УДК 004.056.5

ПОДХОД К ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ВЫЯВЛЕНИЯ ИНСАЙДЕРОВ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

А.В. Снегуров
Кандидат технических наук, доцент*
Контактный тел.: (057) 702-10-67
Email: arksn@rambler.ru
А.Д. Кравченко*
Контактный тел.: 067-251-86-61
Email: kravchenko_ad@rambler.ru
Е.А. Ткаченко*
Контактный тел.: 063-569-54-77
Email: tkachenko_evgen@bigmir.net
*Кафедра телекоммуникационных систем
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, г. Харьков, Украина, 61166

У статті розглядається проблема виявлення інсайдерів в організації. Пропонується підхід до побудови сигнатур (опису) різних типів інсайдерів, пропонуються механізми розпізнавання інсайдерів на підставі різнорідної інформації

Ключові слова: інсайдерство, психологічний портрет, інформаційна безпека

В статье рассматривается проблема выявления инсайдеров в организации. Предлагается подход к построению сигнатур (описания) различных типов инсайдеров, предлагаются механизмы распознавания инсайдеров на основании разнородной информации

Ключевые слова: инсайдерство, психологический портрет, информационная безопасность

The report addresses the problem of identification of insiders in the organization. It is approach to the construction of signatures (description) of different types of insiders, and proposed mechanism of recognition of insiders on the basis of heterogeneous information

Key words: insiders, psychological portrait, information security

Постановка проблемы

Обеспечение информационной безопасности организаций (компаний) в настоящее время является одним из необходимых условий их конкурентоспособного существования. Анализ используемых подходов к построению систем управления информационной безопасностью показывает, что основное внимание уделяется физической защите (охрана периметра, организация физического доступа) и программно-технической защите информации (защита от утечки информации по акустическим каналам, ПЭМИН, защита компьютерной сети и т.д.). Однако аналитические исследования показывают, что одной из самых больших проблем в настоящее время являются внутренние угрозы безопасности информации. Так, по данным компании InfoWatch количество утечек информации в результате реализации внутренних угроз может составлять до 50% от общего их объема [1,2]. Согласно исследованию «National Survey on Managing the Insider Threats», результаты которого были опубликованы Ponemon Institute в сентябре 2006 года, средний ежегодный ущерб в результате утечки информации из-за действий инсайдеров (внутренних нарушителей) из расчета на одну опрошенную компанию составляет 3,4 млн. долл. Для сравнения аналогичный показатель потерь вследствие вирусных атак, согласно исследованию «2006 CSI/FBI Computer Crime and Security Survey» [3], составляет менее 70 тыс. долларов. Компания ChoicePoint лишилась из-за кражи персональных данных почти 60 млн. долларов, а правительство США потратило на ликвидацию последствий утечки приватных сведений ветеранов более 500 млн. долларов [4].

Анализ мер по защите информации от инсайдеров, проведенный в российских компаниях показывает [5], что руководство компаний в основном реализует запретительные меры: подписание документов о неразглашении информации (68% компаний), запрещение использования съемных носителей информации (24% компаний), проверка сотрудников на входе и выходе организации (14% компаний). Однако такие мероприятия не могут в полной мере решить данную проблему. Так, например, современный мобильный телефон, который, как правило, разрешено использовать, позволяет инсайдерам как фотографировать документы с конфиденциальной информацией, так и быть переносчиком электронных данных.

Поэтому необходимо разрабатывать комплексные способы борьбы с инсайдерами, которые включают предупреждающие и корректирующие действия.

Целью данной статьи является рассмотрение проблемы борьбы с инсайдерством, разделение их на классы, составление психологического портрета разных типов инсайдеров, а так же рассмотрение методов борьбы с ними.

