних для підтримки захищеності системи. Фізичне очищення областей оперативної й зовнішньої пам'яті. Наявність підсистеми шифрування конфіденційної інформації, що використовує сертифіковані алгоритми.

Група 1. Багатокористувальницькі системи, у яких користувачі мають різні повноваження доступу до інформації.

Клас 1Д. Перевірка дійсності користувача при вході в систему. Реєстрація входу і виходу користувачів із системи. Облік використовуваних зовнішніх носіїв інформації.

Клас 1Г. Виконуються усі вимоги класу 1Д. Вибірне розмежування доступу. Реєстрація подій, потенційно небезпечних для підтримки захищеності системи. Фізичне очищення областей ОП й зовнішньої пам'яті.

Клас 1В. Виконуються усі вимоги класу 1Г. Повноважне розмежування доступу. Посилені вимоги до підсистеми реєстрації подій, потенційно небезпечних для підтримки захищеності системи. Інтерактивне оповіщення адміністраторів системи про спроби НСД.

Клас 1Б. Виконуються усі вимоги класу 1В. Наявність підсистеми шифрування конфіденційної інформації, що використовує сертифіковані алгоритми.

Клас 1А. Виконуються усі вимоги класу 1Б. Різні суб'єкти доступу мають різні ключі, використовувані для шифрування конфіденційної інформації.

Неважко бачити, що вимоги до захищеності систем класів 3Б, 2Б і 1Д (мінімальний захист у кожній групі) збігаються один з одним і становлять трохи посилену версію класу С1 ЖК (і відповідного йому класу 6 для ЗОТ). Вимоги класу 1Г в основному збігаються з вимогами класу С2 ЖК, а клас 1В з розглянутого документа дуже схожий на клас В1 ЖК.

Аксіома 2.1. Відмінності вимог Держтехкомісії від вимог ЖК у найпоширенішому діапазоні захищеності ОС (С2-В1 по ЖК і 1Г-1В за документами Держтехкомісії), незначні.

Гармонізовані критерії європейських країн

Випливаючи шляхом інтеграції, європейські країни прийняли погоджені Критерії ІБ ІТ (Information Technology Security Evaluation Criteria, ITSEC). Виклад ґрунтується на версії 1.2 цих Критеріїв, опублікованої в червні 1991 року від імені відповідних органів чотирьох країн – Франції, Німеччини, Нідерландів і Великобританії [160]. Вигода від використання погоджених критеріїв очевидна для всіх – для виробників і для споживачів, також для самих органів сертифікації.

Принципово важливою рисою Європейських Критеріїв (ЄК) є відсутність апріорних вимог до умов, у яких повинна працювати СКІ. Нагадаємо, що в "Критеріях" МО США [190] очевидна прив'язка до умов урядової системи, що обробляє секретну інформацію. Так званий спонсор, тобто організація, що запитує сертифікаційні послуги, формулює мету оцінки, тобто описує умови, у яких повинна працювати система, можливі погрози її ІБ і надані нею захисні функції. Завдання органа сертифікації – оцінити, наскільки повно досягаються поставлені цілі, тобто наскільки коректні й ефективні архітектура й реалізація механізмів ІБ в описаних умовах. Таким чином, у термінології ЖК, ЄК ставляться до гарантованості ІБ роботи системи. Вимоги до ПІнБ і до наявності захисних механізмів не є складовою частиною ЄК. Втім, щоб полегшити формулювання мети оцінки, ЄК містять як додаток опис десяти зразкових класів функціональності, типових для урядових і комерційних систем.

ЄК розглядають такі складові ІБ: **конфіденційність**, **цілісність**, **доступність**.

Набір функцій ІБ може специфікуватися з використанням посилань на заздалегідь певні класи функціональності. В ЄК таких класів десять. П'ять із них (F-C1, F-C2, F-B1, F-B2, F-B3) відповідають класам ІБ ЖК.

Клас F-IN призначається для об'єктів оцінки з високими потребами по забезпеченню цілісності даних і програм, що є типовими для СУБД. При описі класу F-IN вводиться поняття ролі, висувається вимога по наданню доступу до певних об'єктів тільки за допомогою визначених процесів. Повинні розрізнятися наступні види доступу: читання, запис, додавання, видалення, перейменування (для всіх об'єктів), виконання, видалення, перейменування (для виконуваних об'єктів), створення й видалення об'єктів.

Клас F-AV характеризується підвищеними вимогами до доступності. Це істотно, наприклад, для АСУ ТП. У розділі "Надійність обслугову-

вання" опису цього класу специфікується, що об’єкт оцінки повинен відновлюватися після відмови окремого апаратного компонента таким чином, щоб всі критично важливі функції залишалися постійно доступними. Те ж повинне бути правильним для вставки відремонтованого компонента, причому після цього об’єкт оцінки вертається в стан, стійкий до одиночних відмов. Незалежно від рівня завантаження повинен гарантуватися час реакції на певні події й відсутність глухих кутів.

Клас F-DI характеризується підвищеними вимогами до цілісності переданих даних. Перед початком спілкування сторони повинні перевірити дійсність один одного. При одержанні даних повинна надаватися можливість перевірки дійсності джерела. При обміні даними повинні надаватися засоби контролю помилок і їхнього виправлення. Зокрема, повинні виявлятися всі ушкодження або навмисні перекручування адресної й користувальницької інформації. Знання алгоритму виявлення перекручувань не повинне давати можливість робити нелегальну модифікацію. Повинні виявлятися й трактуватися як помилки спроби відтворення раніше переданих повідомлень.

Клас F-DC характеризується підвищеними вимогами до конфіденційності переданої інформації. Перед надходженням даних у КПІ повинне автоматично виконуватися шифрування з використанням сертифікованих засобів. На прийомному кінці також автоматично виробляється розшифровка. Ключі шифрування повинні бути захищені від НСД.

Клас F-DX характеризується підвищеними вимогами й до цілісності і конфіденційності інформації. Його можна розглядати як об’єднання класів F-DI і F-DC з додатковими можливостями шифрування, що діють від краю до краю, і з захистом від аналізу трафіка по певним каналам. Повинен бути обмежений доступ до раніше переданої інформації, що у принципі може сприяти нелегальній розшифровці.

Рівні коректності від Е1 до Е6 вибудувані за наростанням вимог до старанності оцінки. Так, на рівні Е1 аналізується лише загальна архітектура об’єкта – вся інша впевненість може бути наслідком функціонального тестування. На рівні Е3 до аналізу залучаються вихідні тексти програм і схеми апаратури. На рівні Е6 потрібний формальний опис функцій ІБ, загальної архітектури, а також моделі ПІнБ. Загалом, розподіл вимог за рівнями гарантованості в ЄК відповідає аналогічному розподілу для класів ІБ С1 – А1 з ЖК.

Стандарт BS 7799

Продовжуючи розгляд стандартів і специфікацій, що ставляться до адміністративного й процедурного рівнів ІБ, розглянемо дві частини британського стандарту BS 7799, що фактично має статус міжнародного (ISO/IEC 17799).

Стандарт складається з двох частин – BS 7799-1 і BS 7799-2, які були прийняті в 2005 році Міжнародною організацією зі стандартизації (Британський інститут стандартів є одним із засновників ISO) і Міжнародною електротехнічною комісією як ISO/IEC 17799 і ISO/IEC 27001.

Перша частина стандарту, іменована "Керування ІБ. Практичні правила", містить систематичний, досить повний, універсальний перелік регуляторів ІБ, корисний для організації будь-якого розміру при веденні бізнесу. Вона призначена для використання як довідковий документ керівниками й рядовими співробітниками, відповідальними за планування, реалізацію й підтримку внутрішньої СІБ. Відповідно до стандарту, мета ІБ – забезпечити безперебійну роботу організації, запобігти й/або мінімізувати збиток від порушень ІБ.

Керування ІБ дозволяє колективно використовувати дані, одночасно забезпечуючи їхній захист і захист ресурсів. Підкреслюється, що захисні міри виявляються значно більш дешевими й ефективними, якщо вони закладені в СКІ і сервіси на стадіях завдання вимог і проектування.

Пропоновані в першій частині стандарту регулятори безпеки розбиті на десять груп:

ПІнБ;

загальорганізаційні аспекти захисту;

класифікація активів і керування ними;

безпека персоналу;

фізична безпека й безпека навколишнього середовища;

адміністрування систем і мереж;

керування доступом до систем і мереж;

розробка й супровід СКІ;

керування безперебійною роботою організації;

контроль відповідності вимогам.

У стандарті виділяється десять ключових регуляторів, які або є обов’язковими відповідно до діючого законодавства, або вважаються структурними основними елементами ІБ. До них відносяться:

документ про ПІнБ;

розподіл обов’язків із забезпечення ІБ;

навчання й підготовка персоналу до підтримки режиму ІБ;

повідомлення про випадки порушення захисту;

антивірусні засоби;

процес планування безперебійної роботи організації;

контроль над копіюванням ПЗ, захищеного законом про авторське право;

захист документації;

захист даних;

контроль відповідності ПІнБ.

Для забезпечення підвищеного рівня захисту особливо цінних ресурсів або надання протидії зловмиснику з винятково високим потенціалом нападу можуть знадобитися інші (більш сильні) засоби, які в стандарті не розглядаються.

Такі фактори виділені в якості начальних для успішної реалізації СІБ в організації:

мета безпеки і її забезпечення повинна ґрунтуватися на виробничих завданнях і вимогах. Функції керування безпекою повинне взяти на себе керівництво організації;

необхідна явна підтримка й прихильність щодо дотримання режиму безпеки з боку вищого керівництва;

потрібне гарне розуміння *ризиків* (як погроз, так і вразливостей), яким піддаються активи організації, й адекватне подання про цінність цих активів;

необхідне ознайомлення із СІБ всіх керівників і рядових співробітників організації.

У другій частині стандарту BS 7799-2:2002 "Системи керування ІБ – специфікація з посібником для використання" предметом розгляду є система управління ІБ.

Під системою *управління ІБ* (СУІБ) (Information Security Management System, ISMS) розуміється частина загальної СІБ, що базується на аналізі *ризиків* і призначена для проектування, реалізації, контролю, супроводу й удосконалення мір в області ІБ. Основу системи складають організаційні структури, ПІнБ, дії з планування, обов’язки, процедури, процеси й ресурси.

В основу керування покладена четирьохфазна модель, що включає: планування, реалізацію, оцінку, коректування.

Модель можна назвати ПРОК (в оригіналі – Plan-Do-Check-Act, PDCA). Детальний аналіз кожної з виділених фаз і становить основний зміст стандарту BS 7799-2:2002.

COBIT

COBIT, створений в 1996 році асоціацією Information Systems Audit and Control Association і IT Governance Institute, призначений для користувачів і IT-фахівців, а також менеджерів з питань захисту й аудиту. Він вважається непоганим практичним рішенням для керування даними, системами й пов'язаними з ними ризиками.

Ця платформа містить у собі інструментальні засоби для оцінки ефективності реалізації в компанії 34 різних IT-процесів. До їхнього числа ставиться набір критично важливих умов успіху, які задають найкращі практичні рішення для кожного IT-процесу, обґрунтовані моделі для тестування й оцінки продуктивності окремих елементів. Цей стандарт стає необхідним компонентом для компаній, що прагнуть виконати вимоги нормативних актів.

"COBIT має тільки один модуль, спеціальним образом присвячений захисту, але, якщо оцінювати стандарт із більш широких позицій, то він торкається багатьох аспектів забезпечення ІБ, – вважає Майк Нельсон, президент консалтингової фірми SecureNet Technologies, що спеціалізується на захисті інформації. Обмеження проявляються, коли мова йде про деталі реалізації. COBIT докладно описує засоби контролю й цілі, але не пояснює, як їх варто реалізовувати".

ISO 27001

ISO 27001 (Information Security Management – Specification With Guidance for Use) відрізняється надмірною деталізацією. Цей стандарт, заснований на ISO 17799, призначений для створення й підтримки ефективних засобів контролю системи захисту при постійному її вдосконаленні.

Стандарт ISO 27001, опублікований у жовтні 2005 року Міжнародною організацією із стандартів, реалізує принципи налагодження економічного співробітництва й розвитку в керуванні захистом даних і мереж. Він визначає план організації захисту, реалізації, керування й підтримки процесів IT на підприємстві.

"ISO 27001 – це перелік засобів контролю. Він формує більшу частину платформи, необхідної для ефективної програми захисту, – зазначив Пол Проктор, аналітик компанії Gartner. COBIT і ISO 27001, – найпопулярніщі з існуючих стандартів".

ITIL

ITIL становить набір найкращих практичних рішень, опублікованих у вигляді книг і покликаних знизити витрати на використання технологій і підвищити якість сервісів, які надаються у рамках організації. ITIL складається із правил, що описують, як більш ефективно надати сервіси за рахунок удосконалення керування процесами у всіх відділах IT, які підтримують мережі, додатки і БД.

Наприкінці 80-х років британська урядова організація, Центральне агентство з обчислювальної техніці й телекомунікацій (Office of Government Commerce), розробила стандарти, яким повинні слідувати компанії, що надають IT-сервіси уряду Великобританії. ITIL охоплює сім основних напрямів: підтримка сервісу, надання сервісу, планування реалізації керування сервісом, інфраструктура керування IT, керування додатками, керування захистом і підтримка розвитку бізнесу.

"У ITIL основна увага приділена керуванню процесами й наданню сервісів; цей документ досить вузько сфальцьований саме на цих областях, – зазначив Нельсон. – Що стосується безпосередньо захисту, то даний стандарт розглядає його лише як один з компонентів керування сервісами й не зачіпає всіх необхідних компонентів захисту. Втім, він і не був споконвічно призначений для рішення цих проблем".

Рубен Мелендез вважає, що ITIL стає кращою методологією для багатьох виробників і відіграє важливу роль у зміцненні ІБ. Р. Мелендез – президент консалтингової компанії Glomark Group, що працює з IT-компаніями і їх клієнтами над створенням стратегій, що дозволяють забезпечити віддачу від інвестицій.

"Усі компанії, з якими я працюю, використовують ITIL, – зазначив він. – Ми багато зробили разом з CA відносно програмних продуктів, пов’язаних з ІБ. Якщо подивитися їх документи, то під час обговорення питань захисту вони завжди посилаються на ITIL і тільки на нього". За словами Мелендеза, до числа виробників, що активно підтримують ITIL, відносяться,також корпорації Microsoft, Intel і Oracle.

SAS 70

SAS 70 – це стандарт на аудит, створений в 1992 році Американським інститутом сертифікованих бухгалтерів (AICPA). Аудит відповідно до SAS 70 показує, чи проводить незалежна бухгалтерська й аудиторська фірма оцінку засобів контролю IT і пов’язаних з ними процесів у даного постачальника послуг. SAS 70 не припускає наявності заздале-

гідь певного набору цілей і засобів контролю. Аудитори повинні додержуватися стандартів AICPA на збір даних, контроль якості й звітність і готувати для постачальника послуг формальний звіт, у якому викладені висновки, зроблені аудитором за результатами перевірки.

Існує два види звітів: один описує засобу контролю, використовувані постачальником у конкретний момент, а іншої приводить засобу контролю й містить у собі детальне тестування операцій контролю процесів, виконуваних постачальником, як мінімум, протягом півроку.

Постачальники послуг повинні продемонструвати, що вони застосовують адекватні засоби захисту при розміщенні або обробці клієнтської інформації. SAS 70 дозволяє сервісним організаціям надавати інформацію про свої засоби контролю клієнтам і аудиторам цих клієнтів у вигляді уніфікованого звіту.

Таким чином, компанії мають можливість одержувати докладні відомості про засоби контролю постачальника послуг і незалежну оцінку ефективності використання цих засобів контролю. Якщо буде потреба компанії можуть надати цю інформацію своїм аудиторам.

На думку Нельсона, SAS 70 дозволяє довідатися, наскільки ефективні наявні засоби контролю, але не дає можливість з'ясувати, чи використовуються у компанії всі необхідні засоби контролю.

Аксіома 2.2. Кожний з перерахованих стандартів здатний допомогти підприємствам захистити свої системи й дані. Компанії, які прагнуть виробити загальну стратегію захисту, повинні проаналізувати ці платформи, щоб визначити, які з них щонайкраще підходять для реалізації обраної стратегії.

10.2. Ідентифікація та автентифікації у комп'ютерних мережах

З метою забезпечення можливості розмежування доступу до ресурсів AIC і можливості реєстрації подій такого доступу кожен суб'єкт (користувач, процес) і об'єкт (ресурс) автоматизованої системи, що захищається, повинен бути однозначно ідентифікований. Для цього в системі повинні зберігатися спеціальні ознаки кожного суб'єкта й об'єкта, за якими їх можна було б однозначно впізнати [65].

Ідентифікація – це, з одного боку, присвоєння індивідуальних імен, номерів чи спеціальних ідентифікаторів суб'єктам і об'єктам системи, з іншого – це їх розпізнавання (впізнання) за привласненим їм унікальним

ідентифікатором. Наявність ідентифікатора дозволяє спростити процедуру виділення конкретного суб'єкта (визначений об'єкт) з безлічі однотипних суб'єктів (об'єктів). Найчастіше як ідентифікатори застосовуються умовні позначки у вигляді набору символів.

