Модель нарушителя, возможные пути и способы его проникновения на охраняемый объект

Характеристика нарушителя, степень его подготовки и оснащенности, общие рекомендации по применению технических способов защиты

Как показывает опыт работы, нормальное безущербное функционирование системы защиты возможно при комплексном использовании всех видов защиты и четко спланированных действиях сил службы охраны по сигналам, получаемым от технических средств охранной сигнализации.

Охрана учреждения, как правило, является достаточно дорогостоящим мероприятием, поэтому при выборе уровня защиты целесообразно оценить возможные потери от "беспрепятственного" действия нарушителя и сравнить их с затратами на организацию охраны. Этот показатель является индивидуальным для каждого объекта и может быть оценен, как правило, весьма приближенно. Практика создания и эксплуатации комплексов технических средств охранной сигнализации показала, что в большинстве случаев для построения эффективной охраны требуется наличие комбинированных ТСОС, учитывающих возможность дублирования функций обнаружения на основе использования различных физических принципов действия средств обнаружения.

В основе эффективного противодействия угрозе проникновения нарушителя в охраняемые помещения лежит проведение априорных оценок:

- приоритетов в системе защиты;

- путей возможного проникновения нарушителей;

- информации, которой может располагать нарушитель об организации системы защиты предприятия;

- технических возможностей нарушителя и т.д., т.е. оценок совокупности количественных и качественных характеристик вероятного нарушителя.

Такая совокупность полученных оценок называется "моделью" нарушителя. Эта модель, наряду с категорией объекта, служит основой для выбора методов организации охраны объекта, определяет сложность и скрытность применяемых технических средств охранной сигнализации и телевизионного наблюдения, варианты инженерно-технической защиты, кадровый состав службы охраны и т.д.

По уровню подготовки и технической оснащенности "нарушителя" условно можно разделить на следующие типы:

- случайные;

- неподготовленные;

- подготовленные;

- обладающие специальной подготовкой и оснащенные специальными средствами обхода;

- сотрудники предприятия.

Наиболее распространенной "моделью" нарушителя является "неподготовленный нарушитель", т.е. человек, пытающийся проникнуть на охраняемый объект, надеясь на удачу, свою осторожность, опыт или случайно ставший обладателем конфиденциальной информации об особенностях охраны. "Неподготовленный нарушитель" не располагает специальными инструментами для проникновения в закрытые помещения и тем более техническими средствами для обхода охранной сигнализации. Для защиты от "неподготовленного нарушителя" часто оказывается достаточным оборудование объекта простейшими средствами охранной сигнализации и организация службы невооруженной охраны.

Более сложная "модель" нарушителя предполагает осуществление им целенаправленных действий, например, проникновение в охраняемые помещения с целью захвата материальных ценностей или получения информации. Для крупного учреждения наиболее вероятной "моделью" является хорошо подготовленный нарушитель, возможно действующий в сговоре с сотрудником или охранником. При этом возможны такие варианты проникновения, как:

- негласное проникновение одиночного постороннего нарушителя с целью кражи ценностей, для установки специальной аппаратуры или для съема информации;

- негласное проникновение нарушителя-сотрудника предприятия с целью доступа к закрытой информации;

- проникновение группы нарушителей в охраняемые помещения в нерабочее время путем разрушения инженерной защиты объекта и обхода средств охранной сигнализации;

- проникновение одного или группы вооруженных нарушителей под видом посетителей с целью силового захвата ценностей;

- вооруженное нападение на объект с целью захвата заложников, ценностей, получения важной информации или организации собственного управления.

Очевидно, "модель" нарушителя может предполагать и сразу несколько вариантов исполнения целей проникновения на 00.

Среди путей негласного проникновения нарушителя прежде всего могут быть естественные проемы в помещениях: двери, окна, канализационные коммуникации, кроме того непрочные, легко поддающиеся разрушению стены, полы, потолки. Поэтому при организации охранной сигнализации в охраняемом помещении в первую очередь должны быть установлены средства обнаружения для защиты окон и дверей. Обнаружение проникновения через стены, полы и потолки выполняют, как правило, СО, предназначенные для защиты объема помещения. Для усиления защиты окон и дверей широко используются металлические решетки и защитные жалюзи. Установка достаточно надежных решеток на окна может иногда позволить отказаться от установки на них средств охранной сигнализации. Однако часто наблюдалось, что неправильная конструкция решеток открывает дополнительные возможности для проникновения в здание. Например, защищая окна первого этажа, решетки могут облегчить доступ к окнам второго этажа.

Возможность проникновения на объект вооруженных нарушителей требует не только усиления вооруженной охраны, но и установки на входах обнаружителей оружия, оборудование особо ответственных рабочих мест сотрудников кнопками и педалями тревожного оповещения, а в ряде случаев и установки скрытых телекамер для наблюдения за работой сотрудников. Входы в хранилища ценностей должны оборудоваться специальными сейфовыми дверями с дистанционно управляемыми замками и переговорными устройствами.

