С. И. Журин

ИНСАЙДЕР: ОСНОВНАЯ ХАРАКТЕРИСТИКА И КОМПЛЕКСНОСТЬ ПРОТИВОДЕЙСТВИЯ

Обеспечение защиты информации в настоящее время приобретает все более актуальный характер. Электронный способ хранения информации, использование электронных платежей, управление различными технологическими процессами с использованием программного обеспечения и компьютерные системы безопасности объекта повышают опасность использования информации для нанесения ущерба как на уровне предприятия, так и на уровне государства.

По статистике МВД, зарубежной информации, количество случаев взлома информационных систем, хищения электронных денег и информации (в основном с участием сотрудников предприятий) ежегодно возрастает в два-три раза. Объемы ежегодных потерь от таких инсайдерских действий исчисляются миллиардами долларов и, соответственно, ежегодно возрастают.

Одним из наиболее сложных вариантов инсайдерской угрозы является сговор сотрудников. При этом происходит увеличение количества должностных полномочий у нарушителя, что позволяет совершить беспрепятственно акцию хищения электронных денег или важной информации.

Для противодействия инсайдерской угрозе на предприятиях необходима комплексная защита, начиная от психологии поведения потенциальных инсайдеров и формирования их преступного правосознания и заканчивая организационно-техническими средствами защиты информации.

1. Основные параметры инсайдера

В настоящее время существует много разных определений инсайдера. Введем обобщенное определение инсайдера и несколько других основных определений, которые будут использоваться в статье.

Инсайдер — лицо, имеющее право доступа на территорию охраняемого объекта (или в информационную область) без сопровождения и совершающее несанкционированное действие.

Инсайдерское правонарушение — действие или совокупность действий инсайдера или инсайдеров, приводящих к прямому или косвенному ущербу для объекта.

Несанкционированное действие — несанкционированное службами объекта совершение или попытка совершения:

- хищения охраняемых предметов,
- копирования, изменения, удаления охраняемой информации,
- информационного доступа к охраняемой информации,
- выноса носителей с охраняемой информацией,
- вывода из строя или нарушения функционирования различных информационных систем.

Основные параметры инсайдерского правонарушения

Инсайдерские правонарушения (преступления) можно проклассифицировать по следующим характерным направлениям (с точки зрения основных параметров расследования преступления):

по виду предмета интересов для хищения/воздействия:

- информация,
- носимый (транспортабельный) предмет,
- сложная техническая установка, информационное воздействие на которую может привести к значительным потерям,
- информационная система с важной информацией,

– информационная система управления системой безопасности,
– сотрудник;

по качественному составу инсайдеров:

– одиночный,
– группа инсайдеров,
– одиночный в сговоре с внешним,
– группа инсайдеров в сговоре с внешним;

по осознанности действий:

– преднамеренные (полностью осознаваемые),
– халатные, хулиганские (частично осознаваемые),
– неосознанные;

по типу инсайдера:

– внедренный агент,
– бывший преступник,
– сотрудник с психическими аномалиями,
– сотрудник, получивший психические аномалии во время работы,
– сотрудник, поменявший свое правосознание во время работы;

по мотиву совершения:

– получение личной выгоды,
– интерес (кража информации с целью посмотреть, взломать),
– равнодушие,
– желание мести,
– действия под принуждением,
– идеологический (политический),
– самореализация, повышение адреналина;

по должностным возможностям:

– без возможности доступа к объекту интересов (ОИ),
– с периодической/постоянной возможностью доступа к ОИ без надзора / под надзором,
– обеспечивающий управление доступом к ОИ,
– разрабатывающий систему управления доступом к ОИ;

по обнаружению после совершения или по факту подготовки:

– мгновенно,
– по факту случайного восприятия, доступа,
– по факту очередного контроля,
– по факту расследования,
– никогда;

по степени наказания/воздействия при обнаружении:

– подпадающие под статью Уголовного кодекса,
– подпадающие под административное наказание на объекте,
– подпадающие под общественное порицание.