Автентифікація – це перевірка (підтвердження) дійсності ідентифікації суб'єкта чи об'єкта системи. Мета автентифікації суб'єкта – переконатися у тому, що він є саме тим, ким представився (ідентифікувався). Мета автентифікації об'єкта – переконатися, що це саме той об'єкт, який потрібний.

Автентифікація користувачів здійснюється зазвичай шляхом перевірки знання ними паролів (спеціальних секретних послідовностей символів), володіння якими-небудь спеціальними пристроями (картками, ключовими вставками і т. п.) з унікальними ознаками чи шляхом перевірки унікальних фізичних характеристик і параметрів (відбитків пальців, особливостей райдужної оболонки ока, форми зап'ястя рук і т. п.) самих користувачів за допомогою спеціальних біометричних пристроїв.

При цьому до пароля висувають дві конфліктуючі вимоги: він повинен бути досить складними для розкриття і в той же час добре запам'ятовуватися. До цих вимог слід додати кілька рекомендацій з вибору пароля:

1. Пароль повинен включати не менше 6 – 7 символьно-цифрових знаків. При цьому доцільно використовувати цифри і арабські, і римські, літери – і великі, і малі.

2. Пароль не повинен включати однакові цифри, літери, їх комбінації, що повторюються.

3. Як пароль не можна використовувати дату поточного дня, своє прізвище, ім'я, назви мультфільмів, книжок, фільмів, міст, ім'я літературних героїв, особисту інформацію: ім'я чоловіка, телефонний номер, номер автомобіля, кличку собаки, хобі, номер службового кабінету та ін.

4. Не використовуйте послідовність клавіш на клавіатурі.

5. Обирайте пароль, що не має ніякого смислового навантаження для вас.

Засоби ідентифікації й автентифікації повинні бути стійкими до мережних загроз та забезпечувати концепцію єдиного входу в мережу.

Уведення значень користувачем свого ідентифікатора і пароля здійснюється найчастіше з клавіатури. Але можуть використовуватися й

інші типи ідентифікаторів – магнітні картки, радіочастотні безконтактні картки, смарт-карти, електронні таблетки Touch Memory.

Використання біометричних засобів дозволяє здійснювати ідентифікацію й автентифікацію людини одночасно. Біометричні методи (наприклад, сканування відбитків пальців) характеризуються, з одного боку, високим рівнем вірогідності впізнавання користувачів, а з іншого – можливістю помилок розпізнавання першого й другого роду (пропуск чи помилкова тривога) і більш високою вартістю їх систем, що реалізують.

Створення системи захисту інформації в корпоративній мережі СКІ породжує цілий комплекс проблем. У комплексі корпоративна система захисту інформації повинна вирішувати такі завдання:

1) забезпечення конфіденційності інформації;

2) захист від перекручування;

3) сегментування (поділ на частини) й забезпечення індивідуальності ПІнБ для різних сегментів системи;

4) автентифікація користувачів – процес достовірної ідентифікації ототожнення користувача, процесу або пристрою, логічних і фізичних об’єктів мережі для різних рівнів мережного керування;

5) протоколювання подій, дистанційний аудит, захист реєстраційних протоколів та ін.

Таким чином, архітектурну концепцію системи захисту інформації в мережах можна представити у вигляді трьох шарів: засобу захисту мережного рівня, middleware-системи й засоби захисту, пропоновані прикладними системами.

10.3. Методи та засоби інформаційної безпеки в комп’ютерних мережах

Створення систем ІБ (СІБ) в СКІ і ІТ ґрунтується на таких принципах [63; 109].

Системний підхід до побудови системи захисту, що означає оптимальне поєднання взаємозалежних організаційних, програмних, апаратних, фізичних та інших властивостей, підтверджених практикою створення вітчизняних і закордонних систем захисту й застосовуваних на всіх етапах технологічного циклу обробки інформації.

Принцип безперервного розвитку системи. Цей принцип, що є одним із основних для комп'ютерних інформаційних систем, ще більш актуальний для СІБ. Способи реалізації загроз інформації в ІТ безупинно вдосконалюються, а тому забезпечення безпеки СКІ не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні й реалізації найбільш раціональних методів, способів і шляхів удосконалювання СІБ, безперервному контролі, виявленні її вузьких і слабких місць, потенційних каналів витоку інформації й нових способів несанкціонованого доступу.

Поділ і мінімізація повноважень з доступу *до* оброблюваної інформації й процедур обробки, тобто надання як користувачам, так і самим працівникам СКІ мінімуму суворо певних повноважень, достатніх для виконання ними своїх службових обов'язків.

Повнота контролю й реєстрації спроб несанкціонованого доступу, тобто необхідність точного встановлення ідентичності кожного користувача й протоколювання його дій для проведення можливого розслідування, а також неможливість здійснення будь-якої операції обробки інформації в ІТ без її попередньої реєстрації.

Забезпечення надійності системи захисту, тобто неможливість зниження рівня надійності при виникненні в системі збоїв, відмов, навмисних дій зломщика або ненавмисних помилок користувачів і обслуговуючого персоналу.

Забезпечення контролю за функціонуванням СЗІ, тобто створення засобів і методів контролю працездатності механізмів захисту.

Забезпечення засобів боротьби зі шкідливими програмами.

Забезпечення економічної доцільності використання системи захисту, що виражається в перевищенні можливого збитку СКІ і ІТ від реалізації загроз над вартістю розробки й експлуатації СІБ.

У результаті вирішення проблем безпеки інформації сучасні СКІ і ІТ повинні мати такі основні ознаки:

наявність інформації різного ступеня конфіденційності;

забезпечення криптографічного захисту інформації різного ступеня конфіденційності при передачі даних;

ієрархічність повноважень суб'єктів доступу до програм до компонентів СКІ і ІТ (до файлів-серверів, каналів зв'язку й т. п.);

обов'язковим керуванням потоками інформації як у локальних мережах, так і при передачі каналами зв'язку на далекі відстані;

наявність механізму реєстрації й обліку спроб несанкціонованого доступу, подій в СКІ і документів, виведених на друк;

обов'язковість забезпечення цілісності ПЗ й інформації в ІТ;

обов'язковість обліку магнітних носіїв;

наявність фізичної охорони засобів ОТ й магнітних носіїв;

наявність спеціальної служби ІБ системи.

Під час розгляду *структури СІБ* можливий традиційний підхід – виділення підсистем, що забезпечують.

СІБ, як і будь-яка СКІ, повинна мати певні види власного ПЗ, опираючись на які вона буде здатна виконати свою цільову функцію.

1. *Правове забезпечення* – сукупність законодавчих актів, нормативно-правових документів, положень, інструкцій, керівництв, вимоги яких є обов'язковими в рамках сфери їх діяльності в СЗІ.

2. Організаційне забезпечення. Мається на увазі, що реалізація ІБ здійснюється певними структурними одиницями, такими, наприклад, як служба безпеки фірми і її складових структур: режим, охорона та ін.

3. *Інформаційне забезпечення, що* включає в себе відомості, показники, параметри, що лежать в основі рішення завдань, що забезпечують функціонування СІБ. Сюди можуть входити як показники доступу, обліку, зберігання, так і інформаційне забезпечення розрахункових завдань різного характеру, пов'язаних з діяльністю служби безпеки.

4. *Технічне (апаратне) забезпечення.* Передбачається широке використання технічних засобів як для захисту інформації, так і для забезпечення діяльності СІБ.

5. Програмне забезпечення. Маються на увазі різні інформаційні, облікові, статистичні й розрахункові програми, що забезпечують оцінку наявності й небезпеки різних КВІ та способів НСД до інформації.

6. *Математичне забезпечення.* Це – математичні методи, використовувані для різних розрахунків, пов'язаних з оцінкою небезпеки технічних засобів, які мають зловмисники, зон і норм необхідного захисту.

7. Лінгвістичне забезпечення. Сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері забезпечення ІБ.

8. *Нормативно-методичне забезпечення.* Сюди входять норми й регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації; різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах твердих вимог дотри-

мання конфіденційності. Нормативно-методичне забезпечення може бути злите із правовим.

Як правило, завдання керування й контролю вирішуються адміністративною групою, склад і розмір якої залежать від конкретних умов. Дуже часто в цю групу входять адміністратор безпеки, менеджер безпеки й оператори.

Забезпечення й контроль безпеки становлять собою комбінацію технічних і адміністративних мір. За даними закордонних джерел у співробітників адміністративної групи зазвичай 1/3 часу займає технічна робота й близько 2/3 – адміністративна (розробка документів, пов'язаних із захистом СКІ, процедур перевірки системи захисту й т. д.). Розумне поєднання цих заходів сприяє зменшенню ймовірності порушень ПІнБ.

Адміністративну групу іноді називають групою ІБ. Ця група може бути організаційно злита з підрозділом, що забезпечує внутрішньомашинне інформаційне забезпечення, тобто з адміністратором БД. Але частіше вона відособлена від усіх відділів або груп, що займаються керуванням самої СКІ, програмуванням і іншими стосовними до системи, завданнями, щоб уникнути можливого зіткнення інтересів.

До обов'язків співробітників, що входять у цю групу, повинне бути включене не тільки виконання директив вищого керівництва, але й участь у вирішенні всіх питань, пов'язаних із процесом обробки інформації з погляду ІБ. Усі їхні розпорядження, що стосуються цієї області, обов'язкові до виконання співробітниками всіх рівнів і організаційних ланок СКІ і ІТ.

Нормативи й стандарти щодо ЗІ накладають вимоги на побудову ряду компонентів, які традиційно входять у забезпечуючі підсистеми самих СКІ, тобто можна говорити про наявність тенденції до злиття забезпечуючих підсистем СКІ і СІБ [49].

Методи й засоби забезпечення ІБ інформації в СКІ подані на рис. 10.2.

Перешкода – метод фізичного перегородження шляхів зловмисникові для захисту інформації (до апаратури, носіям інформації й т. д.).

Керування доступом – методи захисту інформації регулюванням використання всіх ресурсів СКІ і ІТ. Ці методи повинні протистояти всім можливим шляхам несанкціонованого доступу до інформації. Керування доступом включає такі функції захисту:

ідентифікацію користувачів, персоналу й ресурсів системи (присвоєння кожному об'єкту персонального ідентифікатора);

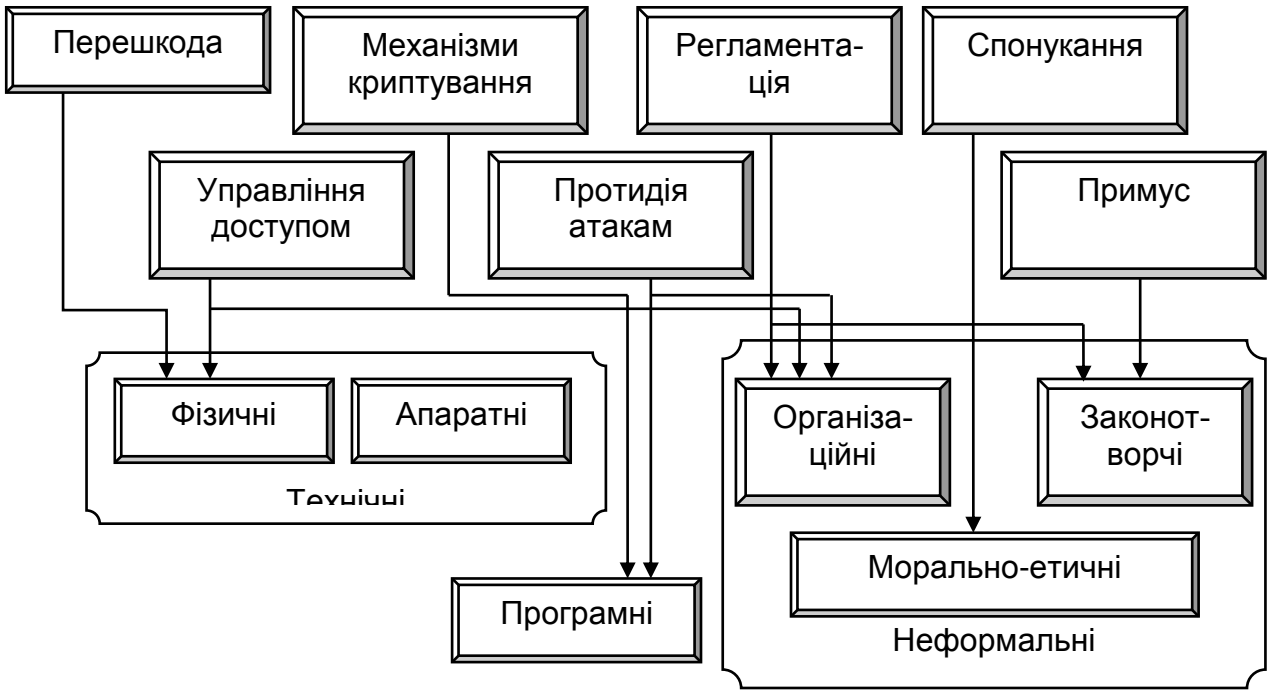


Рис. 10.2. **Методи та засоби забезпечення безпеки інформації**

упізнання (установлення дійсності) об'єкта або суб'єкта за пред'явленим ідентифікатором;

перевірку повноважень (перевірка відповідності дня тижня, часу доби, запитуваних ресурсів і процедур установленому регламенту);

дозвіл і створення умов роботи в межах установленого регламенту;

реєстрацію (протоколювання) звертань до захищених ресурсів;

реагування (сигналізація, відключення, затримка робіт, відмова в запиті й тому подібне) при спробах несанкціонованих дій.

Протидія атакам шкідливих програм припускає комплекс різноманітних заходів організаційного характеру й використання антивірусних програм. Мета прийнятих заходів – це зменшення ймовірності інфікування АІС, виявлення фактів зараження системи; зменшення наслідків інформаційних інфекцій, локалізація або знищення вірусів; відновлення інформації в СКІ. Оволодіння цим комплексом засобів вимагає знайомства зі спеціальною літературою [51].

Регламентація – створення таких умов автоматизованої обробки, зберігання й передачі захищеної інформації, при яких норми й стандарти із захисту виконуються найбільшою мірою.

Примус – метод захисту, при якому користувачі й персонал СКІ змушені дотримуватися правил обробки, передачі й використання захи-

щеної інформації, що під погрозою матеріальної, адміністративної або кримінальної відповідальності.

Спонукання – метод захисту, що спонукує користувачів і персонал СКІ не порушувати встановлені порядки за рахунок дотримання сформованих моральних і етичних норм.

Уся сукупність технічних засобів підрозділяється на апаратні й фізичні.

Апаратні засоби – пристрої, що вбудовуються безпосередньо в ОТ, або пристрої, які сполучаються з нею за стандартним інтерфейсом.

Фізичні засоби включають різні інженерні пристрої й прилади, що перешкоджають фізичному проникненню зловмисників на об'єкти ЗІ й здійснюють захист персоналу (особисті засоби безпеки), матеріальних засобів і фінансів, інформації від протиправних дій. Приклади фізичних засобів: замки на дверях, ґрати на вікнах, засоби електронної охоронної сигналізації й т. п.

Програмні засоби – це спеціальні програми й програмні комплекси, призначені для ЗІ в СКІ. Багато хто з них злиті з ПЗ самої СКІ. Із засобів ПЗ системи захисту виділимо ще програмні засоби, що реалізують механізми шифрування (криптографії). Криптографія – це наука про забезпечення таємності й/або автентичності (дійсності) переданих повідомлень.

Організаційні засоби здійснюють регламентацію виробничої діяльності в СКІ і взаємин виконавців на нормативно-правовій основі таким чином, що розголошення, витік і НСД до конфіденційної інформації стають неможливими або істотно ускладнюються за рахунок проведення організаційних заходів. Комплекс цих заходів реалізується групою інформаційної безпеки, але повинен перебувати під контролем першого керівника.

Законотворчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила користування, обробки й передачі інформації обмеженого доступу й установлюються міри відповідальності за порушення цих правил.

Морально-етичні засоби захисту включають будь-які норми поводження, які традиційно склалися раніше, складаються в міру поширення СКІ і ІТ у країні й у світі або спеціально розробляються. Морально-етичні норми можуть бути неписані (наприклад, чесність) або оформлені в якийнебудь звід (устав) правил або приписань. Ці норми, як правило, не є законодавчо затвердженими, але оскільки їхнє недотримання приводить до зниження престижу організації, вони вважаються обов'язковими для виконання. Характерним прикладом таких приписань є Кодекс професійного поводження членів Асоціації користувачів ПК США.

11. Правові основи інформаційної безпеки

Основні юридичні поняття

Під ***безпекою СКІ*** розуміється захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого одержання) інформації, модифікації або фізичного руйнування її компонентів. Інакше кажучи, це здатність протидіяти різним негативним впливам, **на СКІ.**

Під *загрозою безпеки інформації* розуміються події або дії, які можуть привести до перекручування, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів [42].