Уровни технической оснащенности нарушителя и его знаний о физических принципах работы СО, установленных на объекте, определяют возможность и время, необходимое ему на преодоление средств инженерной защиты и обход сигнализационной техники. Наиболее эффективны СО, физический принцип действия и способ обхода которых нарушитель не знает. В этом случае вероятность его обнаружения приближается к единице.

В конечном счете, поскольку задачей системы охраны является оказание противодействий нарушителю в достижении его целей, при построении системы охраны в ее структуру закладывается принцип создания последовательных рубежей на пути движения нарушителя. Угроза проникновения обнаруживается на каждом рубеже и ее распространению создается соответствующая преграда. Такие рубежи располагаются последовательно от прилегающей к зданию территории до охраняемого помещения, сейфа. Эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по минимальному значению времени, которое нарушитель затратит на преодоление всех зон безопасности. За это время, с вероятностью близкой к 1, должна сработать система охранной сигнализации. Сотрудники охраны установят причину тревоги и примут необходимые меры.

Если "модель" нарушителя рассматривает негласное проникновение в охраняемое помещение нарушителя-сотрудника, в состав средств охранной сигнализации необходимо включить устройства документирования работы средств обнаружения, чтобы фиксировать несанкционированные отключения каналов сигнализации. Обычно указывается время постановки и снятия с охраны помещения. Аппаратура документирования должна устанавливаться в специальном помещении, куда имеют доступ только начальник охраны или ответственный сотрудник службы безопасности.

Итак, сложность системы охраны, ее насыщенность средствами инженерной и технической защиты определяются "моделью" нарушителя, категорией и особенностями объекта охраны. Количество необходимых зон безопасности определяется, исходя из состава материальных и информационных ценностей, а также специфических особенностей самого объекта. Если объект расположен в здании с прилегающей к нему территорией, то ограждение и периметральная охранная сигнализация образуют первую зону безопасности объекта. Последней зоной безопасности, например сейфовой комнаты, будет специальный сейф с кодовым запирающим устройством и сигнализационным средством, передающим информацию о попытках его вскрытия.

Очевидно, что для разработки "модели" нарушителя применительно к некоторому 00 необходимо обобщение большого опыта как отечественной, так и зарубежной практики построения систем охраны объектов, аналогичных рассматриваемому. С течением времени "модель" нарушителя, а следовательно, и вся концепция охраны могут меняться. Отсюда следует вывод о необходимости периодического дополнения концепции охраны объекта, обновления системы инженерной защиты, системы охранной сигнализации, телевизионного наблюдения, системы контроля доступа и всех иных систем, рассматриваемых системной концепцией обеспечения безопасности.

Способы получения "нарушителем" информации об объекте и технических способах защиты объекта, вероятные пути проникновения

Целями "нарушителя" или "нарушителей", проникающих на объект, как отмечалось выше, могут быть: кража материальных и/или информационных ценностей, установка закладных устройств, разрушение объекта, захват заложников, а возможно и захват управления функционированием объекта. Злоумышленник будет искать наиболее оптимальные пути проникновения в нужное ему помещение для осуществления поставленной противозаконной цели, будет стараться оставить как можно меньше следов своих действий, разрушений. С этой целью он будет изучать обстановку на объекте, алгоритм охраны, неохраняемые переходы, помещения, способы и условия хранения ценностей.

Применение систем охранной сигнализации с высокими тактико-техническими характеристиками на всех возможных путях движения "нарушителя" совместно с инженерной и физической защитой позволит достаточно надежно защитить объект на требуемом уровне.

Таким образом, неоспорима важность принятия мер, максимально затрудняющих получение "нарушителем" сведений об основных характеристиках технических средств охраны, их принципе действия, режимах работы.

В то же время некамуфлируемость средств охранной сигнализации в местах скопления посетителей, распространение слухов об их сложности, уникальности и невозможности их "обойти" будет способствовать отпугиванию некоторых потенциальных "нарушителей".

Наиболее вероятными путями физического проникновения "нарушителя" в здание являются:

- через двери и окна первого этажа;

- по коммуникационным и техническим проемам подвала или цокольного этажа;

- с крыши через окна или другие проемы верхних этажей;

- путем разрушения ограждений;

- имеются и иные способы, связанные с применением нарушителем специальных технических средств.

Необходимо максимально предусмотреть физические преграды перед нарушителем на пути его движения к материальным и информационным ценностям.