Опасность инсайдерской угрозы

Опасность инсайдерской угрозы состоит в том, что сотрудник предприятия в отличие от внешнего нарушителя обладает следующими характеристиками:

– знания и должностные полномочия,
– связи и возможность получения информации от других сотрудников,

– возможность ожидания наиболее «удобного» (известного и ожидаемого) момента совершения: профилактические работы, временное делегирование больших полномочий и др.,

– бóльшая возможность вступления в сговор с другими сотрудниками с «недостающими» для акции должностными полномочиями.

При этом всегда имеется много групп сотрудников, которые могут совершить любое преступление исходя из совокупности их должностных полномочий.

Однако стоит отметить, что совершение преступления может произойти только при наличии трех условий:

– насущная необходимость,

– психологическая готовность,

– возможность безуликового совершения.

При этом отсутствие хотя бы одного из этих условий приводит к невозможности совершения преступления. В понятие возможность совершения зачастую входит еще и возможность реализации похищенного, обналичивания электронных средств и т. п.

2. Противодействие инсайдерской угрозе

Противодействие инсайду на уровне предприятия в целом обеспечивается на следующих 3 основных уровнях:

1. Прием на работу: предупреждение трудоустройства:

– внедряемого агента,

– сотрудника, который может стать инсайдером в силу своих психологических или других характеристик вследствие:

- обстоятельств на работе (снижение зарплаты, ухудшение отношений/условий, снижение уровня безопасности),

- личных обстоятельств (долги, болезни, семейные проблемы, юридические проблемы).

При этом проводится комплексная проверка сотрудника с применением: психологических тестов, полиграфа, баз данных, информации с предыдущих мест работы, собеседования и др. и с учетом результатов комплексного анализа всей информации.

2. В процессе работы [1]:

Исходя из практики предложить следующий вариант системы защиты от инсайдерской угрозы в процессе работы:

1. Создание условий невозможности совершения преступления:

– информационно (система организационно-технических мер по защите информации),

– физически (система физической защиты),

– психологически (система управления персоналом — работа с персоналом по формированию высокой культуры правосознания и мотивации к работе),

– организационно (система разграничения полномочий, контроля, ответственности, наказаний),

– юридически (система юридической защиты — наличие системы санкций за неразрешенные действия и система наказания),

– технологически (система защиты от аварий).

2. Создание системы мониторинга информации о сотрудниках, прогнозирования совершения преступлений и их раскрытия.

3. Создание системы работы с сотрудниками с проблемами по психологической и должностной коррекции.

4. Создание системы аудита по выполнению правил внутри предприятия и поиску слабых мест и их устранению (по п. 1–3).

5. Наличие системы внешнего аудита (Прокуратура, Ростехнадзор, ФСБ и т. д.).

3. При увольнении:

– анализ знаний, возможно похищенной информации, которыми владеет сотрудник, сферы дальнейшей работы,

– корректирование защищенности предметов защиты на основе анализа увольняемых сотрудников,

– работа с увольняемыми и уволенными сотрудниками, наблюдение.

Элементы противодействия инсайду в процессе работы

Система физической защиты (СФЗ)

СФЗ дает невозможность совершения акции инсайда за счет:

– невозможности визуального получения информации за границей, куда сотрудник не допущен,

– наличия барьеров, препятствующих физическому проникновению в неразрешенную зону,

– отказа в допуске при попытке пройти в неразрешенную зону,

– обнаружения нарушителя и его задержания,

– контроля местоположения предмета защиты.

Основу физической защиты составляют:

– комплекс инженерно-технических средств охраны,

– силы охраны.

Система информационной защиты

Система информационной защиты (СИЗ) дает невозможность совершения акции инсайда за счет:

– невозможности получения информации о системах защиты и защищаемых документах, их расположения,

– наличия информационных барьеров, препятствующих информационному проникновению в неразрешенную зону,

– информационного обнаружения, его блокировки и информационного контроля местоположения нарушителя.