Якщо виходити із класичного розгляду кібернетичної моделі будь-якої керованої системи, що здійснюють впливи на неї, можуть носити випадковий характер. Тому серед загроз безпеки інформації варто виділяти як один із видів загрози випадкові*, а*бо *ненавмисні.* Їхнім джерелом можуть бути вихід із ладу апаратних засобів, неправильні дії працівників СКІ або її користувачів, ненавмисні помилки в програмному забезпеченні й т. д. Такі загрози теж варто мати на увазі, тому що збиток від них може бути значним. Однак у даному розділі найбільша увага приділяється загрозам *навмисним,* які на відміну від випадкових мають на меті завдання збитків керованій системі або користувачам. Це робиться часто заради одержання особистого зиску.

Людину, що намагається порушити роботу інформаційної системи й одержати несанкціонований доступ до інформації, зазвичай називають зломщиком, а іноді "комп’ютерним піратом" (хакером). У своїх протиправних діях, спрямованих на оволодіння чужими секретами, зломщики прагнуть знайти такі джерела конфіденційної інформації, які б давали їм найбільш достовірну інформацію в максимальних обсягах з мінімальними втратами на її одержання. За допомогою різного роду хитрощів і безлічі прийомів і засобів підбираються шляхи й підходи до таких джерел. У цьому випадку під джерелом інформації розуміється матеріальний об’єкт, що володіє певними відомостями, які становлять конкретний інтерес для зловмисників або конкурентів.

Захист від навмисних загроз – це свого роду змагання оборони й нападу: хто більше знає, передбачає дійові заходи, той і виграє.

Численні публікації останніх років показують, що зловживання інформацією, яка циркулює в СКІ або передається каналами зв'язку, удосконалювалися не менш інтенсивно, ніж міри захисту від них. У цей час для забезпечення захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємозалежних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних мір протидії й т. д.). Комплексний характер захисту виникає з комплексних дій зловмисників, що прагнуть будь-якими способами добути важливу для них інформацію. Сьогодні можна стверджувати, що народжується нова сучасна технологія – *технологія захисту інформації* в комп'ютерних інформаційних системах і в мережах передачі даних. Реалізація цієї технології вимагає збільшення витрат і зусиль. Однак все це дозволяє уникнути значно переважаючих втрат і збитку, які можуть виникнути при реальному здійсненні загроз СКІ і ІТ.

11.1. Структуризація нормативно-правового забезпечення

Відсутність правового регулювання щодо результатів інтелектуальної діяльності в режимі секретності, зокрема ноу-хау, комерційної таємниці, конфіденційної інформації. Це негативно позначається на загальній вартості підприємств, що їх активно використовують, обмежує можливості щодо капіталізації витрат на створення і придбання цього виду інтелектуальних результатів, гальмує торгівлю ними.

Особливої гостроти проблема обліку інтелектуальної власності як нематеріальних активів набуває в контексті приватизаційних процесів. Акціонування капіталу державних підприємств під час приватизації раніше відбувалося без урахування вартості нематеріальних активів, що часто могли переважати за вартістю матеріальні активи підприємства. Особливо це стосується тих суб'єктів господарювання, які функціонують у галузі, де проводиться значна кількість досліджень і розроблень. Це стало причиною втрати Україною вагомої частини її інтелектуального капіталу. Так, у 2005 – 2007 рр. приватизовано 6 об'єктів науково-технічної сфери, 3 з них продано за ціною, що в кілька разів нижча їх номінальної вартості. Серед них високотехнологічне підприємство Спеціальне конструкторське бюро мікроелектроніки в приладобудуванні (Рішення Комітету з питань науки і освіти ВРУ від 16.04.2008 р. № 14).

На думку західних теоретиків-економістів, успішний розвиток підприємництва істотно залежить від того політико-економічного середовища (командно-адміністративного або ринково-конкурентного), у якому воно здійснює свою діяльність. У зв'язку з розвитком ринкових відносин підприємницьку діяльність у нашій країні доводиться здійснювати в умовах зростаючої невизначеності ситуації й мінливості економічного середовища. Виходить, виникає неясність та невпевненість в одержанні очікуваного кінцевого результату, а отже, зростає ризик, тобто небезпека непередбачених втрат. Особливо це властиво початковим стадіям освоєння підприємництва.

Багато питань на підприємстві регулюються й забезпечуються цивільним, адміністративним, трудовим, авторським, карним та іншим законодавством (повний перелік нормативних актів наведений у додатку А та у джерелах [63; 65; 108]). Вести мову про те, що за допомогою тільки правового регулювання й охорони можна вирішити всі проблеми, що пов'язані із забезпеченням ІБ, не тільки передчасно, але й не можливо здійснити в доступному майбутньому.

У нових ринково-конкурентних умовах виникає маса проблем, які пов'язані із забезпеченням ІБ, майнової власності, а також ІОД, як виду інтелектуальної власності. Для захисту ІОД використовуються як правові, так і спеціальні заходи, а в необхідних випадках комплексне їх застосування. Сукупність ІОД [111; 114; 118; 121; 188], що циркулює на підприємстві умовно групується за напрямами (рис. 11.1).

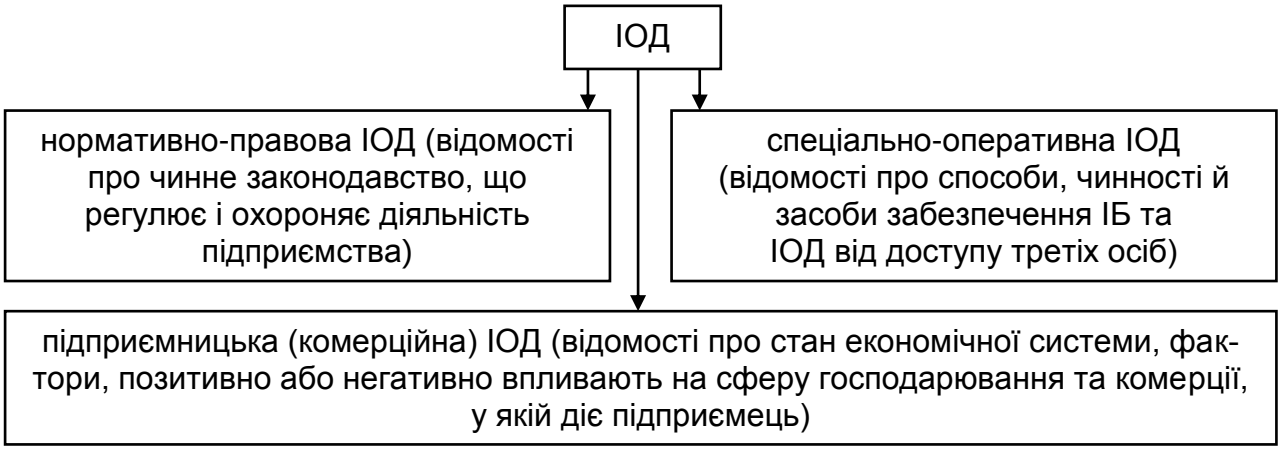


Рис. 11.1. **Групування ІОД, що циркулює на підприємстві**

Використання визначених груп ІОД, а також існуючі взаємовідносини на підприємстві між суб'єктами та об'єктами потребує визначення та створення таксономії нормативно-правового забезпечення СІБ (рис. 11.2).

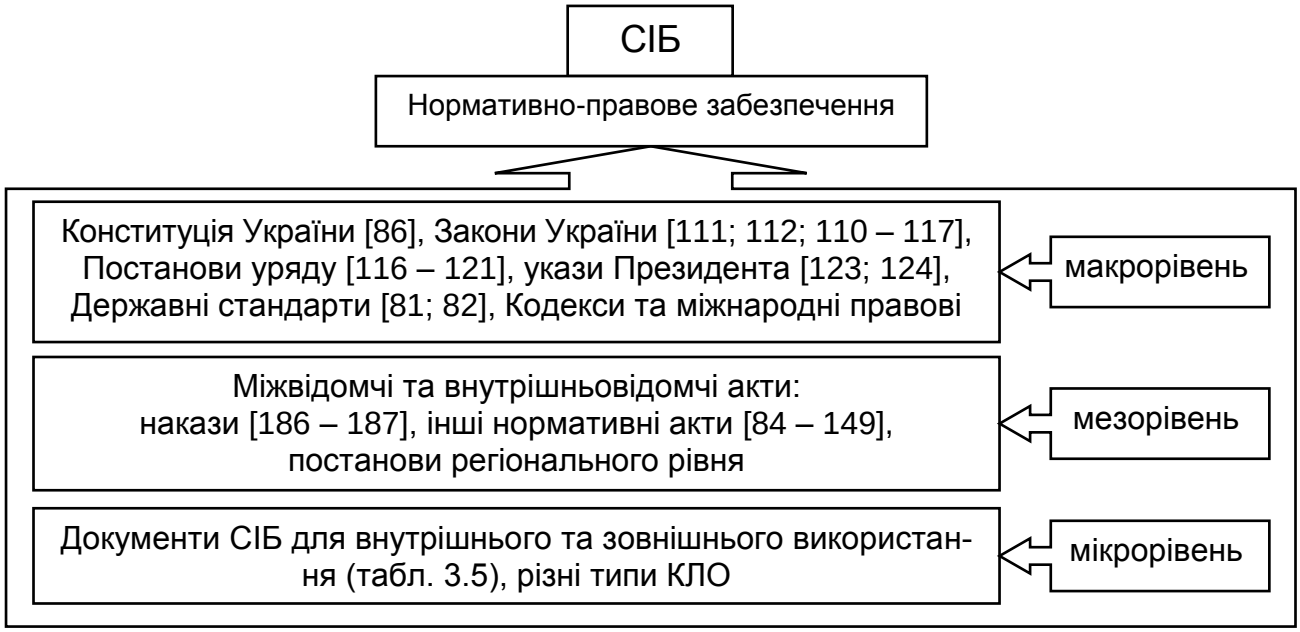


Рис. 11.2. **Таксономія нормативно-правового забезпечення СІБ**

Крім того, на створення та функціонування нормативно-правового забезпечення СІБ істотно впливають такі фактори: діяльність провідних фахівців та професійних організацій; економічні наслідки впровадженої облікової та податкової системи; загальний економічний стан у державі; національні особливості; стан юридичного середовища; джерела фінансування та їх поточний стан; загальна атмосфера в розрізі всіх таксонометричних рівнів.

Усі ці фактори, а також таксономія нормативно-правового забезпечення СІБ вимагають створення різних класифікаційних ознак: нормативно-правового забезпечення СІБ табл. 11.1), видів економічного шахрайства з боку найманих робітників рис. 11.3), видів комерційної, ділової та виробничої ІОД у структурі СІБ рис. 11.4).

Виходячи з аналізу можливих виглядів атак на систему обміну й зберігання електронних документів (ІОД), можна зробити висновок про те, що основним поняттям у системі обміну електронними документами є система автентифікації.

Таблиця 11.1

Класифікаційні ознаки нормативно-правового забезпечення СІБ

Вид забезпечення	Види документів (актів)
1	2
Документи СЕБП	посадові інструкції
	накази

Продовження табл. 11.1

1	2
для внутрішнього та зовнішнього використання	плани
	акти
	інші види інструкцій
	алгоритми (порядки) дій співробітників при виникненні подій
	процедури
	переліки
	протоколи
	паспорта
	типові положення
Кодекси України	про адміністративні правопорушення [84]
	кримінальний [88]
	цивільний [149]
	законів про працю
	інші
Міжнародні правові акти	Загальна декларація прав людини (ООН)
	Європейська конвенція про захист прав людини і основних свобод (Рим, 4 листопада 1950 р.)
	Всесвітня конвенція про авторське право (1952)
	Конвенція про обмін офіційними виданнями і урядовими документами між державами (1958)
Міжнародні правові акти	Конвенція про міжнародний обмін виданнями (1958)
	Конвенція про заснування Всесвітньої організації інтелектуальної власності (1967)
	Бернська конвенція про охорону літературних і художніх творів (1971)
	Конвенція про охорону інтересів виробників фонограм від незаконного відтворення їх фонограм (1971)
	Вашингтонський договір про інтелектуальну власність відносно інтегральних мікросхем (1989)
	Чорноморська конвенція про співробітництво в галузі культури, освіти, науки, інформації (1993)
	Концепція автоматизованої системи інформаційного обміну між державами – учасницями Співдружності Незалежних Держав (1994)
	Постанова Міжпарламентської асамблеї СНД "Про формування в межах Співдружності Незалежних Держав міжнародної системи правової інформації" (1994)
	Угода з торгових аспектів прав інтелектуальної власності (ТРІПС) (1995)

Продовження табл. 11.1

1	2
	Директива Європейського парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" (1995)
	Рекомендації Європейського Союзу ENFOPOL про законний моніторинг електронних мереж (1995)
	Угода Всесвітньої організації інтелектуальної власності з авторського права (ДАП) (1996 – досі не набрала чинності)
	Резолюція Комісії ООН з права міжнародної торгівлі "Про типовий закон з електронної торгівлі" (1996)
	Угода Всесвітньої організації інтелектуальної власності з виконання і фонограм (ДІФ) (1996 – досі не набрала чинності)
	Концепція формування інформаційного простору Співдружності Незалежних Держав (1998)
	Концепція інформаційної безпеки держав – учасниць Співдружності Незалежних Держав (1999)
	Директива Європейського парламенту і Ради "Про правові основи Співтовариства з використання електронних підписів" (1999)
	Рекомендації Комітету Міністрів Ради Європи про захист прав людини в Інтернеті (1999)
	Закон Європейського парламенту "Про електронну комерцію"
	Міжнародна угода про патентне право (PLT) (2000)
	Окінавська хартія глобального інформаційного співтовариства (2000)
	Доктрина інформаційного розвитку людства в XXI столітті (2001)
Кодекс про адміністративні правопорушення [84]	Стаття 164-9. Незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних
	Стаття 195-5. Незаконне придбання або зберігання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації
	Стаття 212-6. Здійснення незаконного доступу до інформації в автоматизованих системах
Кримінальний кодекс [88]	Стаття 176. Порушення авторського права і суміжних прав
	Стаття 359. Незаконне використання спеціальних технічних засобів негласного отримання інформації
	Стаття 360. Умисне пошкодження ліній зв'язку
	Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Закінчення табл. 11.1

1	2
	Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут
	Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації
	Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї
	Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється
	Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

11.2. Структуризація класифікаційних ознак у сфері безпеки

Узагальнення різних точок зору вітчизняних та закордонних авторів дозволяє дати розширене трактування КЛО цієї та інших (рис. 11.4) складних категорій [62].

Основні характеристики системи автентифікації (частина СІБ): час реакції на порушення, необхідні для реалізації обчислювальні ресурси; ступінь захищеності (стійкість) до можливих (відомих на сьогодні) атак на засоби захисту. Крім того, система автентифікації як частина СІБ забезпечує існування поняття комерційна таємниця підприємства як вид ІОД зі своїми особливостями.

Комерційна таємниця підприємства – це відомості, що не є державними секретами й пов'язані з виробництвом, технологічною інформацією, керуванням, фінансами та іншими видами, розголошення (передача, витік) яких може завдати шкоди економічним інтересам підприємства. Така загальна характеристика категорії "комерційна таємниця" підприєм-

ства є законодавчою [121].