Внутренние переходы, подходы к наиболее важным помещениям должны быть оснащены не только средствами охранной сигнализации и телевизионного наблюдения, но и иметь надежную инженерную защиту в виде тамбуров с дистанционно управляемыми дверями, решетками, а сами хранилища ценностей - укрепленными перегородками.

Готовясь к преступлению, "нарушитель", используя легальную возможность посетить учреждение, ходит по некоторым его помещениям, может тщательно изучить наименее охраняемые места, расположение постов охраны, действия охранников при проходе сотрудников в различные режимные зоны. В этом случае очень важно разделять потоки клиентов учреждения от сотрудников. Проходы, помещения, где клиенты не обслуживаются, должны иметь кодовые замки или средства контроля доступа.

Некоторые подробности режима охраны преступник может получить, "разговорив" кого-либо из сотрудников учреждения или охраны.

Наибольшую опасность представляют сотрудники охраны, вступившие в преступную связь с "нарушителем". От них можно получить информацию и о принципах работы аппаратуры охранной сигнализации, ее режимах, "слабых" местах, оптимальных путях проникновения в требуемые помещения, а в решающий момент они могут отключить отдельные каналы охранной сигнализации. В связи с этим станционная аппаратура охранной сигнализации должна иметь систему документирования, должны протоколироваться дата и время включения/выключения каналов сигнализации, режимы проверки неисправности аппаратуры с фиксацией даты и времени происшедшего сбоя, отключения на профилактику и т.д.

Информация о состоянии охраны на объекте, оптимальных путях движения к требуемому помещению и путях отхода нужна любому "нарушителю", как стремящемуся похитить какой-либо документ, установить подслушивающее устройство, так и "нарушителю", осуществляющему разбойное нападение или преследующего иные цели.

Исходя из анализа возможных "моделей" нарушителя, способов получения им информации, конкретной архитектуры здания, характеристик территории, прилегающих зданий, рельефа местности и т.д., вырабатываются требования к инженерной защите, системе охранной сигнализации и размещению постов. Последнее означает, что для каждого конкретного объекта, здания, помещения должен разрабатываться конкретный проект его оснащения ТСОС-ТСН, СКД с учетом требований "Системной концепции...", дабы не допустить пробелов в системе защиты, которые раньше или позже но будут обнаружены грамотным злоумышленником.

Классификация нарушителей на основе моделей их действий

Разработка моделей нарушителей осуществляется на основе исследования возможных видов угроз объекту и способов их реализации.

Угрозы могут носить общий или локальный характер и исходить:

- от людей;

- от природных факторов;

- от нарушения систем жизнеобеспечения из-за техногенных факторов, а также угрозы могут носить случайный характер.

При рассмотрении вопросов классификации нарушителей нас интересуют способы реализации угроз, исходящих от людей.

Рассматривают три типа нарушителей - неподготовленный, подготовленный, квалифицированный и две группы способов реализации угроз - контактные, бесконтактные.

Способы проникновения на объект, в его здания и помещения могут быть самые различные, например:

- разбитие окна, витрины, остекленной двери или других остекленных проемов;

- взлом двери, перепиливание дужек замка и другие способы проникновения через дверь;

- пролом потолка, подлежащего блокировке;

- пролом капитального потолка, не подлежащего блокировке;

- пролом стены, подлежащей блокировке;

- пролом капитальной стены, не подлежащей блокировке;

- пролом капитального пола, не подлежащего блокировке;

- пролом пола, подлежащего блокировке;

- проникновение через разгрузочный люк;

- проникновение через вентиляционное отверстие, дымоход или другие строительные коммуникации;

- проникновение подбором ключей;

- оставление нарушителя на объекте до его закрытия;

- свободный доступ нарушителя на объект в связи с временным нарушением целостности здания из-за влияния природно-техногенных факторов или в период проведения ремонта;

- проникновение через ограждение, используя подкоп, перелаз, разрушение, прыжок с шестом и т.д.

Очевидно, что каждый тип нарушителей будет осуществлять проникновение на объект по разному - менее грамотно или более грамотно, используя различные условия, способствующие проникновению, как то:

- взрыв;

- пожар;

- разбойное нападение;

- наводнение;

- химическое заражение;

- общественные беспорядки;

- отключение электроэнергии на объекте, в районе, городе;

- постановка нарушителем помех ТСО на объекте;

- постановка нарушителем помех в канале связи объекта с охраной;

- предварительный вывод из строя ТСО на объекте;

- предварительный вывод из строя канала связи объекта с охраной;

- предварительный сговор нарушителя с персоналом объекта;

- предварительный сговор нарушителя с персоналом службы охраны объекта;

- создание и использование многих и многих других условий для проникновения на охраняемый объект, например: использование дрессированных животных и птиц, специальных технических средств обхода ТСО, специальных технических средств для предварительного изучения объекта и т.д.

