УДК [658.15:005.934]:005.92

Марунич А. В.

Магістр 1 року навчання
факультету обліку і аудиту ХНЕУ ім. С. Кузнеця

ІНФОРМАЦІЙНА СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Анотація. Розкрито сутність поняття "інформаційна безпека підприємства", її взаємозв'язок із суб'єктом інформаційного середовища. Розглянуто вимоги щодо інформації, окреслено категорії суб'єктів інформаційної безпеки, а також подано механізм забезпечення захисту суб'єктів інформаційних відносин від негативного інформаційного впливу, що є складовою інформаційної безпеки.

Аннотация. Раскрыта сущность понятия "информационная безопасность предприятия", ее взаимосвязь с субъектом информационной среды. Рассмотрены требования к информации, обозначены категории субъектов информационной безопасности, а также представлен механизм обеспечения защиты субъектов информационных отношений от негативного информационного воздействия, что является составляющей информационной безопасности.

Annotation. The essence of the concept "information security" of a company and its relationship with the subject of the information environment is studied. Requirements to information are outlined, categories of information security subjects are discussed and a mechanism of protecting the subjects of information relations from the negative impact of information is provided as part of information security.

Ключові слова: інформаційна безпека, суб'єкти інформаційного середовища, захищеність суб'єктів інформаційних відносин, інформаційні потреби, небезпечна інформація.

Спочатку поняття інформаційна безпека в науковій літературі ототожнювалося з поняттям безпека інформації. Пізніше стали використовувати інший термін – "захищеність суб'єктів інформаційних відносин від негативних інформаційних впливів".

У сучасній літературі з питань інформаційної безпеки наведено цілий ряд визначень поняття "інформаційна безпека": захищеність інформації, що обробляється в інформаційно-обчислювальній системі від випадкових або навмисних впливів внутрішнього або зовнішнього характеру, що можуть нанести шкоду власникам інформаційних ресурсів або користувачам інформації [1].

Відповідно до цього визначення забезпечення інформаційної безпеки не зводиться тільки до захисту від протиправних дій з боку тих чи інших осіб. Найважливіше значення тут має захист від можливих впливів, що носять випадковий характер (аварії, збої в устаткуванні, у системі електропостачання, опаленні, водопостачанні, природні катастрофи тощо), а також від випадкових помилок користувачів і обслуговуючого персоналу інформаційних систем.

Вивченням проблеми інформаційної безпеки підприємства займалися такі вітчизняні вчені, як: В. Геєць, Л. Абалкін, Г. Пастернак-Тапущенко, Б. Гунський, Н. Реверчук, С. Реверчук, І. Кульчицький, Ю. Лисенко, Р. Руденський, А. Спірідонов, Т. Кузенко, Г. Козаченко, В. Пономарьов, О. Ляшенко, С. Міщенко, О. Новікова, Р. Покотиленко, Т. Соколенко, О. Сумець, М. Тумар та ін.

Мета статті полягає в дослідженні теоретичних положень щодо оцінки та забезпечення інформаційної безпеки підприємства, зокрема суб'єктів інформаційного середовища та запобігання негативного інформаційного впливу на них. Для досягнення поставленої мети були вирішені такі завдання:

1) визначення сутності поняття інформаційна безпека;

2) виявлення факторів і проблем, що негативно впливають на інформаційну безпеку суб'єкта інформаційного середовища;

3) охарактеризування категорії суб'єктів інформаційної безпеки.

У практичному плані інформаційна безпека існує лише у взаємозв'язку із суб'єктом інформаційного середовища, саме суб'єкт диктує показники такої безпеки. Це відноситься не тільки до конкретних суб'єктів, але і до особистості, суспільства та держави. Інформаційна безпека суб'єкта не може бути забезпечена без наявності у нього необхідної інформації. Інформаційні потреби різних суб'єктів не однакові, але для будь-якого суб'єкта відсутність можливості отримання необхідної інформації може мати негативні наслідки. Ці наслідки можуть носити різний характер, їх важкість залежить від складу відсутньої інформації.

Необхідна для задоволення інформаційних потреб інформація повинна відповідати певним вимогам:

1) інформація повинна бути відносно повною, оскільки абсолютно повної інформації жоден суб'єкт мати не може. Повнота інформації характеризується її достатністю для прийняття правильних рішень;

2) інформація повинна бути достовірною, бо недостовірна інформація призводить до прийняття неправильних рішень;

3) інформація повинна бути своєчасною, оскільки необхідні рішення ефективні лише тоді, коли вони приймаються вчасно [1].