<table>
<tr><td>Шахрайство із готівкою з каси</td><td>Використання готівки не за призначенням</td><td>Фальсифікація касових книг</td><td>Підробка чеків</td><td>Фальсифікація звітності про відрядження</td><td>Фальсифікація транспортних накладних</td></tr>
<tr><td>Шахрайство за допомогою чеків</td><td>Фальсифікація записів у бухгалтерських книгах</td><td>Завищення видатків</td><td>Штучне здуття цін</td><td>Включення у звіт про відрядження особистих витрат</td><td>Завищене фактурування</td></tr>
<tr><td>Шахрайство зі страховкою</td><td>Фальсифікація годин переробки</td><td colspan="2" rowspan="2">КЛО видів економічного шахрайства з боку найманих робітників</td><td>Несанкціонований продаж майна фірми</td><td>Змова із клієнтами або постачальниками</td></tr>
<tr><td>Неповернення виданих авансом сум</td><td>Оплата праці тимчасових працівників</td><td>Використання майна фірми</td><td>Фальсифікування податкових декларацій</td></tr>
<tr><td>Не задекларовані доходи</td><td>Шахрайство з рахунками від медичних установ</td><td>Розготівковування незатребуваних чеків</td><td>Переплата "зверху"</td><td>Шахрайство із виплатою заробітної плати</td><td>Маніпуляції із кредитними картками</td></tr>
<tr><td rowspan="2">Використання надходжень у пенсійні фонди не за призначенням</td><td rowspan="2">Використання співробітників, устаткування або матеріалів фірми з особливою метою</td><td rowspan="2">"Кикбеки", тобто одержання "подяки" за певні послуги, різновид хабара</td><td>Завищення цін</td><td rowspan="2">Фальсифікація сум на банківських рахунках</td><td rowspan="2">Видача фальшивих векселів, так званий "кайтинг"</td></tr>
<tr><td>Комп’ютерні злочини</td></tr>
<tr><td>Дрібні крадіжки готівки з каси</td><td>Оплата особистих рахунків чеками фірми</td><td>Подання фальсифікованих рахунків-фактур</td><td>Крадіжки інвентарю</td><td>Надання замовлень за хабарі</td><td>Використання підставних постачальників</td></tr>
</table>

Рис. 11.3. **Класифікаційні ознаки видів економічного шахрайства**

<table>
<tr><td colspan="5">КЛО видів комерційної ІОД</td></tr>
<tr><td>торговельні відносини фірм</td><td>організація та розміри обороту коштів</td><td>про отримування патентів, ліцензій, моделей</td><td>банківські операції</td><td>про постачальників та споживачів</td></tr>
<tr><td>стан ринку збуту</td><td>структура капіталів</td><td>плани інвестицій</td><td>укладені контракти</td><td>формування ціни на товар</td></tr>
<tr><td>дослідницькі роботи</td><td>раціоналізаторські впровадження</td><td colspan="2">нові технології, вироби, обладнання</td><td>результати аналізу конкурентоспроможної продукції</td></tr>
<tr><td colspan="5">розмір прибутку й обсяг виробництва</td></tr>
<tr><td colspan="5">КЛО видів виробничої ІОД</td></tr>
<tr><td>цілі і характер дослідницьких робіт</td><td>організація праці</td><td colspan="2">технічні відкриття й винаходи</td><td>способи виробництва та технології</td></tr>
<tr><td>способи виробництва та технологія</td><td>обсяги виробництва та плани реалізації продукції</td><td colspan="2">рівень запасів</td><td>система організації праці</td></tr>
<tr><td>плани рекламної компанії</td><td>час та умови виходу на ринок</td><td colspan="2">свідомості про поставщиків, клієнтів, конкурентів</td><td>характер та умови укладання контрактів</td></tr>
<tr><td colspan="3">плани інвестувань у реконструкцію виробництва та на нову побудову</td><td colspan="2">методологія організації управління</td></tr>
<tr><td colspan="5">КЛО видів ділової (фінансової) ІОД</td></tr>
<tr><td colspan="5">фінанси підприємства (фінансова звітність, стан розрахунків із клієнтами, заборгованість, кредити, платоспроможність, прибуток, собівартість продукції та ін.)</td></tr>
<tr><td>плани рекламної діяльності</td><td>методи й організація управління</td><td>система організації праці</td><td colspan="2">власна оцінка характеру та репутації персоналу й підприємства</td></tr>
<tr><td>структура капіталів</td><td>дані про банківські та торгові операції</td><td>дані про стан ринків збуту</td><td colspan="2">обсяг прибутку та рівень собівартості продукції</td></tr>
<tr><td>стан рахунків із клієнтами</td><td>рівень платоспроможності підприємства</td><td>механізми формування ціноутворення</td><td colspan="2">свідомості про фінансовий стан постачальників, користувачів, конкурентів</td></tr>
<tr><td colspan="2">свідомості про ефективність експорту та імпорту</td><td colspan="3">організація та розмір оборотних засобів</td></tr>
<tr><td colspan="5">стратегічні й тактичні плани розвитку виробництва, у тому числі з використанням нових технологій, винаходів, ноу-хау</td></tr>
<tr><td colspan="5">плани та обсяги реалізації продукції (плани маркетингу, характер і обсяг торгівельних операцій, рівень цін, складські запаси)</td></tr>
<tr><td colspan="5">аналіз конкурентоспроможності своєї продукції, ефективності експорту та імпорту, передбачуваний час виходу на ринок</td></tr>
<tr><td colspan="5">списки торгівельних та інших клієнтів, конкурентів, відомості про взаємовідносини з ними, їх фінансовий стан, умови контрактів та ін.</td></tr>
</table>

Рис. 11.4. **Класифікаційні ознаки видів комерційної, ділової**

та виробничої ІОД

На додаток до сказаного, на кожному підприємстві при створенні СІБ необхідно правильно організувати [72] такі дії, які становлять частину рекомендацій щодо удосконалення планування стратегічного управління підприємством: облік і охорону деяких видів матеріалів і готових виробів (особливо досвідчених зразків); порядок діловодства з документами, що містять підприємницьку таємницю (правила циркуляції, обліку, зберігання, знищення та ін.); контроль за засобами копіювання й розмноження документів; захист комерційної ІОД в засобах зв'язку й обчислювальної техніки; охорону території підприємства, його основних будинків, споруджень; контроль за відвідуваннями підприємства сторонніми особами.

Одним з елементів таксономії правового забезпечення СІБ є структуризація заходів захисту ІОД (рис. 11.5).

Регламентований перелік відомостей, що відносяться до ІОД підприємства	Система контролю за засобами копіювання й розмноження документів
Система обліку й охорони нових матеріалів і продукції	Порядок захисту ІОД в засобах зв'язку й комп'ютерної техніки
Система охорони території підприємства, його основних будинків і споруджень	Порядок використання відкритих КВІ при передачі ІОД
Система контролю за відвідуванням підприємства сторонніми особами	Система мотивації й навчання персоналу підприємства способам захисту ІОД
Порядок діловодства з документами, що містять ІОД	Спеціалізовані служби з захисту ІОД підприємства

Рис. 11.5. **Структуризація заходів захисту ІОД**

Одним з видів ІОД, що циркулює на підприємстві у структурі СІБ є інформація для службового користування (ДСК), для якої порядок дій та заходів на підприємстві під час використання виду ІОД визначається згідно джерела [186]:

розробку й введення в дію міністерствами, іншими центральними органами виконавчої влади, обласними, Київської й Севастопольської міськими державними адміністраціями переліків конфіденційної інформації, що перебуває в їхньому володінні, користуванні й розпорядженні і

є власністю держави;

присвоєння документам, що містять інформацію відповідно до переліку, гриф обмеженого доступу "ДСК", що передбачає допуск до таких документів лише певних категорій працівників;

здійснення контролю за нерозголошенням відомостей, що втримуються в документах із грифом "ДСК" режимно-секретними підрозділами;

надання громадянам доступу до інформації, що втримується в документах із грифом "ДСК" лише при наявності письмового запиту від організації, у якій працює громадянин, по згоді керівника установи або в масових бібліотеках по аналогічному письмовому клопотанню;

надання представникам ЗМІ доступу після попереднього розгляду конкретних документів експертними комісіями з письмового дозволу керівника установи, що надало документу гриф "ДСК".

Процедура доступу по інструкції, що передбачає використання грифа "ДСК", установлення порядку роботи з документами і їхнє зберігання, умов технічного захисту інформації, функціонування експертних комісій як органа для рішення питання доступу до інформації, нагадує порядок, установлений щодо ІОД, що є державною таємницею [186]. Істотна відмінність укладається у тому, що загальне відношення, пов’язане з віднесенням інформації до державної таємниці, засекречуванням, розсекреченням її матеріальних носіїв і охороною державної таємниці, регулюються відповідним законом, яким, до речі, чітко встановлений перелік інформації, що не може бути віднесена до державної таємниці [186], і забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть змінюватися втримування й обсяг конституційних прав і волі людини й громадянина. Користуючись положеннями інструкції, державні органи не мають змоги привласнювати гриф "ДСК" будь-якому документу, обмеживши таким способом доступ до інформації, що втримується в документі [124]. У підсумку маємо ще вид ІОД, що, при відсутності будь-яких правил щодо втримування й обсягу інформації підлягає категоруванню, фактично ховається від зацікавлених осіб.

Основні способи злочинних дій у системі обміну електронними документами

Загальноприйнятою є модель автентифікації, у якій функціонують чотири учасники: A-передавач, B-приймач, C-супротивник і D-арбітр. A – посилає повідомлення, B – приймає, C – намагається зробити злочинні дії; D – приймає рішення в спірних випадках, тобто визначає, твердження

чиєї сторони з найбільшою ймовірністю є помилковими. Природно, як С можуть виступати А та В. Метою автентифікації документів є захист від можливих видів злочинних дій, серед яких виділимо:

1) активне перехоплення – порушник (що підключився до мережі) перехоплює документи (файли) і змінює їх;

2) порушення конфіденційності;

3) маскарад – абонент С посилає документ від імені абонента А;

4) переробка – абонент В змінює документ і затверджує, що даний документ (змінений) одержав від абонента А;

5) підміна – абонент В формує документ (новий) і заявляє, що одержав його від абонента А;

6) повтор – абонент В повторює раніше переданий документ, що абонент А послав абонентові В;

7) втрата або знищення документа кожним із абонентів;

8) фальсифікація часу відправлення повідомлення;

9) руйнування електронних архівів.

10) ренегатство – абонент А повідомляє, що не посилав повідомлення абонентові В, хоча насправді посилав;

11) відмова від факту одержання – абонент В відмовляється від факту одержання документа від абонента А;

12) компрометація секретного ключа;

13) включення в каталог не верифікованого відкритого ключа;

14) НСД до термінала.

Ці види злочинних дій завдають істотної шкоди функціонуванню банківських, комерційних структур, державним підприємствам і організаціям, приватним особам, що застосовують у своїй діяльності комп'ютерні інформаційні технології. Крім того, можливість злочинних дій підриває довіра до комп'ютерної технології. У зв'язку із цим завдання автентифікації є важливим.

Аксіома. При виборі технології автентифікації повідомлень у мережі необхідно передбачити надійний захист від усіх перерахованих видів злочинних дій.

Основні заходи щодо забезпечення захисту електронних документів

Безпека електронних документів повинна досягатися застосуванням взаємозалежного комплексу заходів, до числа яких належать:

електронний підпис документів;

шифрування повідомлень при передачі каналами зв’язку;
керування ключовою системою;
розмежування повноважень при роботі з електронними документами;
захист на рівні протоколів зв’язку;
захист архівів від руйнування;
існування арбітра;
організаційні заходи.

Основою комплексу заходів із захисту інформації є **електронний підпис**, за відсутності якого важко досягти прийнятного рівня безпеки в системі. Винятком можуть бути ситуації, де існує повна довіра між сторонами, що обмінюються інформацією. У цьому випадку міри захисту повинні бути спрямовані на запобігання можливого проникнення в систему сторонніх осіб.

Електронний підпис повинен виконувати завдання, які виконує підпис, поставлений на документі від руки. Причому ніяких засобів для реалізації контролю дійсності інформації, крім аналізу самої інформації, не існує. Вирішення цієї проблеми стало можливим після створення криптографічних алгоритмів, що дозволяють одній або більше сторонам, що знають секретні частини інформації (ключі), здійснювати операції обробки інформації, які з великою ймовірністю не можуть бути відтворені тими, хто не знає цих секретних ключів.

Тут необхідно використовувати схеми, засновані на двоключовій криптографії. У таких випадках у передавального абонента мережі є свій секретний ключ підпису, а в приймаючого абонента – несекретний відкритий ключ підпису передавального абонента. Цей відкритий ключ можна трактувати як набір перевірочних співвідношень, що дозволяють говорити про істинність підпису передавального абонента, але не дозволяють відновити секретний ключ підпису. Передавальний абонент несе одноосібну відповідальність за свій секретний ключ. Ніхто, крім нього, не в змозі згенерувати коректний підпис. Секретний ключ передавального абонента можна розглядати як особисту печатку, і власник повинен усіляко обмежувати доступ до нього сторонніх осіб.

Принцип їхньої дії заснований на застосуванні однобічних функцій, що дозволяють розділити функції шифрування й дешифрування. При цьому, не знаючи ключа шифрування, що є секретним, можна лише прочитати зашифрований текст.

На практиці, як правило, у схемах підпису замість документа *x* розглядають його хеш-функцію *h(x)*, що володіє рядом спеціальних властивостей, найважливіші з яких – відсутність "колізій", тобто практична неможливість створення двох різних документів з однаковим значенням хеш-функції (ХФ).

Найбільш відомі такі математичні схеми підпису: RSA – названа за першими буквами прізвищ авторів (R. L. Rivest, A. Shamir, L. Adleman), OSS (H. Ong, C. P. Schnorr, A. Shamir), Ель-Гамаля (T. ElGamal), Рабіна (M. Rabin), Окамото-Shiraishi (T. Okamoto, A. Shiraishi), Many-moto-Imai (T. Matsumoto, H. Imai).

Труднощі завдань підробки підпису в цих схемах полягають в обчислювальній складності завдань факторизації або дискретного логарифмування. Серед схем, запропонованих вітчизняними вченими, можна відзначити оригінальну схему Грушо А. А. (1992 р.). Її односпрямована функція, на відміну від перерахованих вище, заснована не на складності теоретико-числових завдань, а на складності рішення систем нелінійних бульових рівнянь.

Сьогодні практичні додатки найбільшого поширення одержали дві схеми: метод RSA і метод Ель-Гамаля.

У стандарті США для цифрового підпису DSS – Digital Signature Standard використовуються спеціально створені алгоритми. В основу цих алгоритмів покладені схеми Ель-Гамаля й Шнора [191].

У Росії прийняті стандарти: ДЕРЖСТАНДАРТ Р 34.10-94 "Процедури виробітку й перевірки електронного цифрового підпису на базі асиметричного криптографічного алгоритму" і ДЕРЖСТАНДАРТ Р 34.11-94 "Функція хешування". В основу ДЕРЖСТАНДАРТ Р 34.10-94 покладена односпрямована функція, заснована на дискретному зведенні в ступінь.

Конфіденційність і цілісність переданих каналами зв’язку даних забезпечуються застосуванням **засобів криптографічного захисту**, що використовують одноключові (той самий ключ, що є секретним, використовується й для шифрування й для дешифрування) алгоритми. Серед безлічі алгоритмів цього типу найбільшою довірою користуються криптографічні перетворення, що відповідають стандартам.

Найбільше поширення одержав уведений у дію в 1977 році національний стандарт США DES (Data Encryption Standard [191]), практично повсюдно використовуваний у банківській сфері. Вітчизняний стандарт криптографічного перетворення інформації, – ДЕРЖСТАНДАРТ 28147-89, був уведений у дію з липня 1990 року. Обидва ці стандарти використо-

вуються російськими комерційними банками для закриття повідомлень, переданих каналами зв'язку.

Цілісність фінансових повідомлень при передачі і їх захисту від різних маніпуляцій забезпечується перевіркою поля даних, що додається до повідомлення й змісті, що є функцією від повідомлення й секретного ключа. Спосіб формування цього поля також описується стандартами: обчислення коду перевірки дійсності даних (МАО в ISO 8730 і одержання імітовставки в ДЕРЖСТАНДАРТ 28147-89).

Використання криптографічних засобів вимагає створення **надійної ключової системи**, у якій операції генерації, зберігання, розсилання й знищення ключів задовольняли б вимоги безпеки. Для побудови ключової системи американськими банками в основному використовується стандарт на керування ключами фінансових повідомлень ANSI X9.17, що припускає існування в системі Центра розподілу ключів (ЦРК), що виконує всі операції з керування ключами.

У криптосистемі зі ЦРК існують три види ключів: головний ключ; ключі шифрування ключів; сеансові ключі.

Міжнародний стандарт ISO 8532 (Banking-Key-Management) також описує ієрархічну ключову систему із центром розподілу ключів. Ці стандарти вимагають передачі старшого ключа неелектронним способом (фельдзв'язком), що виключає його компрометацію. Ієрархічні схеми є досить дорогими й вимагають повної довіри до ЦРК, що генерує й розсилає ключі.

Метод з відкритим ключем дозволяє значно спростити ключову систему. При тому відпадає необхідність використання захищених каналів зв'язку. Однак виникає необхідність надійної автентифікації абонента, що прислали відкритий ключ. Роль адміністратора в системі зводиться до перевірки приналежності відкритих ключів, переміщення їх у довідник і розсилання цього довідника всім абонентам системи. Ці функції виконуються Центром верифікації ключів (ЦВК).

Основна операція, здійснювана ЦВК – сертифікація ключів. Суть її полягає у такому. Абонент, що бажає брати участь в обміні повідомленнями, посилає ЦВК свій відкритий ключ у роздрукованому вигляді, завіривши його мастичною печаткою своєї організації й підписами посадових осіб. Усі інші абоненти одержують цей ключ від ЦВК. Підставою для включення нового відкритого ключа в каталог є наявність електронного підпису ЦВК. Крім того, на ЦВК покладається завдання з повідомлення

всіх учасників обміну електронними документами у випадку компрометації ключів.

Найслабкішою ланкою в системі електронних документів з погляду безпеки є секретний ключ. Тому найбільшу увагу варто приділяти збереженню його в таємниці. Із цього погляду надзвичайно важливо правильно вибрати тип носія для збереження секретного ключа. Критеріями оцінки при виборі носія є:

наявність перезаписуваної пам'яті необхідного обсягу;

складність копіювання інформації;

зручність зберігання;

захищеність від зовнішніх впливів.

Зазначені вимоги найбільшою мірою задовольняють електронні картки. (Один з варіантів – електронні картки Touch Memory американської фірми Dallas Semiconductor, розміщені в металевому корпусі, що мають унікальний код і до 2 Кб перезаписуваної пам'яті).

Застосовувані організаційні заходи повинні:

передбачати періодичну зміну секретних ключів,

визначати порядок зберігання носіїв і схему повідомлення про події, пов'язані з компрометацією ключів.

Заява про компрометацію секретного ключа спричиняє виключення з каталогів усіх абонентів відповідних відкритих ключів і припинення обробки документів, підписаних за допомогою даного ключа.