Ряд моделей действий нарушителей достаточно широко представлены в художественной литературе, кинофильмах, в телепередачах с криминальными сюжетами, в научно-технических изданиях в открытой печати. Таким образом, потенциальному злоумышленнику вполне доступно повышение квалификации на материалах открытой печати, телепередач и кино. Этот неоспоримый факт, безусловно, должна в своей деятельности учитывать СБ и соответственно строить тактику охраны учреждения. Очевидно, информация о тактике охраны является строго конфиденциальной, секретной и совершенно секретной.

В зависимости от поставленных целей злоумышленник создает те или иные условия для проникновения на объект и в его помещения, пользуясь теми или иными контактными или бесконтактными способами проникновения.

К контактным способам совершения враждебных действий относятся:

1. Контактное проникновение на объект охраны:

- несанкционированное проникновение на территорию 00;

- проход на основе маскировки;

- установка средств негласного слухового, визуального, электромагнитного и др. наблюдения.

2. Контактное нарушение целостности или характера функционирования объекта:

- нарушение линий жизнеобеспечения 00;

- физическая ликвидация потенциала 00;

- затруднение штатного режима функционирования объекта.

К бесконтактным способам совершения враждебных действий относятся:

1. Бесконтактные проникновения на объект охраны:

- перехват физических полей;

- контроль радио- и телефонных переговоров;

- визуальное и слуховое наблюдение;

2. Вывод объекта из строя без проникновения на него, как то:

- нарушение целостности объекта посредством использования направленного взрыва или дистанционного оружия;

- отключение линий жизнеобеспечения объекта.

Нарушителем считается лицо, нарушающее контрольно-пропускной режим, случайно или преднамеренно нарушающее режим безопасности объекта охраны.

Для описания моделей нарушителей в качестве критериев классификации рассматриваются:

1. Цели и задачи вероятного нарушителя:

- проникновение на охраняемый объект без причинения объекту видимого ущерба;

- причинение ущерба объекту;

- освобождение спецконтингента;

- преднамеренное проникновение при отсутствии враждебных намерений;

- случайное проникновение.

2. Степень принадлежности вероятного нарушителя к объекту:

- вероятный нарушитель - сотрудник охраны;

- вероятный нарушитель - сотрудник учреждения;

- вероятный нарушитель - посетитель;

- вероятный нарушитель - постороннее лицо.

3. Степень осведомленности вероятного нарушителя об объекте:

- детальное знание объекта;

- осведомленность о назначении объекта, его внешних признаках и чертах;

- неосведомленный вероятный нарушитель.

4. Степень осведомленности вероятного нарушителя о системе охраны объекта:

- полная информация о системе охраны объекта;

- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;

- информация о системе охраны вообще, но не о системе охраны конкретного объекта;

- неосведомленный вероятный нарушитель.

5. Степень профессиональной подготовленности вероятного нарушителя:

- специальная подготовка по преодолению систем охраны;

- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.

6. Степень физической подготовленности вероятного нарушителя:

- специальная физическая подготовка;

- низкая физическая подготовка.

7. Владение вероятным нарушителем способами маскировки:

- вероятный нарушитель владеет способами маскировки;

- вероятный нарушитель не владеет способами маскировки.

8. Степень технической оснащенности вероятного нарушителя:

- оснащен специальной техникой для преодоления системы охраны;

- оснащен стандартной техникой;

- не оснащен техническими приспособлениями.

9. Способ проникновения вероятного нарушителя на объект:

- использование негативных качеств личного состава охраны объекта;

- "обход" технических средств охраны;

- движение над поверхностью земли;

- движение по поверхности земли.

На основе изложенных критериев можно выделить четыре категории нарушителя:

- нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель-профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов;

- нарушитель второй категории - непрофессиональный нарушитель с враждебными намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект;

- нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;

- нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

В принципе под моделью нарушителя понимается совокупность количественных и качественных характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны и/или его составным частям.

Существуют определенные методики количественной оценки вероятностей обнаружения нарушителя, пытающегося проникнуть на объект охраны. Здесь учитываются гамма параметров, характеризующих категорию важности объекта, конфигурацию, архитектуру и тактико-технические характеристики применяемых в КТСО ТСОС, ТСН, СКД, а также количественных и качественных характеристик нарушителя и возможных моделей его действия.

Вопросы классификации угроз информационной безопасности

В системе обеспечения безопасности объектов одно из ведущих мест занимает обеспечение информационной безопасности. Действительно, любой потенциальный нарушитель до проникновения на объект и проведения преступных действий проводит в зависимости от поставленных им конечных целей более или менее глубокую разведку с тем, чтобы обезопасить себя и выполнить поставленную преступную задачу. Поэтому защита от посторонних лиц жизненно важной информации об объекте, а также информации о системе обеспечения охранной деятельности является наиболее приоритетной задачей, от успешного решения которой зависит уровень эффективности защиты объекта в целом.