Основной материал исследования

Одним из наиболее перспективных направлений деятельности в сфере борьбы с инсайдерами является разработка способов комплексной проверки кандидатов при их приеме в организацию, а также в случае необходимости в ходе их служебной деятельности. Необходимо отметить, что в настоящее время такими проверками компании практически не занимаются. Так, при приеме на работу только 4% российских компаний проводит проверку будущих сотрудников на детекторе лжи, а устные беседы проводятся только в 1% компаний [5]. Комплексная проверка кандидатов при приеме на работу может включать не только проверку биографии, трудового стажа, квалификации, но и, например, включать элементы, позволяющие оценить потенциальную возможность попадания кандидата в какую-либо из категорий инсайдеров.

В настоящее время используется следующая классификация видов инсайдеров [6], приведенная в табл. 1.

Механизм комплексного анализа сотрудников для выявления возможности попадания в какую-либо из данных категорий инсайдеров может выглядеть в следующем виде (рис. 1).

Автобиография и объективная информация с места прежней работы позволяет получить развернутую характеристику сотрудника, в том числе и участие в инцидентах ИБ на прежнем месте работы.

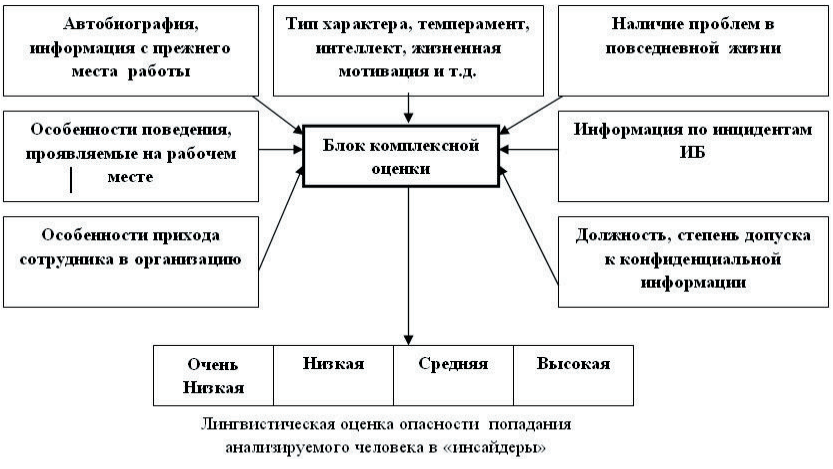

Рис. 1. Механизм комплексного анализа сотрудников при выявлении расположенности к инсайдерству

Таблица 1

Классификация видов инсайдеров

Виды инсайдеров	Краткое описание	Психологический портрет	Мотив
Халатные	Сотрудники, которые по своей халатности допустили нарушение конфиденциальности, целостности или доступности информации (КЦД)	В основном меланхолик, либо флегматик. Люди, которые могут быть не обременены интеллектом и крайне невнимательные	Мотива нет. Старается на благо компании, но из-за своей халатности может допустить нарушение КЦД информации
Манипу-лируемые	Сотрудники, подвергшиеся атакам методами социальной инженерии	Люди со слабым характером, которые легко могут поддаваться влиянию.	Мотива нет. Стараются на благо компании, но из-за неправильного определения этого “блага” могут допустить нарушение КЦД информации
Обиженные	Сотрудники, которые по личным мотивам стремятся нанести вред компании.	В основном холерики. Люди с сильно развитым чувством мести.	Мотив – отомстить. Обида может быть по разным причинам (маленькая заработная плата, недостаточная оценка труда и т.д.).
Нелояльные	Сотрудники, как правило, меняющие место работы и уносящие всю информацию, до которой были доступны.	В основном холерики либо сангвиники. Продуманные люди, всегда пытаются думать на пару ходов вперед. Такие люди постоянно ищут лучшей жизни.	Мотив – получить информацию для дальнейшего использования. Украденная ими информация также может являться гарантом “комфортного увольнения” (выдача хороших рекомендаций, выплата компенсаций).
Завербованные	Сотрудник изначально лояльный, а затем подкупленный либо запуганный.	Люди давно работающие в организации, занимающие должности среднего и высокого уровня.	Нарушают КЦД информации по указанию извне. Основной мотив - деньги, либо выполнение требований шантажиста.
Внедрённые	Сотрудник специально устроенный в организацию для похищения информации.	В основном сангвиники либо холерики. Высоко профессиональные люди, целеустремлённые, коммуникабельные	Стараются получить всю информацию, которую заказал заказчик. Основной мотив - деньги.