Крім загроз, пов'язаних із порушенням цілісності, конфіденційності й дійсності повідомлень у системах електронних документів, існують загрози, **пов'язані із впливом на повідомлення**. До їх числа належать знищення, затримка, дублювання, переупорядкування, переорієнтація окремих повідомлень, маскування під іншого абонента або інший вузол. Загрози цього типу нейтралізуються використанням у системі **захищених протоколів зв'язку**.

Захист на рівні протоколів досягається вживанням таких заходів: керування з'єднанням; квотування; нумерація повідомлень; підтримка єдиного часу.

Керування з'єднанням необхідне при використанні ліній зв'язку, що комутуються, і містить у собі і запит **ідентифікатора**, автентифікацію джерела повідомлення й розрив з'єднання при одержанні неправильного ідентифікатора.

Існує кілька схем керування з'єднанням. Як правило, дається кілька спроб для уведення ідентифікатора, і якщо всі вони виявляються невдалими, зв'язок розривається.

Більш надійним способом керування з'єднанням є автоматичний зворотний виклик. При спробі встановити з'єднання прийомною стороною запитується ідентифікатор, після чого зв'язок розривається. Потім залежно від результатів перевірки або виробляється повторне з'єднання за обраним зі списку номером, або зв'язок припиняється. Надійність такого способу залежить від якості каналів зв'язку й правильності заповнення списку доступних номерів.

Квотування – це процедура видачі підтвердження (квитанції) про одержання повідомлення вузлом або адресатом, що дозволяє відслідковувати стан переданого документа. Додатковою гарантією може бути включення до складу квитанції електронного підпису. Для запобігання можливості відмови однієї зі сторін від факту одержання повідомлення протокол може передбачати повернення копій отриманих документів (за аналогією з паперовим документообігом) з електронним підписом одержувача.

Значне число навмисних атак і випадкових помилок можна виявити, якщо ввести **нумерацію повідомлень**. Одержання документа із уже використаним номером або номером, що значно перевищує поточний, є подією, що вказує на порушення правильності роботи системи й потребує негайної реакції з боку відповідального за безпеку.

Установлення й підтримка в системі електронних платежів **єдиного часу** для всіх абонентів значно знижує ймовірність загроз, пов'язаних з відмовою від авторства повідомлення, а також зменшує кількість помилок. При цьому переданий документ повинен містити незмінні дату й час підписання, що заносяться в нього автоматично.

Захист від НСД до терміналів, на яких ведеться підготовка й обробка повідомлень, повинна забезпечуватися застосуванням програмних і програмно-апаратних засобів і організаційною підтримкою. Засоби захисту повинні забезпечувати ідентифікацію й надійне впізнавання користувачів, розмежування повноважень за доступом до ресурсів, реєстрацію роботи й облік спроб НСД.

Організаційні заходи в системах електронних документів, як правило, спрямовані на чіткий розподіл відповідальності при роботі з документами й створення декількох меж контролю.

Перелік посадових осіб і їх обов'язків може виглядати таким чином:

бухгалтер підприємства – уведення документа, підпис, шифрування документа на ключі директора, складання балансу;

директор підприємства – верифікація документа, підпис, шифрування на ключі банку;

оператор клієнта-відправника й прийом зашифрованих повідомлень;

оператор банку – відправника й прийом зашифрованих документів;

операціоніст – розшифрування й перевірка одержуваних документів, підготовка виписок, підпис, шифрування на ключі клієнта;

менеджер – верифікація документів і відбиття їх в операційному дні банку, підпис;

адміністратор – керування ключами, зв'язок із ЦБК, обробка облікових і реєстраційних журналів, підтримка системи захисту.

Обов'язковою умовою існування системи електронних платежів є **підтримка архівів електронних документів**. Строк зберігання архівного документа може становити кілька років. Тому необхідно вживати заходів для захисту архівів від руйнування. Досить ефективним способом захисту є завадостійке кодування.

Таким чином, можна кожному виду загроз поставити у відповідність певні заходи захисту (табл. 11.2).

Додатково необхідно враховувати практичні рекомендації з таких позицій.

Персоніфікація документів

Недостатньо просто застосувати підпис. Необхідно домагатися того, щоб під документом стояло мінімум два ЕЦП, що належать конкретним людям з конкретною відповідальністю.

Контроль за виведенням документів на друк

Не слід забувати, що електронний документообіг не скасовує звичні паперові документи. Частіше відбувається навпаки – кількість паперів зростає. І часто виникає парадоксальна ситуація: поки документ існує в електронному вигляді, його захищають всіма можливими способами. Потім його виводять на принтері незліченну кількість разів і зрештою розкидають по сміттєвих кошиках через непотрібність.

Працівники режимно-секретних служб знають, що із введенням комп'ютерної техніки на робочі місця контролювати процес підготовки документів обмеженого поширення став набагато складнішим. Звичайні

засоби захисту від несанкціонованого доступу, безумовно, полегшують життя, але не дають можливості автоматизувати процес обліку документів і контроль за їх підготовкою. Що ж необхідно зробити для забезпечення безпечного процесу виведенням документів на друк?

Таблиця 11.2

Відповідність загрозам заходів захисту

Нейтралізовані загрози	Заходи захисту
Підробка документа. Відмова від авторства. Несанкціонована модифікація	Застосування електронного цифрового підпису. Ведення електронних архівів
Порушення конфіденційності	Криптографічне закриття
Помилки при заповненні документів	Контроль правильності уведення документів Проходження документів за суворим певним маршрутом
Уведення помилкових даних	Контроль маршруту проходження документа. Персоніфікація документів
Помилки в роботі системи	Реєстрація й облік документів на етапах підготовки
Дублювання документів	Нумерація документів. Контроль часу відправлення документа. Забезпечення одиничності виконання документа
Спроби одержання секретного ключа	Керування ключовою системою
Несанкціонована модифікація ПЗ	Верифікація ПЗ
Руйнування даних	Резервне копіювання
Несанкціонований доступ до конфіденційної інформації	Фізичний захист приміщень. Розмежування прав учасників електронного документообігу. Застосування засобів захисту інформації від НСД
Крадіжки й втрати документів	Контроль за виведенням документів на друк

Забезпечення конфіденційності документів

У документах Держтехкомісії Росії на це питання є вичерпна відповідь:

"...повинен бути передбачений адміністратор (служба) захисту інформації, відповідальний за ведення, нормальне функціонування й контроль роботи ЗЗІ від НСД. Адміністратор повинен мати свій термінал і необхідні засоби оперативного контролю й впливу на безпеку АС";

"...повинна здійснюватися реєстрація видачі друкованих (графічних) документів на "тверду" копію. Видача повинна супроводжуватися автоматичним маркуванням кожного аркуша (сторінки) документа порядковим номером і обліковими реквізитами АС із зазначенням на останньому аркуші документа загальної кількості аркушів (сторінок). У параметрах реєстрації вказуються:

дата й час видачі (звертання до підсистеми виводу);

специфікація пристрою видачі (логічне ім'я (номер) зовнішнього пристрою);

короткий зміст (найменування, вид, шифр, код) і рівень конфіденційності документа;

ідентифікатор суб'єкта доступу, що запросив документ;

обсяг фактично виданого документа (кількість сторінок, аркушів, копій) і результат видачі: успішний (весь обсяг), неуспішний.

11.3. Нормативні положення, що регламентують інформаційну безпеку

Окремі положення Кодексу про адміністративні правопорушення [84]

Стаття 164-9. Незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних. Розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних, упаковки яких не марковані контрольними марками або марковані контрольними марками, що мають серію чи містять інформацію, які не відповідають носію цього примірника, або номер, який не відповідає даним Єдиного реєстру одержувачів контрольних марок, тягне за собою накладення штрафу від десяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією цих примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, БД.

Та сама дія, вчинена особою, яка протягом року була піддано адміністративному стягненню за одне з правопорушень, зазначених у частині першій цієї статті, тягне за собою накладення штрафу від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян з конфіскацією цих примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, БД.

Стаття 195-5. Незаконне придбання або зберігання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації.

Незаконне придбання або зберігання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації – тягне за собою накладення штрафу на громадян від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації та на посадових осіб – від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян з конфіскацією спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації.

Стаття 212-6. Здійснення незаконного доступу до інформації в автоматизованих системах. Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в автоматизованих системах, тягне за собою накладення штрафу від п'яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу або без такого.

Та сама дія, вчинена особою, яка протягом року було піддана адміністративному стягненню за порушення, передбачене в частині першій цієї статті, тягне за собою накладення штрафу від десяти до двадцяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу.

Окремі положення Кримінального кодексу [88]

Стаття 176. Порушення авторського права і суміжних прав.

1. Незаконне відтворення, розповсюдження творів науки, літератури і мистецтва, **комп'ютерних програм і баз даних**, а так само незаконне відтворення, розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, або інше умисне порушення авторського права і суміжних прав, якщо це завдало матеріальної шкоди у великому розмірі, караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк із конфіскацією всіх примірників творів, матеріальних носіїв комп'ютерних програм, БД, виконань, фонограм, відеограм, програм мо-

влення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

2. Ті самі дії, якщо вони вчинені повторно, або за попередньою змовою групою осіб, або завдали матеріальної шкоди в особливо великому розмірі, караються штрафом від тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк від двох до п'яти років, з конфіскацією всіх примірників творів, матеріальних носіїв комп'ютерних програм, БД, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

3. Дії, передбачені частинами першою або другою цієї статті, вчинені службовою особою з використанням службового становища щодо підлеглої особи, караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до двох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Примітка. У статтях 176 та 177 цього Кодексу матеріальна шкода вважається завданою у великому розмірі, якщо її розмір у двісті та більше разів перевищує неоподатковуваний мінімум доходів громадян, а завданою в особливо великому розмірі, якщо її розмір у тисячу й більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 359. Незаконне використання спеціальних технічних засобів негласного отримання інформації.

1. Незаконне використання спеціальних технічних засобів негласного отримання інформації – карається штрафом від ста до двохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк.

2. Ті самі дії, якщо вони вчинені повторно, за попередньою змовою групою осіб або організованою групою, або заподіяли істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб, – караються позбавленням волі на строк від трьох до семи років.

Стаття 360. Умисне пошкодження ліній зв'язку. Умисне пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, дротового мовлення або споруд чи обладнання, які входять до їх складу, якщо воно спричинило тимчасове припинення зв'язку, – карається штрафом від ста до двохсот

неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до одного року, або обмеженням волі на строк до двох років.

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років, або без такого та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено несанкціоноване втручання і які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено несанкціоноване втручання і які є власністю винної особи.

Примітка. Значною шкодою у статтях 361 – 363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-

обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, караються штрафом від п'ятисот до тисячі неоподаткованих мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут чи розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Стаття 362. Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

1. Несанкціоновані зміна, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах),

автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміни, знищення або блокування інформації, що є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється.

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років із позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електро-зв'язку, карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, що є власністю винної особи.

Юридична практика, як завжди, відстає від досягнень техніки. На думку авторів, загальне подання про можливі правові наслідки використання вірусів, а також про правові наслідки публікації програм-вірусів дає користувачам-програмістам фундаментальна робота *"Комп'ютерні віруси й право"*. Ця робота, відома дотепер лише вузькому колу фахівців, була написана кандидатом юридичних наук з Гамбургу Стефаном Акерманом, що цікавиться всіма правовими питаннями, яка належить до апаратного, ПЗ й телекомунікації. Первісна версія цієї роботи була вперше опублікована в гамбурзькій поштовій скриньці CLINCH (а потім і в деяких інших некомерційних поштових скриньках); тут вона вперше представляється широкій читацькій аудиторії в стислому й переробленому вигляді.

Завдяки зростаючій руйнівній силі комп'ютерних вірусів (КВ) вони стали улюбленою темою загальної й спеціальної преси, радіо й телебачення. У повідомленнях йдеться в основному про чисто технічні питання, наприклад, що таке вірус, як він програмується й застосовується й, зрозуміло, як можна захиститися від КВ.

Але при цьому майже зовсім ігноруються або розглядаються не компетентно не менш актуальні правові аспекти програмування й застосування КВ.

Матеріал призначений не тільки для юристів. У досить доступній і зв'язаній формі тут пояснено, які правові наслідки можуть мати розробка, публікація й поширення програм-вірусів. Зрозуміло, що обговорюються правові можливості відшкодування винуватцем потерпілому збитку, заподіяного дією програм-вірусів. При цьому не зупиняються на надзвичайно складному питанні доказу провини.

КВ, як і вся комп'ютерна технологія, досить нова проблема. А правова наука реагує на технічні нововведення з більшим запізненням. Наприклад, тема КВ практично не порушена в сучасній літературі і юридичній практиці. Тому висловлені тут ідеї не опираються не сформовані подання в літературних джерелах, і до них варто ставитися з розумною обережністю, а не розглядати як непорушний закон природи. Проте Акерман Г. С. схильний думати, що доти, доки юридична практика не буде забезпечувати надійну правову захищеність і чітке формулювання правових норм, ці ідеї можуть бути необхідним орієнтиром.

Кримінально-правові наслідки

Спочатку розглянемо норми карного права, що стосуються, в першу чергу, використання КВ. Потім торкнемося питань виконавства й співучасті.

1. Існуючі норми карного права. КВ найчастіше руйнують програми, що зберігаються в пам'яті, або масиви даних або змінюють ці дані без їх руйнування.

2. Виконання й співучасть. Порівняно зі злочином, зробленим однією особою за чинними нормами, набагато складніше; класифікуються випадки посереднього виконання, співвиконання, підбурювання й пособництва. Йдеться про те, що злочинець необов'язково сам впроваджує вірус, а сприяє іншому в здійсненні такого діяння. І тут наступає карне покарання, оскільки співучасть у різних формах повинна класифікуватися з урахуванням ступеня участі, передбаченого спеціальною частиною КК.

Тут лише дається спроба коротко описати ситуації, коли наступає караність за співучасть, посереднє виконання, підбурювання й пособництво.

3. Співвиконання. При впровадженні вірусу групою осіб однаковому покаранню піддається кожен із членів групи. Співвиконання має місце тоді, коли учасники ухвалили рішення щодо здійсненні діяння спільно, рівноправно, з поділом функцій, і відповідно до цього рішення зробили спільну дію, спрямовану на здійснення злочину. Співвиконання має місце

також у тому випадку, якщо розподіл функцій характеризується тим, що один учасник програмує вірус, а інший його впроваджує. Отже, злочинцем є не тільки той, хто безпосередньо впровадив вірус у чужу систему.

4. Посереднє виконання. Злочинним уважається й діяння, коли злочинець діяв не сам, а спонукав діяти у своїх інтересах іншу особу, а сам як посередній виконавець залишився в тіні. Посереднє виконання має місце, якщо (посередній) виконавець використовується приблизно як інструмент (хоча інструмент проти самого себе). Використання як інструмент має місце найчастіше тоді, коли посередній виконавець знає набагато більше, ніж використовуваний ним "інструмент". Наприклад, злочинець знає, що дискета, яка лежить поруч із ПК, містить вірус. Власник комп'ютера цього не знає. Якщо посередній виконавець запропонує власникові завантажити дискету із цікавою ігровою програмою, і власник, нічого не підозрюючи, зробить це, то він як би сам впровадить шкідливий вірус. Проте діяння приписується посередньому виконавцеві, тому що в цьому випадку власник комп'ютера через перевагу злочинця в знаннях був використаний лише як інструмент проти самого себе.

5. Підбурювання. Покарання за підбурювання наступає тоді, коли деяка модель поводження передбачається злочинцем, що мотивує небезпеку, щоб передбачувані виконавці прийняли відповідне рішення, а потім і реалізували його. Якщо злочинець дійсно приймає відповідне злочинне рішення й реалізує його в протиправному діянні, то підбурювач повинен зазнавати кари.

Караність за підбурювання до зміни даних і інші злочини, пов'язані із КВ, приховує у собі деякою мірою "підривну силу" у зв'язку з усе більшим поширенням програм-вірусів і радою про те, як використовувати КВ.

6. Пособництво. За своїм характером пособництво дуже близьке до підбурювання. Для складу злочину необхідне сприяння, запропоноване злочинцеві, прийняте ним і використане потім при здійсненні основного злочину. Злочинець не обов'язково повинен знати про те, що йому надана допомога. Запропоноване й прийняте сприяння, але не реалізоване потім в основному злочині, не розглядається як пособництво.

У деяких випадках пособництво важко відрізнити від співвиконання, причому особливості цих різновидів злочини є предметом запеклих суперечок. У досить спрощеному вигляді співвиконання має місце, якщо

діюча особа здійснює діяння зі своєї волі, а пособництво – якщо із чужої волі. Відповідно до іншого трактування, яке поділяє автор посібника, варто виходити з того, хто здійснював панування над діянням.

Цивільно-правові наслідки

Спочатку розглянемо найбільш важливі норми громадянської відповідальності, а потім торкнемося питання про відповідальність учасників за відповідне діяння.

1. Норми відповідальності. У першу чергу розглядається відповідальність за відшкодування збитку.