Проблемы защиты информации решаются в каждом из блоков задач, рассматриваемых системной концепцией обеспечения комплексной безопасности объекта, и в каждом блоке эти проблемы решаются своими способами и методами, хотя имеются и некоторые общие особенности.

В каждом случае работа СБ начинается с моделирования потенциальных угроз безопасности информации, их классификации и выбора адекватных угрозам мер информационной защиты.

Рассмотрим для примера вопросы классификации угроз при решении проблем обеспечения безопасности автоматизированных систем обработки информации, т.е. ПЭВМ, ЛВС, серверов баз данных и т.д. и их информационного и программного обеспечения.

В большинстве случаев нарушения по НСД к АСОИ исходят от самих сотрудников учреждений. Потери в денежном выражении составляют от них около 70%, остальные потери приходятся на хакеров, террористов и т.п.

Можно выделить три основные причины внутренних нарушений: безответственность, самоутверждение и корыстный интерес пользователей АСОИ. Кроме того существуют угрозы, исходящие от хакеров и иных нарушителей извне.

Есть опасность нанесения ущерба и не по злому умыслу, когда сотрудник учреждения, имеющий доступ к базам данных ЛВС или ПЭВМ обладает малой квалификацией, невнимателен, недисциплинирован, неряшлив в соблюдении технологии обработки информации или в пользовании программными продуктами, либо просто утомлен, омрачен какими-то личными переживаниями, что также приводит к невнимательности. При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности. Предусмотреть все такие ситуации маловероятно. Более того, во многих случаях система в принципе не может предотвратить подобные нарушения. Иногда ошибки поддержки адекватной защищенной среды могут поощрять такого рода нарушения. Система защиты может быть также неправильно настроена.

О самоутверждении. Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, ведя своего рода игру "пользователь - против системы" ради самоутверждения либо в собственных глазах, либо в глазах коллег. Хотя при этом намерения могут быть и безвредными, эксплуатация ресурсов АСОИ считается нарушением политики безопасности. Пользователи с "более криминальными намерениями" могут найти конфиденциальные данные, попытаться испортить или уничтожить их. Такой вид нарушений называется зондированием системы. Большинство систем имеет ряд средств противодействия подобным "шалостям".

Нарушение безопасности АСОИ может быть вызвано и корыстным "злоумышленником". Под "злоумышленником" понимается человек, обладающий достаточными знаниями в вопросах автоматизированной обработки информации, преследующий цели сознательного воздействия, направленного на кражу секретной информации о деятельности учреждения, его планах, процедурах проведения операций, организации системы охраны и т.д., т.е. той информации, которая позволит злоумышленнику в конце концов осуществить кражу средств, материальных или финансовых, или дезорганизовать деятельность учреждения. В этом случае он целенаправленно пытается преодолеть систему защиты от несанкционированного доступа к хранимой, передаваемой и обрабатываемой в АСОИ информации. Полностью защититься от таких проникновений практически невозможно. В какой-то мере утешает лишь то, что опаснейшие нарушения встречаются крайне редко, ибо требуют необычайного мастерства и упорства от злоумышленника, и его злонамеренное действие при грамотно организованной системе контроля может быть обнаружено, т.е. вероятность проведения таких акций против АСОИ может быть существенно снижена.

Приведем некоторые данные о количестве и объеме угроз для безопасности со стороны корыстных злоумышленников.

Итальянские психологи утверждают, что из всех служащих любой фирмы 25% - это честные люди, 25% - ожидают удобного случая для разглашения секретов и 50% будут действовать в зависимости от обстоятельств.

В 1994 г. трое репортеров лондонской газеты "Санди Тайме" провели эксперимент. Представляясь бизнесменами, они вышли на двадцать депутатов британского парламента с предложением направить в правительство запрос, в котором они заинтересованы, и получить за это наличными или чеком тысячу фунтов стерлингов. Из двадцати 17 сразу отказались, трое согласились. Аналогичные эксперименты проводила ФБР в начале 80-х гг.: агенты ФБР под видом арабских шейхов обращались к членам американского конгресса, предлагая им вознаграждение в десятки тысяч долларов за то, чтобы "шейхам" были устроены всякие поблажки.

Если эти закономерности перенести, например, на банковских служащих, то более чем от 10% персонала можно ожидать неприятностей, связанных с продажей секретной информации.

Очевидно, ущерб от каждого вида нарушений зависит от частоты их появления и ценности информации. Чаще всего встречаются нарушения, вызванные халатностью и безответственностью, но ущерб от них обычно незначителен и легко восполняется. Например, во многих системах существуют средства, позволяющие восстанавливать случайно уничтоженные наборы данных при условии, что ошибка сразу же обнаружена. Регулярное архивирование рабочих файлов данных, имеющих важное значение, позволяет существенно уменьшить ущерб от их потери.

