форм навчання / О. В. Іванісов, О. А. Єрмоленко, С. О. Садчиков. – Харків: Вид. ХНЕУ, 2006. – 236 с. 11. Мирчев М. К. Улучшение результативности труда менеджеров с целью повышения конкурентности организаций / М. К. Мирчев, Г. В. Шереметов // Персонал. – 2006. – №11. – С. 69 – 74. 12. Оценка деятельности функциональных подразделений промышленных предприятий в условиях коллективного подряда. – М.: Экономика, 1990. – 32 с. 13. Радчук А. Работа руководителя в структурных подразделениях / А. Радчук, Е. Беловодская, А. Кихтенко // Справочник кадровика. – 2005. – №6. – С. 79 – 83. 14. Харченко М. Комплексна система оцінки результатів праці та особистих якостей працівників малих підприємств // Справочник кадровика. – 2003. – №12. – С. 79 – 82. 15. Харченко М. Показники оцінки результатів діяльності працівників підприємств та деякі підходи до організації матеріального стимулювання їх праці / М. Харченко, С. Шкорінов // Україна: аспекти праці. – 2003. – №4. – С. 34 – 40. 16. Боркова Н. В. Методичні засади стратегічного управління діяльністю менеджерів // Вісник Хмельницького національного університету. – 2007. – №5. – Т. 1. – С. 93 – 97. 17. Макаров С. В. Менеджер за работой. – М.: Молодая гвардия, 1989. – 240 с. 18. Молл Е. Г. Управление карьерой менеджера. – СПб.: Питер, 2003. – 352 с. 19. Справочник менеджера / Под ред. проф. И. А. Уткина. – М.: Ассоциация авторов и издателей "Тандем", изд. "ЭКМОС", 1998. – 448 с. 20. Лидер и команда. Практическое руководство лидера эффективной команды. – Днепропетровск: Balances bussiness books, 2005. – 296 с. 21. Ермошенко Н. Н. Управление производством и руководитель (организационно-экономический аспект). – К., Донецк: Вища школа, 1983. – 172 с. 22. Журавльова І. В. Управління людським капіталом. Наукове видання / І. В. Журавльова, А. В. Кудлай. – Харків: Вид. ХНЕУ, 2004. – 284 с.

Стаття надійшла до редакції 26.12.2007 р.

УДК 004.05:338.3

Кавун С. В.

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ ИНСАЙДЕРАМ В ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Different schemes of realization of insiders actions for the managers of different ranks are offered. The planned measures of elimination the channels of information leak are built.

Сегодня в современном мире, в эпоху стремительного развития ИТ-технологий и их внедрения в экономику предприятия, особенно актуальным становится вопрос обеспечения экономической безопасности (ЭБ) предпринимательской деятельности при нежелательных (незаконных) действиях своих сотрудников. Одной из таковых категорий являются **инсайдеры**, которые представляют собой обычных сотрудников предприятия, владеющих категорированной информацией и предоставляющих ее (по каким-либо условиям: за деньги, шантаж, личное недовольство руководством и др.) посторонним предприятиям. Согласно экономическому словарю, инсайдер (англ. insider, от inside − буквально внутри) − лицо, имеющее в силу своего служебного или семейного положения доступ к конфиденциальной информации предприятия; это должностные лица, директора, основные акционеры предприятия с широким владением акций и их ближайшие родственники. В эту группу включаются также лица, добывающие конфиденциальную информацию о деятельности предприятия и использующие ее в целях личного обогащения. Подобные предприятия чаще всего являются конкурентами на рынке. Именно таким образом и организуется один из каналов утечки категорированной информации. Здесь следует оговорить, что данная категория сотрудников действует целенаправленно по отношению к "сливу" информации конкурентам.

Целью статьи является показ возможных схем реализации действий инсайдеров для руководителей различных рангов и построение плановых мероприятий по устранению каналов утечки категорированной информации на предприятии.

Объект исследования — система ЭБ предпринимательской деятельности, построенная на базе различных моделей управления, например, представленной в работе [1].

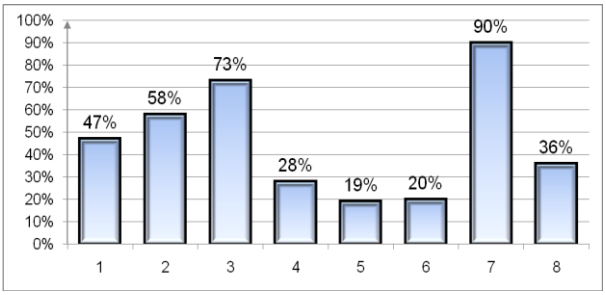
Проведенный сравнительный анализ источников статистической информации (Computer Security Institute, CSI, [2]) показал устойчивую тенденцию роста потерь различных ресурсов предприятия от деятельности инсайдеров. Свидетельством тому является показатель превышения в 2007 году уровня инцидентов на предприятиях, связанных с инсайдерами, по сравнению с вирусными заражениями (рис. 1).