К основным элементам СИЗ относятся:

– программно-аппаратные комплексы контроля доступа;

– средства шифрования информации;

– средства антивирусной защиты;

– средства межсетевого экранирования;

– средства разграничения доступа;

– инструментальные средства администратора безопасности;

– средства видеонаблюдения;

– средства защиты от сбоев электропитания;

– фильтры почтовых серверов и активности на рабочих станциях.

Организационная и психологическая защита

Организационные и психологические меры в достаточной степени переплетены, так как все они формируют желание несовершения преступления.

Система управления персоналом в части предупреждения инсайда предназначена для формирования [2,3]:

– интереса и желания работать (устремленность к достижению целей: роста, выполнения интересной и/или прибыльной работы),

– удовлетворенности работой (получения справедливого вознаграждения (по сумме льгот: зарплата, привилегии, льготы, поблажки, перспективы, хороший коллектив, близость к дому и т. д.) за выполняемую работу),

– осознания неотвратимости наказания.

Такая система формируется наличием следующих направлений:

1. Нормативная регламентация внутри организации и доведение ее до сотрудников, а также обучение знанию законов и различных нормативных актов;

2. Четкая система наказаний. Любой сотрудник должен знать, как и за что его наказывают;

3. Работа с сотрудниками, совершившими проступки, и работа с увольняемыми сотрудниками;

4. Разграничение полномочий и исключение делегирования большого количества полномочий, что снижает вероятность возникновения преступного замысла;

5. Контроль исполнения полномочий;

6. Поддержка. В случае, когда работнику нравится его место, он будет тщательнее следить за соблюдением правил. Нельзя забывать о материальной помощи в трудных ситуациях, о психологическом климате в организации, о поощрениях: премии, льготные кредиты, путевки;

7. Наличие единой политики компании, направленной на формирование корпоративного сознания и далее поведения. При этом сотрудник должен стать составной частью компании;

8. Наличие системы повышения профессионального уровня, карьерного роста.

Юридическая защита

Юридическая защита формирует представление сотрудника о возможном наказании при совершении тех или иных противоправных действий и пересекается с организационной системой в части наказаний за несоблюдение лояльности.

При трудоустройстве сотрудник подписывает контракт (приложение к контракту), в котором он знакомится и соглашается (подписывает) с действующими ограничениями, а также с видами наказаний за них.

Незначительные проступки сотрудника декомпенсируются различными наказаниями в рамках системы управления персоналом или системы работы с сотрудниками.

При совершении преступлений, предусмотренных УК РФ, наказание назначает государственная система наказания. Наличие УК РФ оказывает наиболее сильное сдерживающее воздействие на сознание потенциального инсайдера по сравнению с угрозой увольнения или общественного порицания.

Система технологического контроля

Система технологического контроля за сложной технической установкой (реактор, нефтеперерабатывающий завод и т. п.) обеспечивает стабильность протекающего процесса (химического, ядерного, технического и т. д.) при заданных возможных отклонениях и проектных (запланированных) авариях.

Также в таких системах при выходе одного или нескольких критических элементов из строя, ошибках в управлении срабатывают системы аварийной защиты или аппаратной коррекции (например, клапаны, уменьшающие избыточное давление).

Нарушитель может перепрограммировать системы принятия решений о срабатывании тех или иных устройств, механически их заблокировать. Для предупреждения этого необходим периодический контроль.

Полнота защиты

Рассмотренные системы защиты не являются отдельными компонентами и тесно переплетены. На рис. 1 приведено пересечение систем защит [1].

Данные системы бывают отделены друг от друга: на предприятии могут быть не определены требования лояльности, за информационную и физическую защиту могут отвечать разные подразделения, и они могут быть сформированы независимо.

Наибольшие «дырки» в защите обычно возникают на стыке систем. Например, организационная система явно не учитывает неблагонадежность, физическая защита может отключаться при некоторых технологических действиях, или организационная (информационная) система может не учесть, что бывший сотрудник, укравший секреты, не несет юридическую ответственность. Поэтому на этапе создания (проектирования) систем защиты необходимо учесть взаимосвязи систем на документальном, физическом, информационном и психологическом уровнях взаимодействия.

