Лекция 3
Угрозы информационной безопасности

Основные определения

- ***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.
- 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.

Для большинства *уязвимых* мест *окно опасности* существует долго, 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.

- 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.

Угрозы классифицируют

- 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).

Наиболее распространенные угрозы доступности

- Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются *непреднамеренные ошибки* штатных пользователей.
- По некоторым данным, до 75% потерь - следствие *непреднамеренных ошибок*.

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

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

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 рассматривают 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,

Весьма опасны так называемые *"обиженные" сотрудники* - нынешние и бывшие. Они стремятся:

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

Опасны и *стихийные бедствия* - пожары, наводнения, землетрясения, ураганы. На их долю приходится 13% потерь.

- Необходимо отметить, что в качестве средства вывода системы из штатного режима эксплуатации может использоваться *агрессивное потребление ресурсов*.
- По расположению *источника угрозы* такое **потребление** подразделяется на ***локальное*** и ***удаленное***.

- Пример *удаленного потребления* ресурсов - *атака*, получившая наименование "SYN-наводнение". Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера. При этом сервер выглядит как недоступный.

- *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.
- Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных *атак* на

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

Вредоносное программное обеспечение

Одним из опаснейших способов проведения *атак* является внедрение в *атакуемые* системы *вредоносного программного обеспечения*. Мы выделим следующие грани *вредоносного ПО*:

- вредоносная функция;
- способ распространения;
- внешнее представление.

ПО, осуществляющую разрушительную функцию, предназначено для:

- внедрения другого *вредоносного ПО;*
- получения контроля над *атакуемой* системой;
- *агрессивного потребления ресурсов;*
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

- ***вирусы*** - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- ***"черви"*** - код, способный самостоятельно вызывать распространение своих копий по ИС и их выполнение.

- *Вирусы* обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. *"Черви"*, напротив, ориентированы в первую очередь на путешествия по сети.

- Вредоносный код, который выглядит как функционально полезная программа, называется *троянским*. Например, обычная программа, будучи пораженной *вирусом*, становится ***троянской***.

- ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения" определяет: "Программный *вирус* - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах".

- Следует отметить: из всего *вредоносного ПО* наибольшее внимание общественности приходится на долю *вирусов*.
- Однако "несмотря на экспоненциальный рост числа известных *вирусов*, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил "компьютерной гигиены" практически сводит риск заражения к нулю.

Основные угрозы целостности

- На втором месте по размерам ущерба (после *непреднамеренных ошибок* и упущений) стоят *кражи* и *подлоги*.
- В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних *угроз.*

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

- ввести неверные данные;
- изменить данные.

Отметим, что такое возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

- Заметим, что *угрозой* целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий.
- При этом *уязвимы* с точки зрения нарушения **целостности** не только **данные**, но и **программы**. Внедрение рассмотренного выше *вредоносного ПО* - пример подобного нарушения.

- *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 она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации.

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

- Описанный класс *уязвимых* мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита.
- Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде, которая делает возможным *перехват данных*. Для *атаки* могут использоваться разные технические средства но идея одна - осуществить доступ к данным в тот момент, когда они наименее защищены.

- Весьма опасной *угрозой* являются… *выставки*, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде.

- 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 защита может оказаться весьма сложной и дорогостоящей. При этом технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации.
- Следующий пример кражи оборудования являются *угрозой* не только для резервных носителей, но и для компьютеров, особенно портативных.

- Опасной нетехнической *угрозой* конфиденциальности являются *методы морально-психологического воздействия*, такие как ***маскарад*** - выполнение действий под видом лица, обладающего полномочиями для доступа к данным.
- К неприятным *угрозам*, от которых трудно защищаться, можно отнести ***злоупотребление полномочиями***.

- На многих типах систем привилегированный пользователь способен прочитать любой 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