Понимание проблем сотрудника в повседневной жизни может выявить такие ситуации, при которых данный сотрудник может попасть в категорию «завербованных» инсайдеров. Так, например, болезнь близкого человека и потребность в материальных средствах для лечения может привести к вербовке сотрудника злоумышленниками.

К особенностям поведения, проявляемым на работе, относятся такие, как взаимоотношения с коллегами, отношение к указаниям руководства, конфликтность, качество выполнения своих служебных обязанностей, недовольство отсутствием повышения и т.д. Это позволяет, в первую очередь, выявлять «обиженных» и «нелояльных» инсайдеров.

Информация по инцидентам ИБ, которые имеют отношение к проверяемому сотруднику, позволяет понять причины совершения инцидента ИБ этим человеком.

При этом необходимо классифицировать инциденты ИБ по степени опасности, поскольку не каждый подобный инцидент может привести к увольнению сотрудника. Такая информация помогает, в первую очередь, выявлять «халатных» и «манипулируемых» инсайдеров.

Особенности прихода данного человека в организацию могут позволить выявить его попадание в наиболее опасную категорию инсайдеров – «внедренные». Здесь может анализироваться такая информация, как при каких условиях попал человек в организацию – почему уволился его предшественник, кто рекомендовал нового сотрудника, как этот человек узнал о вакантном месте и т.д.

Должность (занимаемая или предлагаемая) и степень допуска сотрудника к конфиденциальной информации на этой должности позволяют понять критичность для организации нахождения проверяемого человека на этой должности. На наш взгляд необходимо классифицировать все должности организации с точки зрения их критичности для обеспечения информационной безопасности. И уровень проверки сотрудников, потенциальных и действующих, должен зависеть от критичности их должностей.

Как видно из таблицы каждому из видов инсайдеров могут соответствовать свои психологические особенности личности: тип характера, мотивация, интеллект и другие. Можно говорить о психологических портретах (сигнатурах) инсайдеров, кото-

Таблица 2

Лингвистическая оценка опасности попадания анализируемого человека в «инсайдеры»

Название признака	Лингвистическая шкала			
	Очень низкая	Низкая	Средняя	Высокая
Информация по инцидентам ИБ	В инцидентах ИБ не замечен	В инцидентах ИБ не замечен	Участвовал в некритичных инцидентах БИ	Участвовал в критичных инцидентах БИ
Автобиография, информация с прежнего места работы	Информация положительная	Информация положительная	Были проблемы с обеспечением КЦД информации на прежнем месте работы	Был уволен за нарушение КЦД информации с прежнего места работы или были другие существенные проблемы в данной сфере
Психологический портрет	Положительный	Есть предпосылки	Стойкие предпосылки	Стойкие предпосылки
Особенности поведения, проявляемые на рабочем месте	Поведение положительное	Поведение положительное, высказываются критические замечания по ряду вопросов	Существует неудовлетворение положением дел, бывают серьезные споры с коллегами и руководством, часто проявляется болезненное реагирование на действия других сотрудников и руководства	Нервное реагирования на указания руководства, неповышение по работе, низкую зарплату; получение данным сотрудником информации о возможном сокращении (увольнении)
Особенности прихода сотрудника в организацию	Был приглашен из другой организации после анализа его морально-деловых качеств	Был рекомендован одним из лояльных сотрудников высшего звена организации	Предложил свои услуги самостоятельно, есть возможность достоверной проверки предыдущей деятельности	Предложил свои услуги самостоятельно, нет возможности достоверной проверки предыдущей деятельности
Наличие проблем в повседневной жизни	Существенных проблем нет	Есть проблемы, которые сотрудник решает сам или с помощью родственников (организации)	Есть существенные проблемы, которые сотрудник решает сам	Есть критические проблемы у данного сотрудника
Должность, степень допуска к конфиденциальной информации	Должность не предполагает доступа к критической для организации информации	Должность предполагает возможность доступа к объектам, где находится критическая для организации информация	Должность предполагает работу с информацией, степень критичности для организации средняя	Должность предполагает работу с информацией, степень критичности для организации высокая

