Основы информационной безопасности

Лекция 4.

Угрозы безопасности и их классификация. Уязвимости информационных систем.

Литература

- В.А. Галатенко «Основы информационной безопасности», Электронная книга

Основные определения

- **Угроза** – это потенциальная возможность определенным образом нарушить информационную безопасность.
- *Угроза*—это любые обстоятельства или события, которые могут являться причиной нанесения ущерба системе в форме разрушения, распространения или модификации данных; и-или отказа в обслуживании.
- **Угроза (Threat)** — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности.

Основные определения и критерии классификации угроз

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

Основные определения и критерии классификации угроз

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

Уязвимость - любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Уязвимость (Vulnerability) — это некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

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.

Основные определения и критерии классификации угроз

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

Основные определения и критерии классификации угроз

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

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.

Основные определения и критерии классификации угроз

Отметим, что 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.

Риск

Вероятность потерь вследствие того, что определенная угроза при наличии определенной уязвимости реализуется и приведет к негативным последствиям.

Оценка риска

Процесс идентификации информационных ресурсов системы и угроз этим ресурсам, возможных потерь (то есть потенциал потери) основанный на оценке частоты возникновения событий и размере ущерба.

Рекомендуется перед введением новых информационных ресурсов выбрать контрмеры, позволяющие минимизировать возможные потери.

Основные определения и критерии классификации угроз

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы.

Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Основные определения и критерии классификации угроз

Подчеркнем, что 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).

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).

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.

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 рассматриваются следующие угрозы (форсмажор):

- 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.

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.

Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Мы выделим следующие способы воздействия вредоносного ПО:

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

Вредоносное программное обеспечение

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 программное обеспечение

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.

Вредоносное программное обеспечение

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 программное обеспечение

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 программное обеспечение

Таким образом, действие вредоносного ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

Основные угрозы целостности

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

- ввести неверные данные;
- изменить данные.

Основные угрозы целостности

Потенциально 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, 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

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.

Примеры угроз

- Тип 1. Форс мажор
- Тип 2. Организационные недостатки
- Тип 3. Человеческий фактор (ошибки)
- Тип 4. Технические проблемы
- Тип 5. Умышленные действия

Примеры угроз

Тип 1. Форс мажор

Кадровые потери

Отказ ИТ системы

Удар молнии

Пожар

Вода (Все угрозы связанные с избытком или недостатком воды, а также ее качеством)

Пожар кабельной системы

Неприемлемый уровень температуры и/или влажности

Пыль и грязь

Потеря данных под воздействием сильных магнитных полей

Отказ сети в широких масштабах (город, область и так далее)

Воздействия катастроф в близлежащем окружении

Проблемы вызванные большими публичными мероприятиями

Ураганы

Потери данных в следствии яркого света

Деградация вследствие изменения прикладной среды

Примеры угроз

Тип 5. Умышленные действия

- Кража
- Вандализм
- Атака, нападение
- Подключение к линиям связи (перехват)
- Манипуляции с линиями связи
- Неавторизованное использование ИТ систем
- Злоупотребление удаленными портами поддержки
- Перехват телефонных звонков и передаваемых данных
- Прослушивание в комнатах
- Мошенничество при использовании телефонов
- Систематический подбор паролей
- Манипуляции с правами пользователей
- Манипуляции с административными правами
- Троянские кони
- Кража мобильных ИТ систем
- Компьютерные вирусы

Основные методы реализации угроз ИБ ИС

- определение злоумышленником типа и параметров носителей информации;
- получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;
- получение злоумышленником детальной информации о функциях, выполняемых ИС;
- получение злоумышленником данных о применяемых системах защиты;
- определение способа представления информации;
- определение злоумышленником содержания данных, обрабатываемых в ИС, на качественном уровне (применяется для мониторинга ИС и для дешифрования сообщений);
- хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;
- использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН) - конфиденциальные данные перехватываются злоумышленником путем выделения информативных сигналов из электромагнитного излучения и наводок по цепям питания средств вычислительной техники, входящей в ИС;

