маркетинговых политиках компании-производителей и интеграторов промышленных решений, а также специфика работы и адаптации к условиям законодательства Российской Федерации в области защиты информации накладывают на предполагаемые к внедрению решения целый ряд ограничений. Устранение этих недостатков является совместной задачей экспертов по информационной безопасности, представителей ИТ-блока и бизнес-подразделений.

СПИСОК ЛИТЕРАТУРЫ:

1. *Курило А. П. [и др.]*. Обеспечение информационной безопасности бизнеса. М, 2005. — 512 с.
2. Стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
3. Информационная безопасность компьютерных систем с сетей: учебное пособие М., 2008. — 416 с.

А. К. Плешков
Московский инженерно-физический институт (государственный университет)

ФАКТОРЫ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ

В статье рассмотрен термин «инсайдер» (внутренний нарушитель политики информационной безопасности). Предложены к обсуждению внешние и внутренние факторы, способные оказать влияние на изменению уровня «инсайдерской» деятельности в кредитно-финансовой организации Российской Федерации. Продемонстрирован подход к рассмотрению терминов «инсайдер» и «внутренний нарушитель» в контексте основных положений стандарта Банка России СТО БР ИББС-1.0-2006.

За последнее время в лексиконе экспертов по информационной безопасности появилось и укрепилось огромное число новых, ранее неиспользуемых терминов, определяющих субъекты и объекты отношений различного рода, а также действия в отношении каждого из участников: «фишинг» (от англ. — «phishing» — разновидность атак класса «социальной инженерии»), «фрод» (от англ. — «fraud» — мошенничество), «дефейс» (от англ. «deface» — разбор интерфейса на составные части), «досить» (от англ. «Denail of Service» — отказ в обслуживании) и т. д. Особое место в словаре занимает термин «инсайдер» (от англ. «insider» — кто-либо работающий внутри).

Рассмотрим последний термин более подробно применительно к обеспечению информационной безопасности в кредитно-финансовых организациях Российской Федерации.

В сфере торговли ценными бумагами существует следующее частное определение: «инсайдер» — лицо, имеющее доступ к внутренней информации организации в силу: своего служебного положения; договора с организацией, выполнения государственных контрольных функций или иной профессиональной деятельности; а также родственных и иных связей с другим лицом, располагающим такой информацией.

В соответствии с федеральным законом «О рынке ценных бумаг» в редакции 1996 года к «инсайдерам» — лицам, располагающим служебной информацией, — относятся: члены органов управления или профессионального участника рынка ценных бумаг, связанного с этим эмитентом договором; физические лица — профессиональные участники рынка ценных бумаг; аудиторы; служащие государственных органов, имеющие в силу контрольных, надзорных и иных полномочий доступ к

служебной информации. Эти лица не имеют права использовать служебную информацию для заключения сделок, а также передавать ее третьим лицам. Как следствие, «инсайдеры» могут быть первичными (непосредственными, поддерживающими прямую связь с организацией) и вторичными (получающими внутреннюю информацию от первичных).

В области информационной безопасности термин «инсайдер» имеет другое значение. Чаще всего он рассматривается в контексте составления модели потенциального нарушителя информационной безопасности — внутреннего нарушителя: *«инсайдер» — это сотрудник, имеющий договорные отношения с организацией, который сознательно способствует или осуществляет утечку информации для своей выгоды и во вред работодателю. Под утечкой информации будем понимать* утрату информацией свойства конфиденциальности в результате несанкционированного ознакомления с нею, несанкционированного документирования (снятия копий) или неконтролируемого распространение информации, которое привело (может привести) к ее несанкционированному получению третьими лицами.

Разница изложенных выше определений понятна. Один и тот же сотрудник организации в типовой ситуации может подпадать под действие сразу двух указанных определений. К примеру, высокопоставленный руководитель сообщил за ланчем брокеру фондового рынка о планируемых изменениях в организационно-штатной структуре организации, что привело к существенному колебанию и/или резкому снижению общего курса акций компании на рынке ценных бумаг. С точки зрения брокера, руководитель — «инсайдер», обладающий проверенной и гарантировано верной информацией. С точки зрения подразделения в организации, ответственного за обеспечение информационной безопасности, руководитель — внутренний нарушитель, действия которого повлекли за собой нанесение вреда организации [1].

