Основы и методы защиты информации

Основные понятия информационной безопасности

- *Конечные пользователи* – персонал и пользователи, использующие компьютерную систему (КС) с целью удовлетворения информационных потребностей;
- *Объект доступа*, или *объект*, – любой элемент КС, доступ к которому может быть произвольно ограничен (файлы, устройства, каналы);
- *Информационная безопасность* – состояние КС, при котором она способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз и при этом не создавать таких угроз для элементов самой КС и внешней среды.
- *Конфиденциальность информации* – свойство информации быть доступной только ограниченному кругу конечных пользователей и иных субъектов доступа, прошедших соответствующую проверку и допущенных к ее использованию.
- *Целостность информации* – свойство сохранять свою структуру и содержание в процессе хранения, использования и передачи.
- *Достоверность информации* – свойство, выражаемое в строгой принадлежности информации субъекту, который является ее источником.

Основные понятия информационной безопасности

- *Доступ к информации* – возможность субъекта осуществлять определенные действия с информацией.
- *Санкционированный доступ к информации* – доступ с выполнением правил разграничения доступа к информации.
- *Несанкционированный доступ (НСД)* – доступ с нарушением правил разграничения доступа субъекта к информации, с использованием штатных средств (программного или аппаратного обеспечения), предоставляемых КС.
- *Правила разграничения доступа* – регламентация прав доступа субъекта к определенному компоненту системы.
- *Идентификация* – получение от субъекта доступа к сведениям (имя, учетный номер и т.д.), позволяющим выделить его из множества субъектов.
- *Аутентификация* – получение от субъекта сведений (пароль, биометрические параметры и т.д.), подтверждающих, что идентифицируемый субъект является тем, за кого себя выдает.

Основные понятия информационной безопасности

- *Угроза информационной безопасности КС* – возможность воздействия на информацию, обрабатываемую КС, с целью ее искажения, уничтожения, копирования или блокирования, а также возможность воздействия на компоненты КС, приводящие к сбою их функционирования.
- *Уязвимость компьютерной сети* – любая характеристика, которая может привести к реализации угрозы.
- *Атака компьютерной сети* – действия злоумышленника, предпринимаемые с целью обнаружения уязвимости КС и получения несанкционированного доступа к информации.
- *Безопасная, или защищенная, КС*– КС, снабженная средствами защиты для противодействия угрозам безопасности.
- *Комплекс средств защиты* – совокупность аппаратных и программных средств, обеспечивающих информационную безопасность.
- *Политика безопасности* – совокупность норм и правил, регламентирующих работу средств защиты от заданного множества угроз.

Классификация угроз информационной безопасности

По природе возникновения:

- объективные природные явления, не зависящие от человека;
- субъективные действия, вызванные деятельностью человека.

По степени преднамеренности:

- ошибки конечного пользователя или персонала;
- преднамеренного действия, для получения НСД к информации.

По степени зависимости от активности КС:

- проявляющиеся независимо от активности КС (вскрытие шифров, хищение носителей информации);
- проявляющиеся в процессе обработки данных (внедрение вирусов, сбор "мусора" в памяти, сохранение и анализ работы клавиатуры и устройств отображения).

Классификация угроз информационной безопасности

По степени воздействия на КС:

- пассивные угрозы (сбор данных путем выведывания или подсматривания за работой пользователей);
- активные угрозы (внедрение программных или аппаратных закладок и вирусов для модификации информации или дезорганизации работы КС).

По способу доступа к ресурсам КС:

- получение паролей и прав доступа, используя халатность владельцев и персонала, несанкционированное использование терминалов пользователей, физического сетевого адреса, аппаратного блока кодирования и др.;
- обход средств защиты, путем загрузки посторонней операционной защиты со сменного носителя;
- использование недокументированных возможностей операционной системы.

Классификация угроз информационной безопасности

По текущему месту расположения информации в КС:

- внешние запоминающие устройства;
- оперативная память;
- сети связи;
- монитор или иное отображающее устройство (возможность скрытой съемки работы принтеров, графопостроителей, световых панелей и т.д.).

Критерии защищенности средств компьютерных систем

Критерий 1. Политика безопасности. КС должна поддерживать точно определенную политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом.

Критерий 2. Метки. Каждый объект доступа в КС должен иметь метку безопасности, используемую в качестве исходной информации для исполнения процедур контроля доступа.

Критерии защищенности средств компьютерных систем

Критерий 3. Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы. Доступ субъекта к ресурсам КС должен осуществляться на основании результатов идентификации и подтверждения подлинности их идентификаторов (аутентификация).

Критерий 4. Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение для поддержания конфиденциальности и целостности информации, должны отслеживаться и регистрироваться в защищенном файле-журнале.