Рис. 1. **Динамика изменения численности вирусных заражений и действий инсайдеров в процентах**

Кроме того, по данным компании IDC, в 2007 году емкость рынка управления безопасностью и обеспечения защиты данных составила колоссальную сумму в 2,27 млрд. долларов с приростом в 20% за год. На сегодня это превышает суммарные затраты на программное обеспечение в целом с его ростом в 6 − 7% за год.

Все это свидетельствует о возникающих потребностях в профессиональных сотрудниках в сфере экономической безопасности и защиты информации. В ближайшие три года, при соблюдении темпов развития ИТ-инфраструктуры, предприятия просто должны будут львиную долю расходов выделять на реализацию мероприятий и приобретение соответствующих средств обеспечения ЭБ предпринимательской деятельности и защищенности информации, объем которой образует информационный взрыв [3].

Однако еще достаточно большое количество малых предприятий думает, что проблема киберпреступлений − это проблема большого бизнеса. 47% из них, по исследованиям европейских компаний, считают себя достаточно малыми целями для подобных преступлений. Анализ состояния безопасности и защиты данных на предприятиях показан на рис. 2.



Условные обозначения:
1 – считают, что являются малыми целями;
2 – не волнует состояние ЭБ;
3 – считают доступность ресурсов критической для бизнеса;
4 – тратят 1 час в неделю на превентивную безопасность;
5 – считают, что кибератаки лишат их бизнеса вообще;
6 – подтверждают проведение атак на их ресурсы;
7 – считают, что они хорошо защищены;
8 – приняли настройки безопасности по умолчанию.

Рис. 2. **Статистика состояния безопасности предприятий**

По данным ООН, уже сегодня ущерб, наносимый компьютерными преступлениями и деятельностью инсайдеров, сопоставим с доходами от незаконного оборота наркотиков и оружия. Только в США ежегодный экономический ущерб от такого рода преступлений составляет около 100 млрд. долл. Причем многие потери не обнаруживаются или о них не сообщают.

В своей деятельности инсайдеры используют либо известные каналы утечки информации (например, электронная почта, копирование на внешние носители, получение бумажных копий документов, сканирование), либо создают собственные (например, "зомбирование" собственного ПК для возможности удаленного доступа, предоставление аутентификационных данных посторонним лицам, использование заведомо слабых паролей, некачественное уничтожение бумажных носителей).

Перечень используемых программных и аппаратных средств сегодня настолько велик и многообразен, что его перечисление займет достаточно много места. Одно лишь стоит оговорить обязательно – трудностей в нахождении и приобретении подобных средств сегодня не существует никаких.

Каковы же механизмы работы инсайдеров, их методики и используемые организационные методы? Для начала все множество инсайдеров необходимо классифицировать по некоторым признакам. Поскольку основным объектом, на который направлена деятельность инсайдеров, является информация (причем категорированная: коммерческая, банковская, персональная, служебная, аутентификационная, финансовая), то одним из признаков классификации выступает уровень доступности данных для инсайдеров (рис. 3).

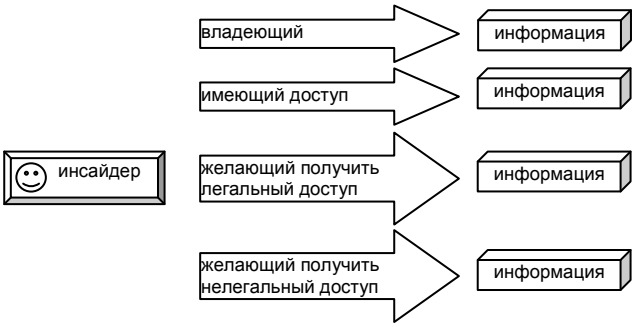


Рис. 3. **Классификация инсайдеров по уровню доступности данных**

Автор умышленно использовал понятие "информация", а не "данные", поскольку первое понятие намного шире, а данные могут быть частным случаем формализованного представления информации, пригодном для использования в любом бизнес-процессе.

Приведем несколько примеров для детального описания введенных различий в табличной форме (таблица).