Ущерб от зондирования системы может быть гораздо больше, но и вероятность его во много раз ниже, ибо для таких действий необходимы достаточно высокая квалификация, отличное знание системы защиты и определенные психологические особенности. Наиболее характерным результатом зондирования системы является блокировка: пользователь вводит АСОИ в состояние неразрешимого противоречия, после чего операторы и системные программисты тратят много времени для восстановления работоспособности системы. К примеру, в скандальной истории с вирусом Морриса в сети Internet, бывшей результатом зондирования системы, ущерб исчислялся миллионами долларов.

Отличительной чертой проникновений, наиболее редких, но и наиболее опасных нарушений, обычно является определенная цель: доступ к определенной информации, влияние на работоспособность системы, слежение за действиями других пользователей и др. Для осуществления подобных действий нарушитель должен обладать теми же качествами, что и для зондирования системы, только в усиленном варианте, а также иметь точно сформулированную цель. Ущерб от проникновений может оказаться в принципе невосполнимым. Например, для банков это может быть полная или частичная модификация счетов с уничтожением журнала транзакций, т.е. если с какого-то счета сняты деньги, то они должны быть записаны в другом счете.

Причины, побуждающие пользователя совершать нарушения или даже преступления, различны. Наиболее серьезный ущерб системе угрожает в случае умышленного воздействия из-за обиды, неудовлетворенности своим служебным и/или материальным положением, или по указанию других лиц, под угрозой шантажа. Шантаж, как одно из средств нелегального доступа к ценной информации, используется преступными организациями, проводящими для этого специальные мероприятия по дискредитации ответственных работников учреждения. Ущерб при этом тем больше, чем выше положение пользователя в служебной иерархии.

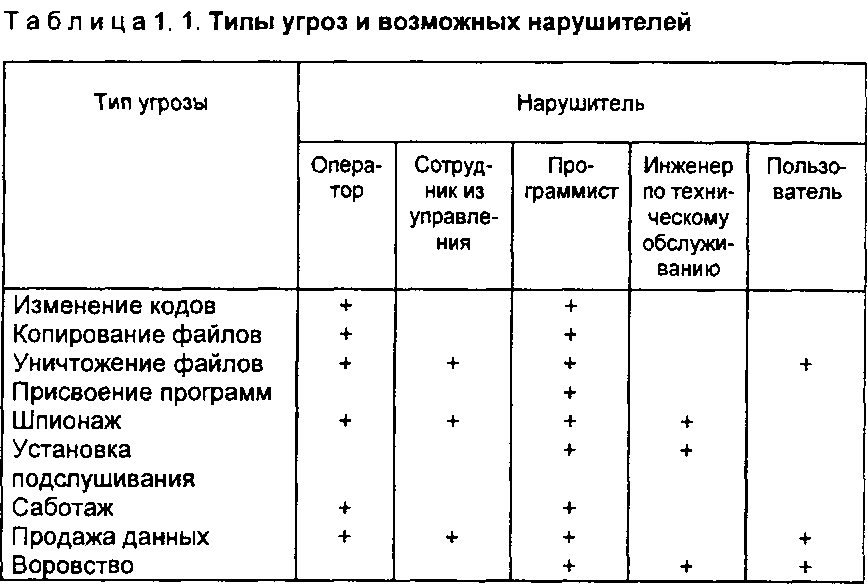
Способы предотвращения ущерба в этом случае вытекают из природы причин нарушений и преступлений. Это - соответствующая подготовка пользователей, поддержание здорового рабочего климата в коллективе, подбор персонала, своевременное обнаружение потенциальных злоумышленников и принятие соответствующих мер. Ясно, что это не только задачи администрации и детективной группы, но и коллектива в целом. Сочетание этих мер способно предотвратить сами причины нарушений и преступлений.

Таким образом, наиболее уязвимым с позиции обеспечения безопасности может стать "человеческий фактор", т.е. недисциплинированность сотрудников, недостаточный профессионализм, возможность подкупа, шантажа, угроз насилия, обиды по поводу неадекватной оценки труда и многое другое. Более детальное описание методов противодействия такого рода угрозам изложены, например, в. Отметим лишь, что коль скоро такие угрозы существуют, следует рекомендовать проведение соответствующих тщательных исследований детективной группой, отделом кадров и администрацией с привлечением профессиональных психологов, психоаналитиков, педагогов и соответствующих технических средств.