2. Відповідно до закону збиток повинен бути відшкодований, якщо через недбайливість або навмисно було порушене право власності або інше право потерпілого.

Порушення права власності, безсумнівно, має місце, якщо КВ призвів до ушкодження апаратних засобів. Але на питання, чи можна кваліфікувати перекручування даних або програм як порушення права власності або якого-небудь іншого права, відповісти досить важко. Порушення права власності виключається, тому що дані й програми не є майном. Отже, закон застосуємо тільки щодо порушення "інших прав". Сумнівно, що "володіння" або "право власності" на програми й дані захищаються в які "інші права". Тут питання можна залишити відкритим, тому що воно розв’язується тільки в окремих конкретних ситуаціях.

3. Відповідно до закону повинен бути відшкодований збиток, заподіяний у результаті порушення того закону, що повинен (щонайменше) захищати потерпілого. Такими охоронними законами є вже написані вище норми карного права. Це значить, що порушення цих норм спричиняє відшкодування збитку на користь потерпілого.

4. І, нарешті, діє параграф, що особа, яка порушила загальноприйняті моральні норми й тим самим навмисно заподіяла збиток іншій особі, повинна відшкодувати збиток. Це положення може, як правило, застосовуватися для тих випадків, коли навмисне впровадження вірусу завдало шкоди, яка має бути відшкодована.

5. Договірні претензії. Поряд із уже розглянутими делікатними претензіями, як виняток, розглядаються й договірні претензії. Але й у цих випадках найчастіше має місце делікатна відповідальність, строки дії якої за певних обставин більш сприятливі для потерпілого (а саме, якщо відпові-

дальність за поставку продукції з порушенням договірних умов). Ці делікатні претензії втрачають силу за давниною через три роки після встановлення збитку і його винуватця (саме пізніше через 30 років).

6. Відповідальність при декількох виконавцях. Згідно з законом під час здійсненні злочинного діяння декількома виконавцями всі учасники відповідають за заподіяний збиток, як солідарні боржники. Форма участі не розрізняється. Це означає, що кожен, хто вніс який-небудь причинний внесок у виникнення збитку й хто несе відповідальність, може бути визнаний єдиним відповідачем із відшкодування всього збитку, навіть якщо він діяв не поодинці або виступав як пособник або співучасник. Потерпілий може вибирати, зажадати або відшкодування збитку від всіх учасників з урахуванням частки збитку, заподіяного дією конкретної особи, або зажадати повної компенсації лише з одного учасника (найбільш платоспроможного або того, кого він хотів би покарати особисто). Правда, усередині є вимоги компенсації, згідно з яким кожному висуваються претензії лише відповідно до його часток заподіяного збитку. А якщо позов на повне відшкодування збитку висувається лише одному зі співучасників, виникає небезпека, що вимогу відшкодування збитку іншим особам, які заподіяли збиток, не вдається задовольнити.

Це досить ризиковано, оскільки суми збитку для КВ, що надзвичайно швидко поширюються й паралізують на тривалий строк велику кількість ЕОМ, можуть досягати сотень і навіть мільйонів.

7. Міра відповідальності. Існує принцип: повинен бути відновлений стан, що існував до заподіяння збитку, або бути зроблене капіталовкладення, необхідне для відновлення цього стану. Мають бути компенсовані всі адекватно-каузальні наслідки збитку, а також недоотриманий прибуток.

Використана література

1. Авдийский В. И. Основы экономико-правового анализа бизнес-процессов (риск-менеджмент): Альбом схем. Предназначен для студентов Института экономической безопасности, обучающихся по специальности 060400 "Финансы и кредит" / Авдийский В. И. – М. : Финансовая академия при Правительстве РФ, 2004. – 50 с.

2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России. – М. : ГТК РФ, 1992. – 39 с.

3. Агеев А. С. Компьютерные вирусы и безопасность информации / Агеев А. С. // Зарубежная радиоэлектроника. – 1989. – № 12. – С. 71–73.

4. Александров М. Н. Национальная и региональная экономическая безопасность : учебн.-метод. комплекс. Для студентов обучающихся в Институте экономической безопасности по специальности 08010565 "Финансы и кредит " (специализация "Экономическая и информационная безопасность в финансо-банковской сфере") / Александров М. Н. – М. : Финансовая академия при Правителстьве РФ, 2005. – 36 с.

5. Андрианов В. И. Охранные системы для дома и офиса / Андрианов В. И., Соколов А. В. – СПб. : БХВ-Петербург ; Арлит, 2002. – 304 с.

6. Андрианов В. И. Устройства для защиты объектов и информации ("Шпионские штучки") / В. И. Андрианов, А. В. Соколов. – М. : ООО "Фирма "Издательство АСТ" ; ООО "Издательство "Полигон", 2000. – 256 с.

7. Анин Б. Ю. Защита компьютерной информации / Анин Б. Ю. – СПб. : BHV-Санкт-Петербург, 2000. – 384 с.

8. Аньшин В. М. Менеджмент инвестиций и инноваций в малом и венчурном бизнесе : учебн. пособ. / В. М. Аньшин, С. А. Филин. – М. : Анкил, 2003. – 91 с.

9. Архипова Н. И. Исследование систем управления / Архипова Н. И., Кульба В. В., Косяченко С. А. – М. : Изд-во "ПРИОР", 2002. – 230 с.

10. Бакаєв О. О. Мікроекономічне моделювання і інформаційні технології / Бакаєв О. О., Гриценко В. І., Бажан Л. І. – К. : Наукова думка, 2003. – 184 с.

11. Балдин К. В. Информационные системы в экономике : учебник / Балдин К. В. – 3-е изд. – М. : Издательскоторговая корпорация "Дашков и К°", 2006. – 395 с.

12. Банковское дело : справ. пособ. / М. Ю. Бабичев, Ю. А. Бабичева, О. В. Трохова и др. ; под ред. Ю. А. Бабичевой. – М. : Экономика, 1993. – 397 с.

13. Баскакова О. В. Экономика организаций (предприятий) : учебн. пособ. / О. В. Баскакова. – М. : Дашков и К^0, 2004. – 269 с.

14. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юрид. Лит., 1991. – 160 с.

15. Безопасность информационных технологий. – Вып. 1. – М. : Госкомитет РФ по высшему образованию, МИФИ, 1994. – 100 с.

16. Белов П. Г. Теоретические основы системной инженерии безопасности / Белов П. Г. – М. : ГНТП "Безопасность", 1996. – 424 с.

17. Белоусов В. Л. Менеджмент : экономическая безопасность : учебн. пособ. / Белоусов В. Л., Гончаренко Л. П., Елисеев В. А. – М. : ФГУ НИИ РИНКЦЕ, 2005. – 174 с.

18. Бияшев О. Г. Основные направления развития и совершенствования криптографического закрытия информации / Бияшев О. Г., Диев С. И., Зазмахнин М. К. / Зарубежная радиоэлектроника. – 1989. – № 12. – С. 16–18.

19. Боденхаузен Г. Парижская конвенция по охране промышленной собственности [Текст] : комментарий / Г. Боденхаузен ; пер. с фр. Н. Л. Тумановой ; под ред. Е. П. Богуславского. – М. : Прогресс, 1977. – 310 с.

20. 18-е Международные плехановские чтения: Тезисы докладов докторантов, аспирантов и научных сотрудников (5 – 7 апреля 2005 г.). – М. : Рос. экон. акад., 2005. – 124 с.

21. Вакуленко Р. Я. Защита бизнеса и стратегия предприятия. Экономический и правовой аспект / Р. Я. Вакуленко, Е. В. Новоселов. – М. : Юркнига, 2005. – 160 с.

22. Варфоломеев А. А. Методы криптографии и их применение в банковских технологіях / А. А. Варфоломеев, М. Б. Пеленицын. – М. : Изд. "Банковское дело", 1995. – 224 с.

23. Веретенникова Г. Б. Економічна безпека підприємства: планування й організація : конспект лекцій / Веретенникова Г. Б. – Х. : Вид. ХНЕУ, 2008. – 84 с.

24. Волчинская Е. К. Есть ли в России компьютерное право / Волчинская Е. К. // Юридический консультант. – 1997. – № 2. – С. 9–19.

25. Воробьев Ю. Л. Катастрофы и человек: Кн. 1. Российский опыт противодействия чрезвычайным ситуациям / Ю. Л. Воробьев,

Л. И. Локтионов, М. И. Фалалеев ; под ред. Ю. Л. Воробьева. – М. : АСТ-ЛТД, 1997. – 319 с.

26. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. Руководящий документ Гостехкомиссии России. – М. : ГТК РФ, 1992. – 29 с.

27. Гайкович В. Безопасность электронных банковских систем / Гайкович В. – М. : Единая Европа, 1994. – 324 с.

28. Гайкович В. Ю. Безопасность электронных банковских систем / В. Ю. Гайкович, А. Ю. Першин. – М. : Единая Европа, 1994. – 363 с.

29. Гаффин Адам. Путеводитель по глобальной компъютерной сети / Гаффин Адам. – М. : ТПП "Сфера", 1995. – 282 с.

30. Гвардейцев М. И. Математическое обеспечение управления. Мера развития общества / М. И. Гвардейцев, П. Г. Кузнецов, В. А. Розенберг. – М. : Радио и связь, 1996. – 176 с.

31. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М. : МОПО РФ – МГИФИ, 1997. – 538 с.

32. Герасименко В. А. Защита информации в автоматизированных системах обработки данных / Герасименко В. А., в 2-х кн. – М. : Энергоатомиздат, 1994. – 400 с.

33. Герасимов П. А. Основы экономической безопасности : учебн.-метод. комплекс. для студ., обучающихся по спец. 08050365 "Антикризисное управление", 08011665 "Математические методы в экономике" / Герасимов П. А. – М. : Фин. акад. при Правительстве РФ, 2005. – 58 с.

34. Герасимов П. А. Экономическая безопасность хозяйствующего субъекта : уч.-метод. комплекс (для студ, обучающихся в Институте экономической безопасности по специальности 08010565 "Финансы и кредит") / Герасимов П. А. – М. : Фин. акад. при Правительстве РФ, 2005. – 73 с.

35. Годин В. В. Управление информационными ресурсами: 17-модульная программа для менеджеров "Управление развитием организации". Модуль 17 / В. В. Годин, И. К. Корнеев. – М. : ИНФРА-М, 2000. – 352 с.

36. Голубев В. В. Компьютерные преступления и защита информации в вычислительных системах / В. В. Голубев, П. А. Дубров, Г. А. Павлов // Вычислительная техника и ее применение – 1990. – № 9. – С. 3–26.

37. Городничев П. Н. Финансовое и инвестиционное прогнозирование : учебн. пособ. / П. Н. Городничев, К. П. Городничева. – М. : Экзамен, 2005. – 224 с.

38. Гражданский кодекс. Ч. 1. – М. : ИНФРА-М ; Норма, 2000. – 1014 с.

39. Гусаров Ю. В. Управление: динамика неравновесности / Гусаров Ю. В. – М. : ЗАО "Издательство "Экономика", 2003. – 382 с.

40. Давыдовский А. И. Введение в защиту информации / А. И. Давыдовский, В. А. Максимов // Интеркомпьютер. – 1990. – № 1. – С. 17–20.

41. Дейтел Г. Введение в операционные системы / Дейтел Г. ; в 2-х т. Т.2. пер. с англ. – М. : Мир, 1987. – 398 с.

42. Демик Н. К. Комплексная защита коммерческой и конфиденциальной информации : метод. пособ. / Демик Н. К. – М. : Рос. экон. акад.,1999. – 95 с.

43. Демик Н. К. Обеспечение безопасности информационных и телекоммуникационных систем : метод. пособ. / Демик Н. К. – М. : Рос. экон. акад., 2003. – 42 с.

44. Дружинин Г. В. Качество информации / Г. В. Дружинин, И. В. Сергеева. – М. : Радио и связь, 1990. – 172 с.

45. Дэвид Стенг. Секреты безопасности сетей / Дэвид Стенг, Сильвия Муи. – К. : "Диалектика", Информейшн Компьютер Энтерпрайз, 1996. – 544 с.

46. Дюбуа Д. Теория возможностей. Приложения к представлению знаний в информатике / Д. Дюбуа, А. Прад. – М. : Радио и связь, 1990. – 288 с.

47. Економічна безпека підприємств, організацій та установ : навч. посібн. / Ортинський В. Л., Керницький І. С., Живко З. Б., та ін. – К. : Всеукраїнська асоціація видавців "Правова єдність", 2009. – 546 с.

48. Жельников В. Криптография от папируса до компьютера / Жельников В. – М. : ABF, 1997. – 336 с.

49. Защита информации в компьютерных системах / под ред. Шмакова Э. М. – СПб. : СПбГТУ, 1993. – 100 с.

50. Защита информации в персональных ЭВМ / А. В. Спесивцев, В. А. Вегнер, А. Ю. Крутяков и др. – М. : Радио и связь, МП "Веста", 1992. – 192 с.

51. Защита прав создателей и пользователей программ для ЭВМ и баз данних. – М. : Ось, 1996. – 186 с.

52. Зимин Н. Е. Анализ и диагностика финансово-хозяйственной деятельности предприятия : учебник для вузов / Н. Е. Зимин, В. Н. Солопова. – М. : КолосС, 2004. – 383 с.

53. Зиннуров У. Г. Методология обеспечения экономической безопасности предприятия на основе стратегического маркетингового планирования и управления / У. Г. Зиннуров, В. С. Исмагилова. – М. : Изд. МАИ, 2004. – 375 с.

54. Кавун С. В. Анализ категорийного аппарата в сфере экономической и информационной безопасности / С. В. Кавун, И. В. Михальчук // Економіка розвитку: науковий журнал. – Х. : Вид. ХНЕУ, 2009. – № 3(51). – С. 9–14.

55. Кавун С. В. Анализ показателей экономической безопасности макроуровня (на примере западных стран) / С. В. Кавун, И. В. Михальчук // Вісник економіки транспорту і промисловості : зб. наук.-практ. статей. – Х. : УкрДАЗТ, 2010. – Вип. 29. – С. 61–65.

56. Кавун С. В. Анализ экономической безопасности предприятий (г. Харькова и Харьковской области) / С. В. Кавун // Економіка розвитку : науковий журнал. – Х. : Вид. ХНЕУ, 2009. – № 1(49). – С. 72–75.

57. Кавун С. В. Анализ экономической безопасности предприятия / С. В. Кавун // Право і безпека : наук. журнал. – Х. : Вид. ХНУВС, 2006. – Т. 5. – № 5. – С. 45–49.

58. Кавун С. В. Вопросы методики разработки системы экономической безопасности предприятия / С. В. Кавун // МСУ. – Вестник международного славянского университета. Сер. Економічні науки : укр. наук.-теор. журнал. – Х. : МСУ, 2008. – Т. XI. – № 1. – С. 34–39.

59. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия / С. В. Кавун // Управління розвитком : наук. журнал. – Х. : Вид. ХНЕУ, 2008. – № 6. – С. 17–21.

60. Кавун С. В. Инсайдер – угроза экономической безопасности / С. В. Кавун, И. В. Сорбат // Управління розвитком : наук. журнал. – Х. : Вид. ХНЕУ, 2008. – № 6. – С. 7–11.

61. Кавун С. В. Инсайдерство – проблема экономической безопасности в условиях реформирования экономики Украины / С. В. Кавун, И. В. Сорбат // Актуальні проблеми економіки : наук. журнал. – К. : Національна академія управління, 2009. – № 4(94). – С. 91–97.

62. Кавун С. В. Информационная безопасность в бизнесе : научное издание / С. В. Кавун. – Х. : Вид. ХНЭУ, 2007. – 408 с.

63. Кавун С. В. Інформаційна безпека : навч. посібн. Ч. 1. / С. В. Кавун, В. В. Носов, О. В. Манжай. – Х. : Вид. ХНЕУ, 2008. – 352 с.

64. Кавун С. В. Інформаційна безпека : навч. посібн. Ч. 2. / С. В. Кавун, В. В. Носов, О. В. Манжай. – Х. : Вид. ХНЕУ, 2008. – 196 с.

65. Кавун С. В. Інформаційна безпека : підручник / С. В. Кавун. – Х. : Вид. ХНЕУ, 2009. – 368 с.

66. Кавун С. В. Концептуальная модель системы экономической безопасности предприятия / С. В. Кавун // Економіка розвитку : науковий журнал. – Х. : Вид. ХНЕУ, 2007. – № 3(43). – С. 97–101.

67. Кавун С. В. Лабораторний практикум з навчальної дисципліни інформаційна безпека : навч.-практ. посібн. / С. В. Кавун, В. В. Носов, В. В. Огурцов, О. В. Манжай. – Х. : Вид. ХНЕУ, 2008. – 256 с.

68. Кавун С. В. Математическая интерпретация задачи выявления инсайдеров в организации (предприятии) / С. В. Кавун, И. В. Сорбат // Економіка: проблеми теорії та практики : зб. наук. праць. – Дніпропетровськ : ДНУ, 2008. – Вип. 246 : В 5 т. – Т. IV. – С. 862–869.

69. Кавун С. В. Матричная модель системы экономической безопасности предприятия / С. В. Кавун // Бизнес-информ. – 2007. – № 10(2). – С. 45 – 49.