рые могут существенно повысить эффективность выявления лиц, предрасположенных к инсайдерской деятельности. Для организаций рекомендуется подключать психологов для создания списка лиц из числа сотрудников, наиболее склонных к инсайдерской деятельности. Подобный список позволит установить контроль за теми, кто с большей степенью вероятности может попасть в инсайдеры. Это позволяет распределить усилия специалистов информационной безопасности между мониторингом действий условно надежных и условно ненадежных сотрудников. Для более успешного составления психологического портрета каждого из сотрудников целесообразно анализировать служебную переписку сотрудников, которая собирается корпоративными системами защиты от утечек данных (DLP-системами). Некоторые системы позволяют вести архив всей перехваченной информации, позволяя существенно повысить качество такой оценки.

Также можно использовать метод “скрытой камеры”. Данный метод заключается в том, что при приёме на работу всё собеседование записывается на скрытую видео камеру без ведома принимаемого. После это запись просматривается психологами и специалистами отдела информационной безопасности. Исходя из таких аспектов, как тембр голоса, жестикуляция, уверенность в себе, реакция на тестовые вопросы и другие признаки составляется его психологический портрет, который увеличивает адекватность принимаемых по данному человеку выводов.

Лингвистическая комплексная оценка опасности попадания анализируемого человека в «инсайдеры» может выглядеть следующим образом (табл. 2).

Количество градаций лингвистической шкалы оценки опасности попадания анализируемого человека в «инсайдеры» может быть и другое (например, низкое, среднее, высокое). Уменьшение количества таких градаций приводит к более их простому описанию, увеличение таких градаций увеличивает точность оценки. При этом, если одни из признаков принимает значение «средний» и «высокий» уровень опасности (например, происходит увольнение сотрудника или у сотрудника критические проблемы в семье), то принимается аналогичное общее решение.

Это дает возможность специалистам по информационной безопасности принять ряд регулирующих или запретительных мер по отношению к данному сотруднику.

Выводы

На данный момент человеческий фактор является одним из критических в системе защиты информации. Именно люди становятся самым большой уязвимостью любой информационной системы. Зачастую инсайдерами являются сотрудники, ответственные если не за защиту конфиденциальных сведений, то, как минимум, за сохранение конфиденциальности информации. По незнанию или рассеянности, со злым умыслом или без него, но именно они могут приносить значительный вред своим работодателям.

Пока не существует единого лекарства от болезни под названием “инсайдер”. Но предлагаемый комплекс мероприятий по своевременному выявлению сотрудников, предрасположенных к инсайдерской деятельности может значительно снизить возможность нарушения конфиденциальности, целостности и доступности информации в организации.

Литература

1. Ульянов В.В. Динамика безопасности: от внешних угроз – к внутренним / В.В.Ульянов // Защита информации. INSIDE. – 2008. - № 4. – С. 34 – 38.
2. Глобальное исследование утечек за 2010 год. [Электронный ресурс] Аналитические отчеты компании InfoWatch. - Режим доступа: URL: http://www.infowatch.ru/analytics.html. - 12.03.2011г - Загл. с экрана.
3. Классификация инсайдерских угроз: вероятные сценарии [Электронный ресурс] / Исследование компании ТехноСвязь. – Режим доступа: URL: http://www.comkas.ru/tech/ins2.html. - 10.03.2011г. - Загл. с экрана.
4. Классификация инсайдерских угроз [Электронный ресурс] / CNew. Интеграция. – Режим доступа: URL: http://corp.cnews.ru/reviews/free/insiders2006/articles/classification.shtml. - 07.03.2011г. - Загл. с экрана.
5. За перепиской сотрудников следят в трети российских компаний [Электронный ресурс] / Журнал Information Security. – Режим доступа: URL: http://www.itsec.ru/keywords.php?keyword=6133. - 07.02.2011г. - Загл. с экрана.
6. Скиба В.Ю. Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.