По материалам аналитических исследований компании «Infowatch» (www.infowatch.ru), за период с 2004 по 2008 год наблюдается динамика роста количества инцидентов по нарушению информационной безопасности собственными сотрудниками организации по отношению к числу «внешних» инцидентов в кредитно-финансовых организация РФ. В настоящее время внешние инциденты составляют около 35%, внешние — около 65%.

Что провоцирует сотрудников кредитно-финансовых организаций становиться «инсайдерами»? Рассмотрим различные категории внешних и внутренних для финансового института факторов, способствующих изменению уровня «инсайдерской» деятельности [2]:

К первой (основной) категории относятся факторы, связанные с активной деятельностью «инсайдера» в организации. К данной категории относятся:

· прогнозирование, подготовки, использование «инсайдером» нештатной или аварийной ситуации с целью возможного нарушения конфиденциальности и целостности обрабатываемой информации;

· использование неопределенностей, возникающих в нештатных и аварийных ситуациях, в своих интересах;

· преодоление «инсайдером» защитных барьерных мер, в том числе превышение выданных полномочий путем использования технических и организационных мер;

· подготовка и умышленное внедрение в автоматизированных системах, технологических и бизнес процессах уязвимостей (потенциальных закладок), которые планируется использовать в дальнейшем;

· исследование злоумышленником системы защиты с целью выявления границ ее возможностей, тестирование активными инструментами, сохраняющими анонимность;

· поиск злоумышленником в границах охраняемой зоны неиспользуемых (бесконтрольных) информационных активов и ИТ-ресурсов, а также проверка возможностей использования без обратной связи со стороны подразделений, ответственных за обеспечение информационной безопасности;

· активное противодействие расследования инцидентов нарушения информационной безопасности, в том числе саботаж, укрывание прямых улик и доказательств, задержки, обусловленные организационно — бюрократическими процедурами;

· использование «инсайдером» полномочий и/или знаний других сотрудников в рамках служебных или неформальных отношений, в том числе применение социальной инженерии с целью получения необходимого объема данных и/или уровня доступа к ранее закрытым сегментам информации;
· активные действия сотрудников по повышению собственных полномочий как техническими, так и организационными мерами;
· изучение технической документации системы исходных кодов программно-технических средств;
· действие организованной группы «инсайдеров» внутри организации;
· исследование автоматизированных систем и технологических процессов работы с целью определения и выявления основных алгоритмических и технологических уязвимостей для дальнейшего активного использования в части осуществления неконтролируемого несанкционированного доступа к обрабатываемой информации;
· активное противодействие процедурам и инструментам регистрации событий и/или работе подсистемы протоколирования (журналирования) действий пользователей в автоматизированных системах;
· несанкционированная установка нештатных программно-аппаратных средств получения, предоставления, контроля доступа на автоматизированном рабочем месте и/или серверной операционной платформе;
· активные действия «инсайдеров», направленные на изменение прав доступа и наделенных ролей в автоматизированных системах;
· использование собственных полномочий за пределами минимально необходимых для реализации служебных задач (использование избыточных прав, злоупотребление выданными полномочиями, использование прав отличное от порядка, представленного в инструкции по эксплуатации);
· поддержка несанкционированных действий из вне организации, в том числе активная работа «инсайдера» (внутреннего злоумышленника) в совокупности с внешними злоумышленниками;
· осуществление распределенных атак, отвлечение внимание и ресурсов системы защиты на другие менее значимые объекты;
· скрытие от средств активного мониторинга (запутывания) путем переноса активов между различными областями регистрации событий в рамках штатных полномочий.