70. Кавун С. В. Методи оцінки ефективності системи економічної безпеки підприємницької діяльності / С. В. Кавун // Вісник Львівського університету ім. І. Франка. Сер. Економічна : наук.-теор. журнал. – Львів : ЛНУ ім. І. Франка, 2008. – Вип. 40. – С. 278–281.

71. Кавун С. В. Методика оцінки одноразових витрат поетапної реалізації системи економічної безпеки / С. В. Кавун, О. Г. Зима // ХНАМГ. – Коммунальное хозяйство городов. Сер. Экономические науки : зб. наук. праць. – К. : Техніка, 2009. – Вип. 89. – С. 440–449.

72. Кавун С. В. Методика построения политики безопасности организации / С. В. Кавун, Г. В. Шубіна // Бизнес-информ. – 2005. – № 1 – 2. – С. 96–102.

73. Кавун С. В. Моделі оцінювання вартості інформації з обмеженим доступом / С. В. Кавун, О. Г. Зима, І. О. Ревак // НЛТУ України. – Науковий вісник Національного лісотехнічного університету України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України, 2009. – Вип. 19.9. – С. 255–260.

74. Кавун С. В. Организация противодействия инсайдерам в предпринимательской деятельности / С. В. Кавун // Економіка розвитку : науковий журнал. – Х. : Вид. ХНЕУ, 2008. – № 1(45). – С. 9–11.

75. Кавун С. В. Оценка эффективности системы экономической безопасности / С. В. Кавун // Економіка розвитку: науковий журнал. – Х. : Вид. ХНЕУ, 2009. – № 4(52). – С. 5–8.

76. Кавун С. В. Оцінка збитку організації внаслідок мережних атак на її ресурси / С. В. Кавун // Економіка розвитку: науковий журнал. – Х. : Вид. ХНЕУ, 2007. – № 1(41). – С. 83–85.

77. Кавун С. В. Робоча програма навчальної дисципліни "Інформаційна безпека" для студентів напряму підготовки "Комп'ютерні науки" всіх форм навчання / С. В. Кавун. – Х. : Вид. ХНЭУ, 2008. – 44 с.

78. Кавун С. В. Аналіз стану інформаційної безпеки в системах дистанційного навчання / С. В. Кавун, О. А. Сахно // Фінансово-кредитна діяльність : проблеми теорії та практики: зб. наук. праць. – Х. : ХІБС УБС НБУ, 2010. – № 1(8). – Частина ІІ. – С. 222–234.

79. Кавун С. В. Классификатор видов информации и форм документов / С. В. Кавун // ПУСКУ. – Науковий вісник Полтавського університету споживчої кооперації України. Сер. Економічні науки : наук. журнал. – Полтава : РВВ ПУСКУ, 2009. – № 5(36). – С. 69–75.

80. Кландер Л. Hacker Proof : Полное руководство для безопасности компьютера / Кландер Л. ; пер. с англ. – Мн. : Попурри, 2002. – 688 с.

81. Класифікація видів економічної діяльності (NACE, Rev.1.1 – 2002) / В. Анісімов (розроб.). – Офіц. вид. – К. : Держспоживстандарт України, 2006. – 192 с.

82. Кузнецов В. Классификатор профессий ДК 003:2005 / В. Кузнецов (сост.). – Х. : Изд. дом "Фактор", 2006. – 440 с.

83. Кляйн Д. Как защититься от "взломщика". Обзор методов парольной защиты и набор рекомендаций по ее улучшению / Кляйн Д. // Программирование. – 1991. – № 3. – С. 59–63.

84. Кодекс про адміністративні правопорушення // Відомості Верховної Ради Української РСР (ВВР). – 1984. – Додаток до № 51. – Ст. 1122.

85. Козаченко Г. В. Економічна безпека підприємства: сутність та механізм забезпечення : монографія / Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. – К. : Лібра, 2003. – 280 с.

86. Конституція України від 28 червня 1996 р. № 254к/96-вр // Відомості Верховної Ради України. – 1996. – № 30.

87. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. – М. : ГТК РФ, 1992. – 9 с.

88. Кримінальний кодекс України // Відомості Верховної Ради (ВВР). – 2001. – № 25 – 26. – С. 131.

89. Куркин Н. В. Управление экономической безопасностью развития предприятия : монография / Куркин Н. В. – Днепропетровск : АРТ-ПРЕСС, 2004. – 284 с.

90. Лафта Дж. К. Управленческие решения : учебн. пособ. – М. : ООО Фирма "Благовест-В", 2004. – 304 с.

91. Леонтьев Б. Хакеры и Интернет / Леонтьев Б. – М. : ЦФТИ, 1998. – 338 с.

92. Малый бизнес. Организация, экономика, управление : учебн. пособ. / под ред. проф. В. Я. Горфинкеля, проф. В. А. Швандара. – 2-е изд., перераб. и доп. – М. : ЮНИТИ-ДАНА, 2003. – 430 с.

93. Малюк В. И. Проектирование структур производственных предприятий / Малюк В. И. – СПб. : Издательский дом "Бизнес-пресса", 2005. – 320 с.

94. Мельников В. В. Защита информации в компьютерных системах / Мельников В. В. – М. : Финансы и статистика; Электроинформ, 1997. – 368 с.

95. Могилевский В. Д. Безопасность динамики экономических систем : оценка и управление. Труды аспирантов кафедры "Инвестиционная политика": Вып. 3 / В. Д. Могилевский, Б. И. Усачев. – М. : Рос. экон. акад., 1999. – 50 с.

96. Моисеенков И. Э. Американская классификация и принципы оценивания безопасности компьютерных систем / Моисеенков И. Э. // Компьютер-пресс. – 1992. – № 2 – 3. – С. 47–54.

97. Моисеенков И. Э. Основы безопасности компьютерных систем / Моисеенков И. Э. // Компьютерпресс. – 1991. – № 10. – С. 19–24. – № 11. – С. 7–21.

98. Мухин В. И. Исследование систем управления / Мухин В. И. – М. : Экзамен, 2002. – 150 с.

99. Одинцов А. Л. К вопросу об управлении инвестиционными рисками. Инвестиции и экономическая безопасность : Доклады на научной конференции 8 февраля 2000 года / А. Л. Одинцов, С. А. Суровегин / под ред. Е. А. Олейникова и И. Г. Шилина. – М. : РЭА им. Г. В. Плеханова, 2000. – С. 77–81.

100. Олейников Е. А. Экономическая и национальная безопасность : учебник для вузов / Олейников Е. А. ; Рос. экон. акад. им. Г. В. Плеханова. – М. : Экзамен, 2005. – 766 с.

101. Паштова Л. Г. Формирование многоуровневой инвестиционной политики как фактор обеспечения экономической безопасности : диссертация д.э.н. спец. 08.00.05 / Паштова Л. Г. – Москва : 2001. – 46 с.

102. Петраков А. В. Основы практической защиты информации : учебн. пособ. / Петраков А. В. – 2-е изд. – М. : Радио и связь, 2000. – 368 с.

103. Петренко И. Н. Безопасность экономического пространства хозяйствующего субъекта / И. Н. Петренко. – М. : Анкил, 2005. – 280 с.

104. Петренко И. О. Экономическая безопасность России : денежный фактор / Петренко И. О. – М. : Маркет ДС, 2003. – 240 с.

105. Пилипенко А. А. Економічна безпека акціонерного товариства в умовах протидії недружньому поглинанню / А. А. Пилипенко // Физические и компьютерные технологии в народном хозяйстве : труды 7-й Междун. науч.-техн. конференции, (Харків, 27 – 28 мая, 2003 р.). – Х. : ХНПК "ФЭД", 2003. – С. 187–189.

106. Пилипенко А. А. Економічна безпека логістичних процесів підприємства / А. А. Пилипенко // Вісник НТУ "ХПІ" : зб. наук. праць. – Х. : НТУ "ХПІ", 2005. – Т. 2. – № 58. – С. 162–164.

107. Пилипенко А. А. Організація обліку і контролю : підручник / А. А. Пилипенко, В. І. Отенко. – Х. : Видавничий Дім "ІНЖЕК", 2005. – 424 с.

108. Пономаренко В. С. Концептуальні основи економічної безпеки : монографія / В. С. Пономаренко, С. В. Кавун. – Х. : Вид. ХНЕУ, 2008. – 256 с.

109. Пономаренко В. С. Экономическая безопасность региона : анализ, оценка, прогнозирование / В. С. Пономаренко, Т. С. Клебанова, Н. Л. Чернов / Харьковский гос. экономический ун-т. – Х. : ИД "ИНЖЭК", 2004. – 144 с.

110. Про авторське право і суміжні права : Закон України від 23.12.1993 р. // Закони України. Т. 6. – К. : Ін-т законодавства ВР України, 1996. – 424 с.

111. Про банки та банківську діяльність : Закон України від 20.03.1991 р. // Закони України. Т. 1. – К. : Ін-т законодавства ВР України, 1996. – 462 с.

112. Про державну таємницю : Закон України від 21.01.1994 р. // Закони України. Т. 7. – К. : Ін-т законодавства ВР України, 1997. – 408 с.

113. Про захист інформації в автоматизованих системах : Закон України від 5.07.1994 р. // Закони України. Т. 7. – К. : Ін-т законодавства ВР України, 1997. – 408 с.

114. Про інформацію : Закон України від 02.10.1992 р. // Закони України. Т. 4. – К. : Ін-т законодавства ВР України, 1996. – 340 с.

115. Про Концепцію (основи державної політики) національної безпеки України : Постанова Верховної Ради України від 18 липня 1995 р. № 532-95-п // Відомості Верховної Ради (ВВР), 1997. – № 10. – Ст. 85.

116. Про Концепцію [основи державної політики] національної безпеки України : Постанова Верховної Ради України від 16 січня 1997 р. № 3/97-ВР // Право України. – 1997. – № 3. – С. 84–89.

117. Про науково-технічну інформацію : Закон України від 25.06.1993 р. // Закони України. Т. 5. – К. : Ін-т законодавства ВР України, 1996. – 288 с.

118. Про охорону прав на винаходи та корисні моделі : Закон України від 15.12.1993 р. //Закони України. Т. 6. – К. : Ін-т законодавства ВР України, 1996. – 424 с.

119. Про охорону прав на знаки для товарів та послуг : Закон України від 15.12.1993 р. // Закони України. Т. 6. – К. : Ін-т законодавства ВР України, 1996. – 424 с.

120. Про охорону прав на промислові зразки : Закон України від 15.12.1993 р. // Закони України. Т. 6. – К. : Ін-т законодавства ВР України, 1996. – 424 с.

121. Про перелік відомостей, що не становлять комерційної таємниці : Постанова Кабінету Міністрів України від 9 серпня 1993 р. № 611 // Збірник постанов Уряду України. – 1993. – № 12.

122. Про рекламу : Закон України від 03.07.96 р. // Відомості Верховної Ради (ВВР). – 1996. – № 39. – Ст. 182.

123. Про заходи щодо забезпечення інформаційної безпеки держави : Указ Президента України від 18 вересня 2002 р. // Офіційний Вісник України. – 2002. – № 38. – Ст. 1771.

124. Про заходи щодо захисту інформаційних ресурсів держави : Указ Президента України від 10 квітня 2000 р. // Офіційний Вісник України. – 2000. – № 15. – Ст. 650.

125. Пушкарь А. И. Стратегические группы предприятий: концепция, методология, управление : научное издание / А. И. Пушкарь, Ю. Е. Жуков, А. А. Пилипенко. – Х. : ООО "Кросс-Роуд", 2006. – 440 с.

126. Пярин В. Российская интеллектуальная карта создана и работает / Пярин В. // Бюллетень финансовой информации. – 1999. – № 12; 2000. – № 1.

127. Расторгуев С. П. Искусство защиты и раздевания программ / Расторгуев С. П. – М. : Радио и связь, 1991. – 224 с.

128. Родин Г. Некоторые соображения о защите программ / Родин Г. // Компьютер-пресс. – 1991. – № 10. – С. 15–18.

129. Румянцева Е. Е. Новая экономическая энциклопедия / Румянцева Е. Е. – 2-е изд. – М. : ИНФРА-М, 2006. – VI. – 810 с.

130. Сажина М. А. Фирма : управление кризисом : учебн. пособ. / М. А. Сажина. – М. : Деловая литература, 2004. – 191 с.

131. Слепов В. А. Финансовая политика компании : учебн. пособ. / В. А. Слепов, Е. И. Громова, И. Т. Кери / под ред. проф. Слепова С. А. – М. : Экономист, 2005. – 283 с.

132. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньнш. – М. : ДМК Пресс, 2002. – 656 с.

133. Соколов А. В. Защита от компьютерного терроризма : справочное пособие / А. В. Соколов, О. М. Степанюк. – СПб. : БВХ-Петербург ; Арлит, 2002. – 496 с.

134. Спесивцев А. В. Защита информации в персональных ЭВМ / А. В. Спесивцев, В. А. Вегнер, А. Ю. Крутяков. – М. : Радио и связь, 1992. – 192 с.

135. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. – М. : ГТК РФ, 1992. – 25 с.

136. Теория и практика обеспечения информационной безопасности. – М. : Изд. агент. "Яхтсмен", 1996. – 192 с.

137. Термины и определения в области защиты от НСД к информации. Руководящий документ Гостехкомиссии России. – М. : ГТК РФ, 1992. – 13 с.

138. Технические средства защиты информации. Каталог ЗАО "Анна". – М. : Изд. "Анна", 1999. – 112 с.

139. Технические средства защиты информации. Каталог НПЦ фирмы "НЕЛК". – М. : Изд. "НЕЛК", 1999. – 92 с.

140. Торокин А. А. Основы инженерно-технической защиты информации / Торокин А. А. – М. : Ось-89, 1998. – 336 с.

141. Тэпман Л. Н. Риски в экономике / Тэпман Л. Н. ; под ред. проф. Швандара В. А. – М. : ЮНИТИ, 2003. – 380 с.

142. Удалов В. И. Безопасность в среде взаимодействия открытых систем / В. И. Удалов, Я. П. Спринцис // Автоматика и вычислительная техника. – 1990. – № 3. – С. 3–11.

143. Уткин Э. А. Риск-менеджмнт / Уткин Э. А. – М. : ТАНДЕМ, 1998. – 288 с.

144. Ухлинов Л. М. Управление безопасностью информации в автоматизированных системах / Ухлинов Л. М. – М. : МИФИ, 1995. – 128 с.

145. Филиппова С. В. Трансформационные процессы в промышленном производстве в условиях нестабильности : [монографія] / Филиппова С. В. – Одесса : ОРИГУ НАГУ, 2005. – 420 с.

146. Хорев А. А. Способы и средства защиты информации / Хорев А. А. – М. : МО РФ, 1998. – 316 с.

147. Хорев А. А. Технические средства и способы технического шпионажа / Хорев А. А. – М. : ЗАТ "Дальснаб", 1997. – 242 с.

148. Хоффман Л. Д. Современные методы защиты информации / Хоффман Л. Д. ; пер. с англ. – М. : Сов. радио, 1980. – 264 с.

149. Цивільний кодекс України // Відомості Верховної Ради (ВВР). – 2003. – № 40 – 44. – Ст. 356.

150. Цыгичко В. Н. Информационное оружие как геополитический фактор и инструмент силовой политики / В. Н. Цыгичко, Г. Л. Смоляк, Д. С. Черепекин. – М. : ИСА АН РФ, 1997. – 252 с.

151. Шапкин А. С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций / Шапкин А. С. – М. : Дашков и К^0, 2005. – 544 с.

152. Шарый Л. Д. Безопасность предпринимательской деятельности : учебник / Л. Д. Шарый, В. М. Родачин ; Нац. ин-т бизнеса. – 2-е изд., доп. и перераб. – М. : Изд-во "ВК", 2005. – 477 с.

153. Энергоинформационная безопасность человека и государства / М. С. Алешенков, Б. Н. Родионов, В. Б. Титов и др. – М. : Паруса, 1997. – 126 с.

154. Экономика предприятия (фирмы) : учебн. пособ. / А. С. Пелих, Т. А. Высоцкая, В. М. Джуха и др. ; под ред. Пелиха А. С. – М. ; Ростов н/Д. : МарТ, 2004. – 505 с.

155. Экономика предприятия (фирмы) : учебник / О. И. Волков, О. В. Девяткин, Н. Б. Акуленко и др. ; под ред. О. И. Волкова, О. В. Девяткина. – 3-е изд., перераб. и доп. – М. : Инфра-М, 2004. – 600 с.

156. Ярочкин В. И. Аудит безопасности фирмы : теория и практика : учебн. пособ. для вузов / В. И. Ярочкин, Я. В. Бузанова. – М. : Акад. Проект ; Королёв: Парадигма, 2005. – 351 с.

157. Ярочкин В. И. Безопасность информационных систем / Ярочкин В. И. – М. : Ось-89, 1997. – 320 с.

158. Яскевич В. И. Секьюрити : Организационные основы безопасности фирмы / Яскевич В. И. – М. : "Ось-89", 2005. – 368 с.