Критерии защищенности средств компьютерных систем

Критерий 5. Контроль корректности функционирования средств защиты. Все средства защиты, обеспечивающие политику безопасности, должны находиться под контролем средств, проверяющих корректность их функционирования и быть независимыми от них.

Критерий 6. Непрерывность защиты. Все средства защиты должны быть защищены от несанкционированного воздействия или отключения. Защита должна быть постоянной и непрерывной в любом режиме функционирования системы, защиты и КС.

Типичные приемы атак на локальные и удаленные компьютерные системы

1. *Сканирование файловой системы*. Злоумышленник пытается просматривать файловую систему и прочесть, скопировать или удалить файлы. Если доступ к файлу закрыт, сканирование продолжается. Если объем файловой системы велик, то рано или поздно обнаружится хотя бы одна ошибка администратора. Такая атака проводится с помощью специальной программы, которая выполняет эти действия в автоматическом режиме.
2. *Кража ключевой информации*. Пароль может быть подсмотрен по движению рук на клавиатуре или снят видеокамерой. Некоторые программы входа в КС удаленного сервера допускают набор пароля в командной строке, где пароль отображается на экране, а иногда для ввода используются пакетные файлы для упрощения входа в ОС. Кража такого файла

Типичные приемы атак на локальные и удаленные компьютерные системы

3. *Сборка мусора*. Информация, удаляемая пользователем, не удаляется физически, а только помечается к удалению и помещается в сборщик мусора. Если получить доступ к этой программе, можно, получить и доступ к удаляемым файлам. Сборка мусора может осуществляться и из памяти.
4. *Превышение полномочий*. Используя ошибки в системном программном обеспечении и/или политики безопасности, пользователь пытается получить полномочия, превышающие те, которые были ему выделены.
5. *Жадные программы*. Программы, преднамеренно захватывающие значительную часть ресурсов КС, в результате чего другие программы работают значительно медленнее или не работают вовсе. Часто запуск такой программы приводит к краху ОС.

Типичные приемы атак на локальные и удаленные компьютерные системы

6. *Атаки маскировкой*. Маскировка – общее название большого класса сетевых атак, в которых атакующий выдает себя за другого пользователя.
7. *Программные закладки*. Программы, выполняющие хотя бы одно из следующих действий:

- внесение произвольных искажений в коды программ, находящихся в оперативной памяти (программная закладка первого типа);
- перенос фрагментов информации из одних областей оперативной или внешней памяти в другие (программная закладка второго типа);
- искажение информации, выводимой другими программами на внешние устройства или каналы связи (программная закладка третьего типа).

Основы противодействия нарушению конфиденциальности информации

Несанкционированный доступ может быть предотвращен или существенно затруднен при организации следующего комплекса мероприятий:

- идентификация и аутентификация пользователей;
- мониторинг несанкционированных действий – аудит;
- разграничение доступа к КС;
- криптографические методы сокрытия информации;
- защита КС при работе в сети.

Идентификация и аутентификация пользователей

При входе в КС, при получении доступа к программам и конфиденциальным данным субъект должен быть идентифицирован и аутентифицирован. Эти две операции обычно выполняются вместе, т.е., пользователь сначала сообщает сведения, позволяющие выделить его из множества субъектов (идентификация), а затем сообщает секретные сведения, подтверждающие, что он тот, за кого себя выдает.

Методы мониторинга несанкционированных действий

Для обеспечения надежной защиты операционной системы в журнале должны регистрироваться следующие события:

- попытки входа/выхода пользователей из системы;
- попытки изменения списка пользователей;
- попытки изменения политики безопасности, в том числе и политики аудита.

Криптографические методы защиты данных

Криптографические методы являются наиболее эффективными средствами защиты информации в КС, при передаче же по протяженным линиям связи они являются единственным реальным средством предотвращения несанкционированного доступа к ней.

1. Шифрование заменой (подстановка)

Наиболее простой метод шифрования. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов.

Наиболее простой метод – прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита.

Но такой шифр имеет низкую стойкость

2. Шифрование методом перестановки

Метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов.

3. Методы шифрования, использующие ключи

Методы предполагают знание ключа при шифровании и дешифровании. При этом важной задачей является безопасная передача ключа, который при этом обычно тоже шифруется. Учитывая короткую длину фразы, содержащей ключ, стойкость шифра ключа значительно выше, чем у основного текста.

4. Электронная цифровая подпись

При обмене электронными документами очень важным является установление авторства, подлинности и целостности информации в полученном документе. Решение этих задач возлагается на цифровую подпись, сопровождающую электронный документ.