Основные методы реализации угроз ИБ ИС

- уничтожение средств вычислительной техники и носителей информации;
- хищение (копирование) носителей информации;
- несанкционированный доступ пользователя к ресурсам ИС в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;
- несанкционированное превышение пользователем своих полномочий;
- несанкционированное копирование программного обеспечения;
- перехват данных, передаваемых по каналам связи;
- визуальное наблюдение - конфиденциальные данные считываются с экранов терминалов, распечаток в процессе их печати и т.п.;
- раскрытие представления информации (дешифрование данных);
- раскрытие содержания информации на семантическом уровне - доступ к смысловой составляющей информации, хранящейся в ИС;
- уничтожение машинных носителей информации;
- внесение пользователем несанкционированных изменений в программно-аппаратные компоненты ИС и обрабатываемые данные;

Основные методы реализации угроз ИБ ИС

- установка и использование нештатного аппаратного и/или программного обеспечения;
- заражение программными вирусами;
- внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи;
- внедрение дезинформации;
- выведение из строя машинных носителей информации без уничтожения информации - выведение из строя электронных блоков накопителей на жестких дисках и т. п.;
- проявление ошибок проектирования и разработки аппаратных и программных компонентов ИС;
- обход (отключение) механизмов защиты - загрузка злоумышленником нештатной операционной системы с дискеты, использование отладочных режимов программно-аппаратных компонент ИС и т. п.;
- искажение соответствия синтаксических и семантических конструкций языка - установление новых значений слов, выражений и т.п.;
- запрет на использование информации - имеющаяся информация по каким-либо причинам не может быть использована.

Уязвимости

- Уязвимость (Vulnerability) - любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Уязвимости

- ошибки при разработке программного обеспечения;
- преднамеренные изменения программного обеспечения с целью внесения уязвимостей;
- неправильные настройки программного обеспечения;
- несанкционированное внедрение вредоносных программ;
- неумышленные действия пользователей;
- сбои в работе программного и аппаратного обеспечения.

Уязвимости

Уязвимости, как и угрозы, можно классифицировать по различным признакам:

- по типу ПО – системное или прикладное.
- по этапу жизненного цикла ПО, на котором возникла уязвимость – проектирование, эксплуатация и пр.
- по причине возникновения уязвимости, например, недостатки механизмов аутентификации сетевых протоколов.
- по характеру последствий от реализации атак – изменение прав доступа, подбор пароля, вывод из строя системы в целом и пр.

Уязвимости

Уязвимости операционной системы и прикладного ПО в частном случае могут представлять:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ ("дыры", "люки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Уязвимости

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Так, например, протокол прикладного уровня FTP, широко используемый в Интернете, производит аутентификацию на базе открытого текста, тем самым позволяя перехватывать данные учетной записи.

Уязвимости

Должны быть:

а) устранены, т. е. должны быть предприняты активные шаги, чтобы выявить, ликвидировать или нейтрализовать уязвимые места, которые могут быть использованы нарушителями;

б) минимизированы, т. е. должны быть предприняты активные шаги, чтобы сократить до приемлемого остаточного уровня потенциальное влияние на безопасность использования любого уязвимого места в системе;

в) контролируемы, т. е. должна быть предусмотрена возможность принятия активных шагов по выявлению любой попытки использовать оставшиеся уязвимые места для того, чтобы принять меры по ограничению величины возможного ущерба.

Подходы к анализу уязвимостей

- доказать отсутствие уязвимостей, допускающих практическое использование.
- наличие уязвимостей не вызывает сомнений; их нужно непрерывно отслеживать, систематизировать их свойства и выбирать контрмеры в зависимости от этих свойств.

Для продуктов ИТ первый подход к оценке уязвимостей можно оправдать и принять, для ИС — нет.

Для ИС предпочтителен второй подход.