Очевидно, что для выбора оптимального варианта нейтрализации действий злоумышленника из известных методов, способов и средств противодействия нужно знать, что собой представляют возможные нарушения и злоумышленник, т.е. нужны модели нарушений, "модель" нарушителя или "модель" его возможных действий. Исследование моделей нарушителей является отправной идеей в разработке стратегии и тактики обеспечения безопасности АСОИ. В самом деле, для выбора средств защиты нужно ясно представлять, от кого защищать АСОИ.

Например, возможен такой подход: на основе доступности компонентов программного и информационного обеспечения в табл.1.1 представлены типы угроз и лица, которые могли бы вызвать такие угрозы.

При создании модели нарушителя и оценке риска потерь от действий персонала дифференцируют всех сотрудников по их возможностям доступа к системе и, следовательно, по потенциальному ущербу от каждой категории пользователей. Например, оператор или программист автоматизированной банковской системы может нанести несравненно больший ущерб, чем обычный пользователь, тем более непрофессионал.



Приведем примерный список персонала типичной АСОИ и соответствующую степень риска от каждого из них:

1. Наибольший риск:

- системный контролер;

- администратор безопасности.

2. Повышенный риск:

- оператор системы;

- оператор ввода и подготовки данных;

- менеджер обработки;

- системный программист.

3. Средний риск:

- инженер системы;

- менеджер программного обеспечения.

4. Ограниченный риск:

- прикладной программист;

- инженер или оператор по связи;

- администратор баз данных;

- инженер по оборудованию;

- оператор периферийного оборудования;

- библиотекарь системных магнитных носителей;

- пользователь-программист;

- пользователь-операционист.

5. Низкий риск:

- инженер по периферийному оборудованию;

- библиотекарь магнитных носителей пользователей.

Итак, при проектировании системы защиты АСОИ следует уделять внимание не только возможным объектам нарушений, но и вероятным нарушителям как личностям. Многолетний опыт функционирования тысяч АСОИ свидетельствует, что совершаемые без причины, а в силу случайных обстоятельств преступления очень редки.

На основе изложенных пояснений сути рассматриваемой проблемы моделирования угроз, нарушителей и их действий можно предложить следующий подход к классификации угроз безопасности АСОИ.

Отметим, что попытки дать исчерпывающую классификацию угроз безопасности АСОИ предпринимались неоднократно, однако список их постоянно расширяется, и потому в данном учебном пособии выделим лишь основные их типы.

Проводимая ниже классификация охватывает только умышленные угрозы безопасности АСОИ, оставляя в стороне такие воздействия как стихийные бедствия, сбои и отказы оборудования и др. Реализацию угрозы принято называть атакой.

Угрозы безопасности можно классифицировать по следующим признакам:

1. По цели реализации угрозы. Атака может преследовать следующие цели:

- нарушение конфиденциальности информации;

- нарушение целостности информации;

- нарушение работоспособности АСОИ. Такие нарушения могут повлечь за собой неверные результаты, отказы от обработки потока информации или отказы при обслуживании.

2. По принципу воздействия на АСОИ:

- с использованием доступа субъекта системы к объекту;

- с использованием скрытых каналов.

Субъектом доступа называется лицо или процесс, действия которого регламентируются правилами разграничения доступа, а объектом доступа - единица информационного ресурса АСОИ, доступ к которой регламентируется правилами разграничения доступа.

Под доступом понимается взаимодействие между субъектом и объектом, приводящее к возникновению информационного потока от второго к первому.

Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимосвязанным процессам обмениваться информацией таким способом, который нарушает системную политику безопасности. Скрытые каналы бывают двух видов:

- скрытые каналы с памятью, позволяющие осуществлять чтение или запись информации другого процесса непосредственно или с помощью промежуточных объектов для хранения информации;

- скрытые временные каналы, при которых один процесс может получать информацию о действиях другого, используя интервалы между какими-либо событиями.

**3.** По характеру воздействия на АСОИ. Различают активное и пассивное воздействие.

Первое всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к наборам данных, программам, вскрытие пароля и т.д.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов и их анализа. Пример - прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации в АСОИ, так как при нем никаких действий с объектами и субъектами не производится.

4. По факту наличия возможной для использования ошибки защиты. Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты.

Такая ошибка может быть обусловлена одной из следующих причин:

- неадекватностью политики безопасности реальной АСОИ. В той или иной степени несоответствия такого рода имеют все системы, но в одних случаях это может привести к нарушениям, а в других - нет. Если выявлена опасность такого несоответствия, необходимо усовершенствовать политику безопасности, изменив соответственно средства защиты;

- ошибками административного управления, под которыми понимают некорректную реализацию или поддержку принятой политики безопасности в данной АСОИ. Пусть, например, согласно политике безопасности в АСОИ должен быть запрещен доступ пользователей к некоторому определенному набору данных, а на самом деле этот набор данных доступен всем пользователям. Обнаружение и исправление такой ошибки требуют обычно небольшого времени, тогда как ущерб от нее может быть огромен;

- ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программ или комплекса программ и из-за которых эти программы могут быть использованы совсем не так, как описано в документации. Такие ошибки могут быть очень опасны, к тому же их трудно найти, а для устранения надо менять программу или комплекс программ;

- ошибками реализации алгоритмов программ, связей между ними и т.д., которые возникают на этапах реализации, отладки и могут служить источником недокументированных свойств.

