

# Угрозы безопасности данных

- Основные определения и критерии классификации угроз
- Наиболее распространенные угрозы доступности
- Некоторые примеры угроз доступности
- Вредоносное программное обеспечение
- Основные угрозы целостности
- Основные угрозы конфиденциальности

# 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).

# Основные определения и критерии классификации угроз

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.

# Основные определения и критерии классификации угроз

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).

# 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.

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

# Наиболее распространенные угрозы доступности

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

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

# Наиболее распространенные угрозы доступности

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.).

# Наиболее распространенные угрозы доступности

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.



# Наиболее распространенные угрозы доступности

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.).

# Наиболее распространенные угрозы доступности

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.

# Некоторые примеры угроз доступности

- Грозы, кратковременные электромагнитные импульсы высоких напряжений
- Протечки систем водоснабжения, теплоснабжения и канализации
- Отказы систем кондиционирования

# Некоторые примеры угроз доступности

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.

# Некоторые примеры угроз доступности: распределенные атаки

Если пропускная способность канала до цели атаки превышает пропускную способность атакующего, то традиционная атака типа “отказ в обслуживании” (UDP Bomb, ICMP Flood и т. д.) не будет успешной. Распределенная же атака происходит уже не из одной точки Интернета, а сразу из нескольких, что приводит к резкому возрастанию трафика и выведению атакуемого узла из строя. Злоумышленник может послать большой объем данных сразу со всех узлов, задействованных в распределенной атаке. Атакуемый узел захлебнется огромным трафиком и не сможет обрабатывать запросы от нормальных пользователей

# Вредоносное ПО

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.

# Вредоносное ПО

Часть, осуществляющую разрушительную функцию, будем называть "**бомбой**". Вообще говоря, спектр вредоносных функций неограничен, поскольку "бомба", как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно "бомбы" предназначаются для:

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

# Вредоносное ПО

По механизму распространения различают:

- **вирусы** – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- **"черви"** – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).



# Вредоносное ПО

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.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, "черви" "съедают" полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных "бомб".

# Вредоносное ПО

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой **троянские программы** изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке

**Вредоносное ПО: определения по ГОСТ Р 51275-99  
"Защита информации. Объект информатизации. Факторы,  
воздействующие на информацию. Общие положения"**

"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".

# Вредоносное ПО

Для внедрения "бомб" часто используются ошибки типа **"переполнение буфера"**, когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные злоумышленнику места определенные данные. Так действовал еще в 1988 году знаменитый "червь Морриса"; в июне 1999 года хакеры нашли способ использовать аналогичный метод по отношению к Microsoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. Окно опасности охватило сразу около полутора миллионов серверных систем...

# Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят **кражи** и **подлоги**. По данным газеты USA Today, еще 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

# Основные угрозы целостности

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

# Основные угрозы целостности

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

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда – служебная информация.

# Основные угрозы целостности

Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...



# Основные угрозы целостности

Из приведенного случая можно сделать вывод не только об угрозах нарушения целостности, но и об опасности слепого доверия компьютерной информации. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя. Отметим, что последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место **взаимодействие разных аспектов информационной безопасности**: если нарушена конфиденциальность, может пострадать целостность

# Основные угрозы целостности

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**. Внедрение рассмотренного выше вредоносного ПО – пример подобного нарушения

# Основные угрозы целостности

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

## **Основные угрозы конфиденциальности**

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

# Основные угрозы конфиденциальности

## **Перехват данных:**

- подслушивание или прослушивание разговоров,
- пассивное прослушивание сети,
- изучение рабочего места
- анализ «памятных» дат и последовательностей

# Основные угрозы конфиденциальности

## Подмена данных:

- Использование страховых копий

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

## Основные угрозы конфиденциальности

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



# Основные угрозы конфиденциальности

Опасной нетехнической угрозой конфиденциальности являются **методы морально-психологического воздействия**, такие как **маскарад** – выполнение действий под видом лица, обладающего полномочиями для доступа к данным

# Основные угрозы конфиденциальности

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.

# Резюме

- вредоносное ПО
- целенаправленные атаки
- необеспечение защиты от форс-мажорных обстоятельств

- перехват
- кражи
- подмена
- злоупотребление полномочиями
- маскарад

- нарушение атомарности транзакций
- активное прослушивание
- необеспечение неотказуемости
- фальсификация
- подлог