Ко второй категории относятся факторы, способные оказать влияние на мотивацию действий «инсайдера», в том числе:
· создание в коллективе (в организации) «социальной среды», располагающей к нарушению установленных правил политики информационной безопасности (отсутствие утвержденной политики информационной безопасности) и/или к пренебрежению мерами защиты;
· экономические факторы, в том числе неудовлетворенность сотрудников заработной платой;
· наличие индивидуальных особенностей менталитета сотрудников, в том числе существование социальных проблем за пределами организации;
· конфликт интересов в коллективе;
· приближенность сотрудников к финансовой информации и операциям с материальными средствам;
· воздействие на сотрудников со стороны внешних источников угрозы для реализации собственных целей и задач.

В третьей категории собраны факторы, способные оказать усиливающее воздействие на позиции, содержащиеся в первых двух категориях. К ним относятся:
· ошибки персонала организации, приводящие к реализации рисковых событий, в том числе реализация рисков, связанных с нарушениями политики информационной безопасности в организациях;
· сложность построения ИТ-ландшафта и/или ИТ-инфраструктуры в целом;
· возможность организованной работы представителей различных направлений (сотрудников одной организации) для достижения поставленной цели;
· конфликт интересов между различными подразделениями при осуществлении регламентированных взаимодействий, в том числе в части касающейся информационной безопасности (мониторинг, проведение служебных расследований);

· несогласованность различных защитных мер в части организации и применения барьерных средств, менеджмента активов, менеджмента инцидентов, мониторинга и регистрации событий в автоматизированных системах.

К четвертой категории относятся факторы прямого действия, наличие которых обусловлено существование регламентов и порядков взаимодействия подразделений в организации:

· нечеткая реализация разграничения доступа и выделения ролей на различных уровнях;

· наличие возможностей для скрытия реальной цели действий субъектов по отношению к объектам доступа;

· риски неустановления причин и обстоятельств возникновения инцидентов, в том числе фактов нарушения политики информационной безопасности;

· концентрация (накапливание) прав доступа субъектами к объектам на протяжении работы в организации в рамках исполняемых должностных обязанностей;

· концентрация (накапливание) знаний у одного субъекта в части касающейся практики работы с различными информационными автоматизированными системами, обрабатывающими информацию;

· сложность своевременного (предварительного) обнаружения характерных признаков подготовки или проведения атак разного уровня и/или оповещения сотрудников подразделения, ответственного за обеспечение информационной безопасности, о готовящихся действиях в отношении защищаемых объектов;

· невозможность адекватного наказания выявленного нарушения;

· в распоряжении «инсайдера» всегда находятся ИТ-ресурсы, доступ к которым предоставляется в соответствии с выполняемыми сотрудником обязанностями.

После детального рассмотрения категорий факторов, способных оказывать влияние на изменение уровня инсайдерской деятельности, возникает сомнение в правомерности классического тождества между терминами «внутренний нарушитель» и «инсайдер».

Под *«инсайдером»* предлагается понимать *потенциального* нарушителя информационной безопасности — лицо (или группу лиц), обладающее служебными полномочиями в отношении ИТ-ресурсов и/или знаниями особенностей организационно-технической среды (инфраструктуры), способными использовать их нежелательным для организации образом. Тогда как под термином *«внутренний нарушитель»* предлагается понимать лицо (или группу лиц), которое *планирует, совершает или совершило* с использованием своих служебных полномочий заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно и могло предвидеть возможность наступления этих последствий.

$$«Инсайдер» \in «Внутренний\ нарушитель»$$
$$«Внутренний\ нарушитель» \notin «Инсайдер»$$

В связи с этим становится понятным, что для любого подразделения, ответственного за обеспечение информационной безопасности, не достаточно применение только организационных или только технических мер защиты. Подход должен быть комплексным, учитывающим, помимо технических, организационные, правовые, социальные, экономические аспекты работы сотрудников в кредитно-финансовых институтах. При этом необходимо соблюдать четкий баланс между требованиями по информационной безопасности и требованиями бизнеса, что очень часто является основной проблемой для правильной организации системы менеджмента информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. *Курило А. П. [и др.]*. Обеспечение информационной безопасности бизнеса. М., 2005. — 512 с;

2. Стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».