Прийняттю неправильних рішень може сприяти наявність шкідливої, небезпечної для суб'єкта інформації, яка найчастіше цілеспрямовано нав'язується. Це вимагає забезпечення захисту суб'єктів інформаційних відносин від

негативного інформаційного впливу, що є ще однією складовою інформаційної безпеки.

При такому підході можна сформулювати таке визначення поняття інформаційна безпека – це стан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу [1].

При забезпеченні інформаційної безпеки важливо враховувати ті завдання, які висуваються перед сторонами, зацікавленими в інформаційній безпеці, а саме [2]:

1) забезпечення доступності інформації, що має на увазі можливість за прийнятний час отримати необхідну інформаційну послугу, а також запобігти несанкціонованій відмові в отриманні інформації;

2) забезпечення цілісності інформації, що передбачає запобігання несанкціонованої модифікації або руйнування інформації;

3) забезпечення конфіденційності інформації, що пов'язано із запобіганням несанкціонованого ознайомлення з інформацією.

Виділяють чотири категорії суб'єктів інформаційної безпеки, які відрізняються один від одного правовим, технічним, фінансовим, організаційним та іншим ресурсним забезпеченням своєї інформаційної безпеки, а саме: держава в цілому; державні організації; комерційні структури; окремі громадяни [2].

У забезпеченні інформаційної безпеки виділяють кілька рівнів [3]:

1) політичний: на цьому рівні приймаються документи, в яких визначаються основні напрями державної політики в галузі інформаційної безпеки, формулюються цілі та завдання забезпечення інформаційної безпеки щодо всіх окреслених суб'єктів, плануються шляхи і засоби реалізації поставлених цілей;

2) законодавчий: на цьому рівні приймаються нормативно – правові акти (закони, постанови уряду тощо), спрямовані ініціювати створення і функціонування системи правового регулювання забезпечення інформаційної безпеки;

3) нормативно-технічний: на даному рівні здійснюється розробка стандартів, керівних і методичних матеріалів та документів, що регламентують процес розробки, впровадження та експлуатації засобів забезпечення інформаційної безпеки. Проводиться приведення у відповідність національних та міжнародних стандартів у сфері інформаційних технологій;

4) адміністративний: здійснення заходів щодо забезпечення безпеки на даному рівні, проводиться в рамках конкретного підприємства, установи, організації. На цьому рівні керівництво організації реалізує конкретні заходи щодо забезпечення інформаційної безпеки. В їх основі лежить політика безпеки підприємства (сукупність документованих управлінських рішень, спрямованих на захист інформації), що визначає стратегію підприємства в галузі інформаційної безпеки, а також обсяг виділених ресурсів для створення та функціонування системи інформаційної безпеки підприємства.

У числі конкретних заходів щодо забезпечення інформаційної безпеки можна виділити кілька основних: управління персоналом підприємства; фізичний захист майна та працівників підприємства; підтримка працездатності персоналу й устаткування підприємства; реагування на порушення режиму безпеки (санкції стосовно порушників, удосконалення системи безпеки, розробка та реалізація запобіжних заходів щодо забезпечення інформаційної безпеки); планування відновлювальних робіт;

5) програмно-технічний рівень: даний рівень передбачає використання як мінімум декількох механізмів забезпечення інформаційної безпеки, серед них: ідентифікація та перевірка справжності користувачів засобів інформатизації; управління доступом до інформації; протоколювання й аудит; криптографія; екранування; забезпечення високої доступності [3].

У сучасних умовах використання різних механізмів забезпечення інформаційної безпеки стало актуальним не тільки для окремих підприємств, установ, організацій, як державних, так і приватних, але і для простих громадян. Несанкціонований доступ до інформації особистого характеру може ініціювати вчинення правопорушень стосовно життя і майна громадян.

Наук. керівн. Мозгова Л. О.

Література: 1. Информационная безопасность государственных организаций и коммерческих фирм : справочное пособие / под общ. ред. Л. Д. Реймана. – М. : НТЦ ФИОРД-ИНФО , 2002. – С. 13. 2. Игнатьев В. А. Информационная безопасность современного коммерческого предприятия : монография / В. А. Игнатьев. – Старый Оскол : ООО "ТНТ", 2005. – 448 с. 3. Садердинов А. А. Информационная безопасность предприятия : учебное пособие. – 2-е изд. – М. : Изд.-торг. корпорация "Дашков и Ко", 2005. – 336 с. 4. Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения / Козаченко А. В., Пономарев В. П., Ляшенко А. Н. – К. : Либра, 2003. – 280 с. 5. Економічна безпека підприємства : підручник / Ортинський В. Л., Керницький І. С., Живко З. Б. та ін. – К. : Алерта, 2011. – 706 с.