Рис. 1. Пересечение систем защит

Система мониторинга информации о сотрудниках

После приема сотрудника на работу необходимо проводить его периодические проверки. Жизненная проверка происходит постоянно, неформально в процессе работы, однако не всегда подчиненные, сотрудники, руководитель обращают должное внимание на поступки, особенно если сотрудник пытается их скрыть.

Для обеспечения оценки состояния сотрудников на предприятии может быть внедрена система мониторинга их состояния, состоящая из:

– источников информации,

– системы сбора, обработки и анализа информации из источников,

– системы принятия решений по работе с сотрудниками,

– системы профилактической работы с сотрудниками, которые могут стать инсайдерами или совершили противоправные поступки.

Система внутреннего аудита

Система внутреннего аудита является одной из основных форм проверки работы сотрудников и их коллективов. Постоянный «легкий» аудит обычно проводится непосредственным начальником как факт контроля выполнения работы. В большинстве случаев «комиссионный» внутренний аудит если и проводится, то формально и зачастую перед предстоящим внешним аудитом.

Во многих случаях сотрудники отдела аудита, не желая портить отношения с коллегами, проводят аудит достаточно мягко, документально не оформляя результаты значительных нарушений. Однако аудит проводится «мягко», если невыполнение другими не приводит к проблемам для них самих, например, если материально ответственный не находит у другого сотрудника какого-либо прибора.

Аудит проводят по различным направлениям:

– инвентаризация — физическое наличие учитываемых материальных ценностей,

– соблюдение требований нормативных документов, например правил физической защиты,

– финансовый аудит — наличие документального подтверждения корректности потраченных средств,

– информационный аудит,

– другие направления.

Основной причиной совершения противоправного действия является наличие мотивов и возможности совершения. И если возможность совершения еще можно предупредить, сформировав мощнейший барьер из пяти уровней защиты (информационной, физической, юридической, технологической, организационной), то выявление возможных мотивов является вторжением в личную жизнь сотрудника и требует значительных затрат.

Формирование пяти уровней высокой защиты также требует значительных затрат и во многих случаях организуется не в полной мере, например в условиях современного кризиса и введения политики экономии. Конечно, «общие слова», что необходимо вкладывать в систему защиту, что она себя «окупает», хороши, но в условиях реальной жизнедеятельности многие идут на значительное сокращение служб безопасности и сил охраны, что естественно снижает защищенность.

В целом, защита от возможных инсайдерских правонарушений должна проводиться комплексно. При хорошей системе защиты незначительные недочеты компенсируются остальными элементами системы. И даже при временных значительных ухудшениях сотрудники ведут себя благонадежно по инерции. Однако при длительных ухудшениях механизм правосознания может нарушиться. Поэтому вложения в систему противодействия внутренней угрозе должны быть постоянны, планомерны, привычны и не должны сильно мешать работе. Резкие и нечастые проверки полезны, однако нарушают установленный ход работы и несколько снижают работоспособность предприятия. Поэтому гораздо важнее создать климат доверия, высокой надежности, лояльности, профессионализма и его поддерживать.

В целом, для обеспечения «оптимальной» защиты от внутренней угрозы необходимо:

1. определить защищаемые объекты,

2. составить возможные модели нарушителей с участием сотрудников исходя из важности защищаемых объектов,

3. определить возможность обнаружения и противодействия данных моделей существующими элементами действующей системы безопасности (ДСБ),

4. оценить варианты модернизации ДСБ, позволяющие полностью противодействовать выбранным моделям нарушителя,

5. при наличии «слишком дорогих» вариантов снизить требования к моделям нарушителей и заново выполнить п. 3, 4, 5.

СПИСОК ЛИТЕРАТУРЫ:

1. *Журин С. И.* Автоматизированная система предупреждения совершения преступлений как составная часть системы безопасности важного государственного объекта (Диссертация на соискание ученой степени кандидата технических наук). М.: МИФИ, 2000. – 130 с.
2. *Кудрявцев Б. Н.* Генезис преступления. М.: «Инфра-М», 1998. – 214 с.
3. *Харский К. В.* Лояльность и благонадежность персонала. СПб., 2003.