Таблица

Примеры вариантов использования понятий

Бизнес-процесс	Данные	Информация
Набор специалистов	Рекламные объявления	Предоставление новой услуги
Подготовка к выпуску новой продукции	Спецификации, рецепты, формуляры, дистрибутив, исходные коды	Уровень готовности продукта, технические характеристики, сроки выхода
Предоставление новой услуги (банковской, юридической, коммерческой, промышленной)	План реализации, техническое описание, модель	Расширение сферы влияния на рынке, выход на более высокий конкурентный уровень, привлечение большего числа клиентов

Исходя из приведенной классификации (рис. 3), можно с достаточной степенью уверенности выделить категории сотрудников предприятия, которые могут быть потенциальными инсайдерами:

1. Менеджеры.
2. Руководители младших рангов (у старших руководителей есть стимулы, заинтересованности, предлоги).
3. Соучредители, владеющие меньшей частью капитала.
4. Рядовые сотрудники, имеющие по роду своей деятельности доступ к категорируемой информации и недовольные объемами предоставляемых ресурсов (должность, денежные вознаграждения, премии, временные вознаграждения: отгулы, отпуска).

Кстати, действиями инсайдеров могут быть не только "слив" информации, но и, например, преднамеренная порча, изменение или уничтожение информации (данных), что является умышленной угрозой. И за всем этим также стоят (хотя и меньшие) ресурсопотери: денежные, временные, финансовые, статистические, банковские и др.

Имея предоставленные выше данные, получаем множество возможных вариантов деятельности инсайдера (рис. 4).

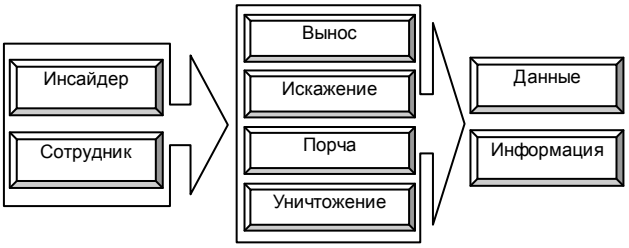


Рис. 4. **Варианты деятельности инсайдера**

При обычном расчете общее количество всех вариантов составит 16 с учетом всех комбинаций.

Дальнейшие организационные меры по выявлению (предотвращению деятельности) и ликвидации последствий являются базовыми и могут быть представлены как методика следующим образом:

1. Усиление правил использования и составления паролей.
2. Внедрение и тщательное соблюдение известных (мировых) стандартов, внутренних инструкций, законодательных актов, норм, правил, законов.
3. Четкое разграничение прав доступа и внимательный выбор объекта для делегирования текущих прав другим сотрудникам.

4. Введение на предприятии собственной службы информационной и экономической безопасности, а также группы улаживания инцидентов по компьютерной (информационной и экономической) безопасности – ГУИКБ [4].

5. Плановое (еженедельное, квартальное, полугодовое, годовое, внеплановое) обследование предприятия на предмет выявления известных (и не известных) каналов утечки информации.

6. Использование системы масштабного "логирования" (записи в файл всех операций, действий, транзакций) для наиболее уязвимых мест системы и критичных ресурсов предприятия.

Данный перечень можно бесконечно долго продолжать и вводить новые рекомендации, тем более при современном уровне развития ИТ-технологий в современном мире. Однако увеличение их количества может дать обратный эффект, когда в гонке за количеством реализаций защитных функций будет существенным образом теряться качество. Кроме того, при этом возрастает сложность, что также скажется на качестве их реализации в предпринимательской деятельности. Поэтому представленное количество автор считает "золотой серединой" и оптимальным множеством для начального внедрения на предприятии.

Применение методики повышения стойкости паролей и улучшения их запоминаемости позволит в значительной степени улучшить качество запоминания вводимых паролей, не снижая при этом их длины. Основные действия (приемы):

1. Использование транслитерации – прием ввода данных (символов пароля), при котором символы вводятся в одной раскладке, например, английской, а само слово (или часть его) вводится, глядя на другую раскладку. Например, слово на русском языке "крепость" реально будет выглядеть как "rhtgjcnm". Этот прием позволит в некоторой степени осложнить использование визуального канала съема информации или обычного подсматривания при вводе пароля.

2. Внедрение в начале/в середине/в конце пароля символа (более одного приводит к усложнению запоминания) с изменяемым регистром, то есть если пароль вводится строчными символами, то использование в указанных местах прописного символа (это дополнительное нажатие клавиши Shift во время ввода, что можно сделать незаметно с помощью мизинца) увеличивает его криптостойкость, не снижая способность к запоминанию. Данный прием основан на психологическом факторе человека, при котором довольно легко можно запомнить символ и его местоположение, отличный от всех вводимых остальных. Таким образом, введенный пароль может выглядеть так: "КРЕПОСТЬ" или "каВун".