ЗАЩИТА ИНФОРМАЦИИ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Определение вирусов

Компьютерным вирусом называется программа, способная самостоятельно создавать свои копии и внедряться в другие программы, в системные области дисковой памяти компьютера, распространяться по каналам связи. Целью создания и применения программ-вирусов является нарушение работы программ, порчи файловых систем и компонентов компьютера, нарушение нормальной работы пользователей.

Компьютерным вирусам характерны определенные стадии существования: *пассивная стадия*, в которой вирус никаких действий не предпринимает; *стадия размножения*, когда вирус старается создать как можно больше своих копий; *активная стадия*, в которой вирус переходит к выполнению деструктивных действий в локальной компьютерной системе или компьютерной

Классификация компьютерных вирусов (по среде обитания)

- *Сетевые вирусы* используют для своего распространения команды и протоколы телекоммуникационных сетей.
- *Файловые вирусы* чаще всего внедряются в исполняемые файлы, но могут внедряться и в файлы с компонентами операционных систем, драйверы внешних устройств, объектные файлы и библиотеки, в командные пакетные файлы. При запуске зараженных программ вирус на некоторое время получает управление и в этот момент производит запланированные деструктивные действия и внедрение в другие файлы программ.
- *Загрузочные вирусы* внедряются в загрузочный сектор дискеты или в главную загрузочную запись жесткого диска. Такой вирус изменяет программу начальной загрузки операционной системы, запуская необходимые для нарушения конфиденциальности программы или подменяя системные файлы.
- *Документные вирусы (макровирусы)* заражают текстовые файлы редакторов или электронных таблиц, используя макросы, которые сопровождают такие документы. Вирус активизируется, когда документ загружается в соответствующее приложение.

Классификация компьютерных вирусов (по способу заражения среды обитания)

- *Резидентные вирусы* после завершения инфицированной программы остаются в оперативной памяти и продолжают свои деструктивные действия, заражая другие исполняемые программы, вплоть до выключения компьютера.
- *Нерезидентные вирусы* запускаются вместе с зараженной программой и удаляются из памяти вместе с ней.

Классификация компьютерных вирусов (по алгоритмам функционирования)

- *Паразитирующие* – вирусы, изменяющие содержимое зараженных файлов. Эти вирусы легко обнаруживаются и удаляются из файла, так как имеют всегда один и тот же внедряемый программный код.
- *Троянские кони* – вирусы, маскируемые под полезные программы, которые очень хочется иметь на своем компьютере.
- *Вирусы-невидимки* способны прятаться при попытках их обнаружения. Они перехватывают запрос антивирусной программы и либо временно удаляются из зараженного файла, либо подставляют вместо себя незараженные участки программы.
- *Мутирующие вирусы* периодически изменяют свой программный код, что делает задачу обнаружения вируса очень сложной.

ДОПОЛНИТЕЛЬНО

Компьютерные вирусы

- сетевые черви
- троянские программы
- зомби
- шпионские программы,
- фишинг
- фарминг
- мобильные вирусы

Компьютерные вирусы

- Червь (Worm) - это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети. Особенностью червей, отличающих их от других вирусов, является то, что они не несут в себе никакой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы.

- Троян или троянский конь (Trojans) - это программа, которая находится внутри другой, как правило, абсолютно безобидной программы, при запуске которой в систему инсталлируются программа, написанная только с одной целью - нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

- Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное количество нежелательных сообщений электронной почты, а также распространяются вирусы и другие вредоносные

Компьютерные вирусы

- Шпионская программа (Spyware) - это программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации. Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы (adware).

- Фишинг (Phishing) - это почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией интернет-банка или другого финансового учреждения. Пользователь, обычно, не догадывается, что находится на фальшивом сайте и спокойно выдает злоумышленникам информацию о своих счетах, кредитных карточках, паролях и т. д.

Компьютерные вирусы

- Фарминг – это замаскированная форма фишинга, заключающаяся в том, что при попытке зайти на официальный сайт интернет банка или коммерческой организации, пользователь автоматически перенаправляется на ложный сайт, который очень трудно отличить от официального сайта. Как и в случае фишинга основной целью злоумышленников, использующих фарминг, является завладение личной финансовой информацией пользователя. Отличие заключается только в том, что вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.

- Мобильные вирусы – это компьютерные (программные) вирусы, разработанные злоумышленниками специально для распространения через мобильные устройства, такие как смартфоны и КПК. Чаще всего мобильные вирусы распространяются с помощью SMS и MMS сообщений, а также по каналу Bluetooth. Основной целью создания и распространения мобильных вирусов является несанкционированный доступ к личным данным владельцев сотовых телефонов и КПК , а также незаконное обогащение путем дистанционной организации звонков и рассылки SMS и MMS с чужих мобильных телефонов на платные номера.