5. По способу воздействия на объект атаки:

- непосредственное воздействие на объект атаки, например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой. Такие действия обычно легко предотвратить с помощью средств контроля доступа;

- воздействие на систему разрешений. При этом несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом;

- опосредованное воздействие:

- "маскарад". В этом случае пользователь присваивает себе каким-либо образом полномочия другого пользователя, выдавая себя за него;

- "использование вслепую". При таком способе один пользователь заставляет другого выполнить необходимые действия, причем последний о них может и не подозревать. Для реализации этой угрозы может использоваться вирус.

Два последних способа очень опасны. Для предотвращения подобных действий требуется постоянный контроль как со стороны администраторов и операторов за работой АСОИ в целом, так и со стороны пользователей за своими собственными наборами данных.

**6.** По способу воздействия на АСОИ:

- в интерактивном режиме;

- в пакетном режиме.

Работая с системой, пользователь всегда имеет дело с какой-либо ее программой. Одни программы составлены так, что пользователь может оперативно воздействовать на ход их выполнения, вводя различные команды или данные, а другие так, что всю информацию приходится задавать заранее. К первым относятся, например, некоторые утилиты, управляющие программы баз данных, в основном - это программы, ориентированные на работу с пользователем. Ко вторым относятся в основном системные и прикладные программы, ориентированные на выполнение каких-либо строго определенных действий без участия пользователя.

При использовании программ первого класса воздействие оказывается более длительным по времени и, следовательно, имеет более высокую вероятность обнаружения, но более гибким, позволяющим оперативно менять порядок действий. Воздействие с помощью программ второго класса является кратковременным, трудно диагностируемым, гораздо более опасным, но требует большой предварительной подготовки для того, чтобы заранее предусмотреть все возможные последствия вмешательства.

**7.** По объекту атаки. Объект атаки - это тот компонент АСОИ, который подвергается воздействию со стороны злоумышленника. Воздействию могут подвергаться следующие компоненты АСОИ:

- АСОИ в целом: злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Используют обычно "маскарад", перехват или подделку пароля, взлом или доступ к АСОИ через сеть;

- объекты АСОИ - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние, так и внутренние, каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому или нарушение их функциональности;

- субъекты АСОИ - процессы и подпроцессы пользователей. Целью таких атак является либо прямое воздействие на работу процессора - его приостановка, изменение характеристик, либо обратное воздействие - использование злоумышленником привилегий, характеристик другого процесса в своих целях. Воздействие может оказываться на процессы пользователей, системы, сети;

- каналы передачи данных. Воздействие на пакеты данных, передаваемые по каналу связи, может рассматриваться как атака на объекты сети, а воздействие на сами каналы - как специфический род атак, характерный для сети. К последним относятся: прослушивание канала и анализ графика; подмена или модификация сообщений в каналах связи и на узлах-ретрансляторах; изменение топологии и характеристик сети, правил коммутации и адресации.

**8.** По используемым средствам атаки. Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ АСОИ хорошо изучены. Использование специально разработанных программ связано с большими трудностями, но может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавления программ в АСОИ без разрешения администратора безопасности системы.

9. По состоянию объекта атаки. Состояние объекта в момент атаки весьма существенно для результатов атаки и содержания работы по ликвидации ее последствий.

Объект атаки может находиться в одном из трех состояний:

- хранения на диске, магнитной ленте, в оперативной памяти или в любом другом месте в пассивном состоянии. При этом воздействие на объект обычно осуществляется с использованием доступа;

- передачи по линии связи между узлами сети или внутри узла, Воздействие предполагает либо доступ к фрагментам передаваемой информации, либо просто прослушивание с использованием скрытых каналов;

- обработки в тех ситуациях, когда объектом атаки является процесс пользователя.

Приведенная классификация показывает сложность определения возможных угроз и способов их реализации.

Более подробно распространенные угрозы безопасности АСОИ рассмотрены, например, в.

В связи с тем, что универсального способа защиты, который мог бы предотвратить любую угрозу, не существует, для обеспечения безопасности АСОИ в целом создают защитную систему, объединяя в ней различные меры защиты.

Изложенный далеко не полно пример решения проблемы классификации угроз информационной безопасности АСОИ убеждает в необходимости проведения глубоких исследований при решении аналогичных проблем в контуре всех иных блоков задач "Системной концепции...".