3. Использование в тех же местах (см. п. 2) цифр, но не более двух, так как большее количество уже будет заметно при вводе. Этот прием также усложняет процесс подсматривания во время ввода пароля. Таким образом, введенный пароль может выглядеть так: "2крепость" или "кавун78".

4. При вводе осмысленных литературных слов (это не рационально с точки зрения криптостойкости и возможности атаки по словарю) рекомендуется подбирать слова, состоящие из рядом находящихся букв на клавиатуре (подразумевается установленная раскладка клавиатуры – QWERTY). Это позволит, не владея достаточной скоростью набора, ввести пароль с необходимой скоростью, что также уменьшит вероятность подсматривания во время ввода пароля. Таким образом, введенный пароль может выглядеть так: "крепость" или "кавун".

5. Использование обратного порядка ввода осмысленных слов – для овладения этим приемом необходимы соответствующие навыки, что может не каждый пользователь. Кроме того, не стоит забывать о подобных возможностях в программах аудита (взлома) парольной защиты, например, SAMInside или L0phtCrack 5. Таким образом, введенный пароль может выглядеть так: "ьтсоперк" или "нувак".

6. Использование ASCII-кодов второй половины таблицы (вводимый код является трехзначной цифрой). Данный прием эффективен, если вводимый пароль представляет собой цифровой код достаточной длины, например, номер сотового телефона с кодом оператора. Тогда вводимая последовательность будет неразрывной при вводе и, следовательно, незаметной. Методика ввода: правой рукой на цифровой панели вводится цифровая последовательность, а левой рукой незаметно нажимаются соответствующие клавиши (Shift+Alt) при вводе альтернативного кода. Таким образом, введенный пароль может выглядеть так "34657**156**45768**210**456", где жирным цветом показаны альтернативные коды – 156 и 210. Кроме того, этим способом можно получить достаточную длину пароля.

7. Использование свойства "обыденности" фразы, что приводит к значительному увеличению длины пароля, то есть в качестве пароля используется известная, обыденная фраза, словосочетание, предложение, афоризм, пословица, стихи, строки песни.

8. Использование свойства "необычности или неординарности", что является противодействием методу социальной инженерии: взломщик, следя за владельцем пароля, составляет индивидуальный словарь пользователя (его привычки, слова-паразиты, жаргон, сленг, клички животных, даты, сокращения, аббревиатуры), который потом будет использовать для атаки по словарю. Тогда, применяя данное правило, пользователь использует в качестве пароля совершенно необычное для него слово, фразу, словосочетание.

Следует также уделить должное внимание возможности защиты от программ, называемых KeyLogger-ами, которые записывают скан-коды всех нажимаемых клавиш на клавиатуре, что вообще лишает смысла использование каких-либо приемов и правил повышения криптостойкости парольной защиты, так как символы считываются еще до момента их использования в пароле. Некоторые подобные программы можно еще и хорошо спрятать от возможности визуального обнаружения. Эти же функции перехвата скан-кодов могут быть реализованы и аппаратно в виде небольшого устройства, которое подключается в разрыве клавиатурного кабеля. Если функции перехвата реализовываются программным способом, то подобные программы должны быть предварительно внедрены в систему и прописаны в одном из следующих источников автозапуска:

1. Пуск → Программы → Автозагрузка.
2. Ветвь реестра → Local Machine Run.
3. Ветвь реестра → Local Machine Run once.
4. Ветвь реестра → Current User Run.
5. Ветвь реестра → Current User Run once.

Для выявления подобных источников можно пользоваться так называемыми программами твикерами (от англ. *Tweak*) – редакторами скрытых настроек ОС или редакторами реестра. Кстати, используя эти же источники, работают некоторые вирусы.

Таким образом, на основе предложенных методик можно получить первичную информацию, необходимую для дальнейшего построения экономической модели работы инсайдеров в предпринимательской деятельности.

Продолжение статьи планируется в следующем номере журнала.

Литература: 1. Кавун С. В. Концептуальная модель системы экономической безопасности предприятия // Економіка розвитку. – 2007. – №3(43). – С. 97 – 101. 2. FBI: Computer Crime Survey // www. fbi. gov/publications. 3. Кавун С. В. Информационная безопасность в бизнесе. Научное издание. – Харьков: Изд. ХНЭУ, 2007. – 408 с. 4. Кавун С. В. Методика построения политики безопасности организации / С. В. Кавун, Г. В. Шубина // Бизнес Информ. – 2005. – №1 – 2. – С. 96 – 102.

Стаття надійшла до редакції 29.11.2007 р.