159. ANSI/X3/SPARC Study Group on Database Management Systems : Interim report, 1975. – P. 92–141.

160. Evaluation Levels Manual, Department of Trade and Industry, Computer Security Branch, Kingsgate House. – V. 22. – P. 66–74.

161. ISO/DIS 2382/8. Data processing. – Vocabulary – Part 8 : Control, integrity and security. – ISO, 1985. – 35 p.

162. ISO/DIS 7498/2. Information Processing Systems – Open Systems Interconnection Reference Model. Part 2: Security Architecture. ISO, 1989. – 41 p.

163. Gladny H. M. In: Performance of Computer Installation, Berke. – 1978, Proceedings. – P. 151–200.

164. HighLand H. J. Novell network virus alert., C&S. – 1990. – V. 9. – № 7. – 570 p.

165. Linde Richard R. Operating System Penetration, Proceedings. – 1975 NCC. – P. 361–368.

166. Linden T. A. (editor) Security Analysis and Enhancements of Computer Operating Systems, Institute for Computer Sciences and Technology of National Bureau of Standarts, Washington, D.C. 20234, Report NBSIR 76-1041, April 1976.

167. Olson I. M. Computer Acces Policy Choices / Olson I. M., Abrams M. D. // Computer & Security. – V. 9(1990). – № 8. – PP. 699–714.

168. Security & Protection. – 1978. – V. 10. – № 2. – PP. 23–40.

169. Smith G.S. 2001. New Age Technology Threats and Vulnerabilities. Journal of Forensic Accounting. – PP. 125–130.

170. Straub D. W. Deviancy by bit and bytes : computer abusers and control measures / Straub D. W., Widom C. S. // Computer security : A Global Challenge. Netherlands,1984. – PP. 431–441.

171. Parker T. A. Application Access Control Standarts for Distributed Systems., Computer&Security. – V. 9. – № 6. – PP. 319–330.

172. Parker T. A. Security in Open Systems – A Report on the Standart work of ECMA's TC32/TG9, PP. 38 – 50 in Proc. 10th Natl. Computer Security Conf., IEEE, Baltimore, September, 1987.

173. Yves le Roux, Technical Criteria For Security Evaluation Of Information Technology Products / Information Security Guide, 1990/1991. – PP. 59–62.

174. Zabihollah Rezaee Financial Statement Fraud: Prevention and Detection, 2002. – PP. 276–279.

175. Концепция внешней политики Российской Федерации : Указ Президента РФ № 24 от 10 января 2000 года // Русская цивилизация [Электронный ресурс]. – Режим доступа : http://www.rustrana.ru/ article.php?nid=9007.

176. О безопасности : Закон РФ от 5 марта 1992 года № 2446-1 // Интернет и Право [Электронный ресурс]. – Режим доступа : http://www.internet-law.ru/law/inflaw/sec.htm.

177. О государственной тайне. Закон РФ // Интернет и Право [Электронный ресурс]. – Режим доступа : http://www.internet-law.ru/law/ inflaw/taina.htm.

178. О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам : Указ Президента РФ от 8 мая 1993 годя № 644 // Алтайский Государственный Технический Университет [Электронный ресурс]. – Режим доступа : http://edu.secna.ru /main/ review/2001/n3/zaginajlov3.txt.

179. О передаче сведений, которые не могут составлять коммерческую тайну : Постановление Правительства РСФСР от 5 декабря 1991 года № 35 // Элементы [Электронный ресурс]. – Режим доступа : www.elementy.ru/LIBRARY/zsecret.htm.

180. О рынке ценных бумаг : Федеральный закон от 22 апреля 1996 года № 39-ФЗ // Коснультант-Плюс [Электронный ресурс]. – Режим доступа : www.consultant.ru/popular/cenbum/.

181. О частной детективной и охранной деятельности в Российской Федерации : Закон РФ от 11 марта 1992 года // РИА Индустрия безопасности [Электронный ресурс]. – Режим доступа : http://www.securpress.ru /documents/21.htm.

182. Об информации, информатизации и защите информации : Закон РФ от 20 февраля 1995 года № 24-ФЗ // Коснультант-Плюс [Электронный ресурс]. – Режим доступа : www.consultant.ru/online/base/?req= doc;base=LAW;n=61798.

183. Об утверждении Концепции национальной безопасности Российской Федерации : Указ Президента РФ от 17 декабря 1997 года № 1300 (в ред. Указа Президента РФ от 10 января 2000 года № 24) // Федеральное государственное унитарное предприятие "Институт стратегической стабильности" [Электронный ресурс]. – Режим доступа : http://www.iss.niiit.ru/doktrins/doktr01.htm.

184. Об участии в международном информационном обмене : Закон РФ // Роспатент [Электронный ресурс]. – Режим доступа : http://www.fips.ru/npdoc/LAW/INFO.HTM.

185. Основы политики Российской Федерации в области развития науки и технологий на период до 2010 года и дальнейшую перспективу, утв. Президентом РФ 30 марта 2002 года // Роспатент [Электронный ресурс]. – Режим доступа : www.fips.ru /ruptoru/str_rf.htm.

186. Про затвердження Зводу відомостей, що становлять державну таємницю. Наказ СБ України № 440 від 12 серпня 2005 р. – [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws /main.cgi?page=1&nreg=z0902-05.

187. Про затвердження методики розрахунку рівня економічної безпеки України : Наказ Міністерства економіки України № 60 від 02.03.2007 р. / Правові системи НАУ [Електронний ресурс]. – Режим доступу : http://zakon.nau.ua/doc/?code=v0060665-07.

188. Про захист персональних даних. Закон України № 2297-VI від 1.06.2010 р. [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1510-17.

189. CSC-STD-003-85, Computer Security Requirements Guidance for Applying the Department of Defense System Evaluation Criteria in Specific Environments // Federation of American Scientist [Electronic recource]. – Access mode : www.fas.org/irp/nsa/ rainbow/std003.htm.

190. DoD 5200.28-STD. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC) 1985 [Electronic recource]. – Access mode : ftp.fas.org/irp/nsa/rainbow /std001.htm.

191. National Bureau of Standards, "Data Encryption Standard", January 1977, NIST NBS-FIPS PUB 46//Безопасность информационных технологий [Electronic recource]. – Access mode : www.security.ukrnet.net/ modules/sections/index.php?artid=181&op=viewarticle.

192. NCSC-TG-001. A Guide to Understanding Audit in Trusted Systems// Federation of American Scientist [Electronic recource]. – Access mode : fas.org/irp/nsa/rainbow/tg001.htm.

193. NCSC-TG-003. A Guide to Understanding Discretionary Access Control in Trusted Systems // Federation of American Scientist [Electronic recource]. – Access mode : ftp.fas.org/irp /nsa/rainbow/tg003.htm.

194. NCSC-TG-005. Version-1. Trusted Network Interpretation of the trusted Computer System Evaluation Criteria // National Technical Information Service [Electronic recource]. – Access mode : http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA255422.

195. NCSC-TG-006. A Guide to Understanding Configuration Management in Trusted Systems // Federation of American Scientist [Electronic recource]. – Access mode : www.fas.org/irp/nsa/rainbow/tg006.htm.

196. NCSC-TG-009. Version-1. Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria // Federation of American Scientist [Electronic recource]. – Access mode : ftp.fas.org/irp/nsa/rainbow/tg009.htm.

197. NCSC-TG-021. Version-1. Draft Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria // Безопасность информационных технологий [Electronic recource]. – Access mode : http://www.security.ukrnet.net/modules/sections/index.php?artid=181&op=viewarticle.

198. Datapro Reports on Information Security, vol.1-3, 1990-1993 // SCM.Portal [Electronic recource]. – Access mode : portal.acm.org/citation.cfm?id=17735.

Додатки

Додаток А

Перелік нормативних законодавчих актів, що регламентують ІБ

1. НД ТЗІ 1.1-004-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

2. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

4. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

5. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

Рекомендований перелік (на сьогодні найбільш повний, який змогли скласти автори) основних нормативно-правових актів України для використання при проведенні робіт, що здійснюються в межах господарської діяльності в галузі технічного захисту інформації (ТЗІ) та криптографічного захисту інформації (КЗІ), наводиться також мовою оригіналу [63]:

1. Закон України "Про інформацію".

2. Закон України "Про ліцензування певних видів господарської діяльності".

3. Закон України "Про захист інформації в АС".

4. Закон України "Про державну таємницю".

5. Указ Президента України від 10.04.2000 р. № 582/2000 "Про заходи щодо захисту інформаційних ресурсів держави".

6. Концепція технічного захисту інформації в Україні. Затверджено Постановою Кабінету Міністрів України від 08.10.97 р. № 1126.

7. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 р. № 1229/99.

8. Положення про контроль за функціонуванням системи ТЗІ. Затверджено наказом ДСТСЗІ СБУ № 61 від 22.12.99 р.

9. Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом ДСТСЗІ СБ України № 62 від 29.12.99.

10. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Затверджено Постановою Кабінету Міністрів України від 16.02.98 р. № 180.

11. Положення про порядок опрацювання, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації. Затверджено наказом ДСТЗІ № 44 від 01.07.96 р.

12. ДСТУ 3396 0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.

13. ДСТУ 33961-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.

14. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.

15. ДБН А.2.2-2-96. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. Затверджені наказом Держкоммістобудування України від 02.09.96 р. № 156.

16. Тимчасове положення про категорування об’єктів (ТПКО-95). Затверджено наказом ДСТЗІ від 10.07.95 р. № 35.

17. Ліцензійні умови провадження господарської діяльності, пов’язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації. Затверджено наказом Державного комітету України з питань регуляторної політики та підприємництва, ДСТСЗІ СБ України від 29.12.2000 р. № 89/67.

18. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). Затверджені наказом ДСТЗІ від 09.06.95 р. № 25.

19. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95). Затверджені наказом ДСТЗІ від 09.06.95 р. № 25.

20. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

21. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

22. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

23. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53.

24. НД ТЗІ 1.5-001-2000. Радіовиявлювачі. Класифікація. Загальні технічні вимоги. Затверджено наказом ДСТСЗІ СБ України № 29 від 13.06.2000 р.

25. НД ТЗІ 1.6-001-96. Правила побудови, викладення, оформлення та позначення нормативних документів системи ТЗІ. Затверджено наказом ДСТЗІ від 26.07.96 р. № 51.

26. НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТЗІ від 09.02.2001 р. № 2.

27. НД ТЗІ 2.3-001-2001. Радіовиявлювачі вимірювальні. Методи та засоби випробувань. Затверджено наказом ДСТЗІ від 27.02.2001 р. № 5.

28. НД ТЗІ 2.3-002-2001. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань. Затверджено наказом ДСТСЗІ СБ України від 06.04.2001 р. № 11.

29. НД ТЗІ 2.3-003-2001. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань. Затверджено наказом ДСТСЗІ СБ України від 06.04.2001 р. № 11.

30. НД ТЗІ 2.3-004-2001. Радіовиявлювачі індикаторні. Методи та засоби випробувань. Затверджено наказом ДСТСЗІ СБ України від 09.04.2001 р. № 12.

31. НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

32. НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

33. НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

34. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

35. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

36. НД ТЗІ 2.5-006-99. Класифікатор засобів копіювально-розмножувальної техніки. Затверджено наказом ДСТСЗІ СБ України від 26.07.99 р. № 34.

37. НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

38. НД ТЗІ 2.7-002-99. Методичні вказівки з використання засобів копіювально-розмножувальної техніки. Затверджено наказом ДСТСЗІ СБ України від 26.07.99 р. № 34.

39. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 р. № 60.

40. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

41. НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова). Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

42. НД ТЗІ 4.7-001-2001. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань. Затверджено наказом ДСТСЗІ СБ України від 06.04.2001 р. № 11.

43. НД ТЗІ Р-001-2000. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація й загальні технічні вимоги. Рекомендації. Затверджено наказом ДСТСЗІ СБ України від 04.09.2000 р. № 41.

44. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22.05.98 р. № 505.

45. Положення про державний експортний контроль в Україні, затверджене Указом Президента України від 13.02.98 р. № 117.

46. Декрет Кабінету Міністрів України від 10.05.93 р. № 46-93 "Про стандартизацію і сертифікацію".

47. Постанова Кабінету Міністрів України від 14.11.2000 р. № 1698 "Про затвердження переліку органів ліцензування".

48. Постанова Кабінету Міністрів України від 29.10.2000 р. № 1755 "Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу".

49. Положення про порядок контролю за експортом, імпортом і транзитом окремих видів виробів, обладнання, матеріалів, програмного забезпечення і технологій, що можуть використовуватися для створення озброєння, військової чи спеціальної техніки, затверджене Постановою Кабінету Міністрів України від 22.08.96 р. № 1005.

50. Ліцензійні умови провадження господарської діяльності з розроблення, виробництва, використання, експлуатації сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації, затверджені наказом Державного комітету України з питань регуляторної політики та підприємництва, Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 29.12.2000 р. № 88/66 і зареєстровані в Міністерстві юстиції України 20.01.2001 р. за № 49/5240.

51. Положення про порядок проведення експертизи в галузі експортного контролю, затверджене Постановою Кабінету Міністрів України від 15.07.97 р. № 767.

52. Положення про порядок надання суб'єктам зовнішньоекономічної діяльності повноважень на право здійснення експорту, імпорту товарів військового призначення та товарів, які містять відомості, що становлять державну таємницю, затверджене Постановою Кабінету Міністрів України від 08.06.98 р. № 838.

53. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затверджена Постановою Кабінету Міністрів України від 27.11.98 р. № 1893.

54. Звід відомостей, що становлять державну таємницю України, затверджений наказом Державного комітету України з питань державних секретів від 31.07.95 р. № 47 і зареєстрований у Міністерстві юстиції України 03.08.95 р. за № 278/814.

55. Інструкція про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави, затверджена наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 22.10.99 р. № 45 і зареєстрована в Міністерстві юстиції України 29.11.99 р. за № 817/4110.

56. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 30.11.99 р. № 53 і зареєстроване в Міністерстві юстиції України 15.12.99 р. за № 868/4161.

57. Тимчасова інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена спільним наказом Держстандарту України та Служби безпеки України від 28.11.97 р. № 708/156 і зареєстрована в Міністерстві юстиції України 17.12.97 р. за № 598/2402.

58. Порядок видачі сертифікатів затвердження типу засобів вимірювальної техніки, сертифікатів відповідності засобів вимірювальної техніки затвердженому типу та свідоцтв про визнання затвердження типу засобів вимірювальної техніки, затверджений наказом Держстандарту України від 31.01.97 р. № 56 і зареєстрований у Міністерстві юстиції України 15.04.97 р. за № 137/1941.

59. Порядок проведення робіт із сертифікації продукції іноземного виробництва, що виготовляється серійно, затверджений наказом Держстандарту України від 18.08.98 р. № 633 і зареєстрований у Міністерстві юстиції України 14.10.98 р. за № 657/3097.

60. Правила визначення вартості робіт із сертифікації продукції та послуг, затверджені наказом Держстандарту України від 10.03.99 р. № 100 і зареєстровані в Міністерстві юстиції України 31.03.99 р. за № 194/3487.

61. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

62. ГОСТ 34.310-95. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

63. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования.

64. ДСТУ 1.0-93. Державна система стандартизації України. Основні положення.

65. ДСТУ 1.3-93. Державна система стандартизації України. Порядок розроблення і побудови, викладення та оформлення технічних умов.

66. ДСТУ 1.4-93. Державна система стандартизації України. Стандарти підприємства. Основні положення.

67. ДСТУ 1.5-93. Державна система стандартизації України. Загальні вимоги до побудови, викладу, оформлення та змісту стандартів.

68. ДСТУ 1.6-97. Державна система стандартизації України. Порядок державної реєстрації галузевих стандартів, стандартів науково-технічних та інженерних товариств і спілок.

69. ДСТУ 2296-93. Національний знак відповідності. Форма, розміри, технічні вимоги та правила застосування.

70. ДСТУ 2462-94. Сертифікація. Основні поняття. Терміни та визначення.

71. ДСТУ 3410-96. Система сертифікації УкрСЕПРО. Основні положення.

72. ДСТУ 3412-96. Система сертифікації УкрСЕПРО. Вимоги до випробувальних лабораторій та порядок їх акредитації.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Кавун Сергій Віталійович
Пилипенко Андрій Анатолійович
Ріпка Дар'я Олександрівна

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ У СИСТЕМІ КОНСОЛІДОВАНОЇ ІНФОРМАЦІЇ

Навчальний посібник
для студентів спеціальності
8.03050901 "Облік і аудит"

Відповідальний за випуск **Пушкар О. І.**

Відповідальний редактор **Сєдова Л. М.**

Редактор **Бутенко В. О.**

Коректор **Мартовицька-Максимова В. А.**

План 2013 р. Поз. № 121-П.
Підп. до друку Формат 60 х 90 1/16. Папір MultiCopy. Друк Riso.
Ум.-друк. арк. 22,75. Обл.-вид. арк. 28,44. Тираж прим. Зам. №

Видавець і виготівник – видавництво ХНЕУ, 61166, м. Харків, пр. Леніна, 9а

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи
Дк № 481 від 13.06.2001 р.