Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации *угрозы* называется ***атакой***, а тот, кто предпринимает такую попытку, - ***злоумышленником***. Потенциальные *злоумышленники* называются ***источниками угрозы*** .

Чаще всего *угроза* является следствием наличия *уязвимых* мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется ***окном опасности***, ассоциированным с данным *уязвимым* местом. Пока существует *окно опасности*, возможны успешные *атаки* на ИС.

Если речь идет об ошибках в *ПО*, то *окно опасности* "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства *уязвимых* мест *окно опасности* существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Мы уже указывали, что новые *уязвимые* места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - как можно более оперативно.

Некоторые *угрозы* нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, *угроза* отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Само понятие " *угроза* " в разных ситуациях зачастую трактуется *по*-разному. Например, для подчеркнуто открытой организации *угроз* конфиденциальности может просто не существовать - вся *информация* считается общедоступной; однако в большинстве случаев нелегальный *доступ* представляется серьезной опасностью. Иными словами, *угрозы*, как и все в ИБ, зависят от интересов *субъектов информационных отношений* (и от того, какой *ущерб* является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие *угрозы* (например, пожар) опасны для всех.

Угрозы можно классифицировать *по* нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого *угрозы* направлены в первую очередь;
- по компонентам информационных систем, на которые *угрозы* нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению *источника угроз* (внутри/вне рассматриваемой ИС).

В качестве основного критерия мы будем использовать первый (*по* аспекту ИБ), привлекая при необходимости остальные.

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения *размера ущерба*) являются *непреднамеренные ошибки* штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих *информационные системы*.

Иногда такие ошибки и являются собственно *угрозами* (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают *уязвимые* места, которыми могут воспользоваться *злоумышленники* (таковы обычно ошибки администрирования). *По* некоторым данным, до 65% потерь - следствие *непреднамеренных ошибок*.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с *непреднамеренными ошибками* - максимальная *автоматизация* и строгий *контроль*.

Другие *угрозы* доступности классифицируем *по* компонентам ИС, на которые нацелены *угрозы*:

- *отказ пользователей*;
- *внутренний отказ* информационной системы;
- *отказ поддерживающей инфраструктуры*.

Обычно применительно к пользователям рассматриваются следующие *угрозы*:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать *диагностические сообщения*, неумение работать с документацией и т.п.);

- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками *внутренних отказов* являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или *повреждение аппаратуры*.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие *угрозы*:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его *угроза*, забастовка и т.п.).

Весьма опасны так называемые *"обиженные" сотрудники* - нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:

- испортить оборудование;
- встроить логическую *бомбу*, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый *ущерб*. Необходимо следить за тем, чтобы при увольнении сотрудника его *права доступа* (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, *стихийные бедствия* и события, воспринимаемые как *стихийные бедствия*,- пожары, наводнения, землетрясения, ураганы. *По* статистике, на долю огня, воды и тому подобных " *злоумышленников* " (среди которых самый опасный - перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Некоторые примеры угроз доступности

Угрозы доступности могут выглядеть грубо - как *повреждение* или даже разрушение **оборудования** (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего - грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования - не редкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом - с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную *угрозу* следует все же признать надуманной.

Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы. Автору курса довелось быть свидетелем ситуации, когда прорвало трубу с горячей водой, и системный блок компьютера (это была *рабочая станция* производства *Sun* Microsystems) оказался заполнен кипятком. Когда кипяток вылили, а *компьютер* просушили, он возобновил нормальную работу, но лучше таких опытов не ставить...

Летом, в сильную жару, норовят сломаться кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный *ущерб* наносится и репутации, и кошельку организации.

Общеизвестно, что периодически необходимо производить *резервное копирование* данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно (к этому мы еще вернемся при обсуждении *угроз* конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться *агрессивное потребление ресурсов* (обычно - полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). *По* расположению *источника угрозы* такое **потребление** подразделяется на ***локальное*** и ***удаленное***. При просчетах в конфигурации системы локальная *программа* способна практически монополизировать *процессор* и/или *физическую память*, сведя скорость выполнения других программ к нулю.

Простейший пример *удаленного потребления* ресурсов - *атака*, получившая наименование "*SYN*-наводнение". Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая *атака по* меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть *сервер* выглядит как недоступный.

По отношению к *атаке* "Papa Smurf" *уязвимы* сети, воспринимающие ping-пакеты с *широковещательными адресами*. Ответы на такие пакеты "съедают" полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме - как скоординированные распределенные *атаки*, когда на *сервер* с *множества* разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала "моды" на подобные *атаки* можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее - владельцы и пользователи систем). Отметим, что если имеет *место* архитектурный просчет в виде

разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных *атак* на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться *уязвимые* места в виде программных и аппаратных ошибок.

Основные угрозы целостности

На втором месте *по* размерам ущерба (после *непреднамеренных ошибок* и упущений) стоят *кражи* и *подлоги*. *По* данным газеты USA Today, уже в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий *ущерб* в размере 882 миллионов долларов. Можно предположить, что реальный *ущерб* был намного больше, поскольку многие организации *по* понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни *ущерб* от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних *угроз*, хотя говорят и пишут о них значительно меньше, чем о внешних.

С целью нарушения *статической целостности злоумышленник* (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда - служебная *информация*.

Еще один урок: *угрозой* целостности является не только *фальсификация* или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить *"неотказуемость"*, компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально *уязвимы* с точки зрения нарушения **целостности** не только **данные**, но и **программы**. *Угрозами динамической целостности* являются нарушение атомарности транзакций, переупорядочение, *кража*, *дублирование данных* или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная *информация* (например, пароли пользователей) не относится к определенной *предметной области*, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если *информация* хранится в компьютере или предназначена для компьютерного использования, *угрозы* ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная *информация*, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые *пользователь* часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации *по* их регулярной (*по* возможности - частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный *класс уязвимых* мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую - и не может быть обеспечена) необходимая защита. *Угроза* же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот *класс* попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, *по* сети), которая делает возможным *перехват данных*. Для *атаки* могут использоваться разные технические средства (подслушивание или прослушивание разговоров, *пассивное прослушивание сети*и т.п.), но идея одна - осуществить *доступ* к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной *угрозой* являются... выставки, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на нем данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищенной сети организации; в объединенной сети выставки - это слишком суровое *испытание* честности всех участников.

Еще один пример изменения, о котором часто забывают, - *хранение данных* на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить *доступ* к ним могут многие.

Перехват данных - очень серьезная *угроза*, и если *конфиденциальность* действительно является критичной, а данные передаются *по* многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную *сеть*, может кто угодно, так что эту *угрозу* нужно принимать во внимание *по* отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются *угрозой* не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

К неприятным *угрозам*, от которых трудно защищаться, можно отнести ***злоупотребление полномочиями***. На многих типах систем привилегированный *пользователь* (например *системный администратор*) способен прочитать любой (незашифрованный) *файл*, получить *доступ* к почте любого пользователя и т.д. Другой пример - нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный *доступ* к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные *угрозы*, которые наносят наибольший *ущерб* субъектам информационных отношений.