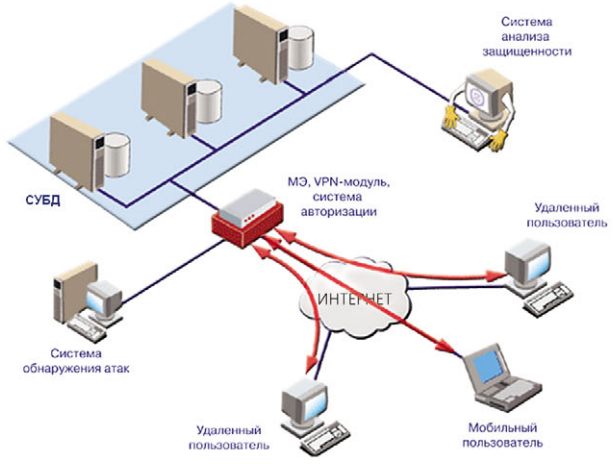
ШАНЬГИН В. Ф.

ЗАЩИТА ИНФОРМАЦИИ

В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

- ТРАДИЦИОННЫЕ И "ОБЛАЧНЫЕ" ИНФОРМАЦИОННЫЕ СИСТЕМЫ
- МНОГОУРОВНЕВАЯ ЗАЩИТА КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
- БЕЗОПАСНОСТЬ "ОБЛАЧНЫХ" ВЫЧИСЛЕНИЙ
- КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
- ТЕХНОЛОГИИ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ И ЗАЩИТЫ ОТ ВИРУСОВ



АДМИНИСТРИРОВАНИЕ И ЗАЩИТА

ДМК ПРЕСС ИЗДАТЕЛЬСТВО

УДК 004.056.5
ББК 32.973.202-018.2

Ш22

Ш22 **Шаньгин В. Ф.**
Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.

ISBN 978-5-94074-833-5

Книга посвящена методам и средствам многоуровневой защиты информации в компьютерных системах и сетях. Формулируются основные понятия защиты информации, анализируются угрозы информационной безопасности в компьютерных информационных системах. Обсуждаются базовые понятия и принципы политики информационной безопасности. Анализируются международные и отечественные стандарты информационной безопасности. Описываются криптографические методы и алгоритмы защиты информации. Обсуждаются методы и средства идентификации, аутентификации и управления доступом в корпоративных информационных системах. Обосновывается комплексный многоуровневый подход к обеспечению информационной безопасности корпоративных систем. Анализируются инфраструктура и безопасность «облачных» вычислений. Рассматриваются средства обеспечения безопасности операционных систем UNIX и Windows 7. Обсуждаются методы и средства формирования виртуальных защищенных каналов и сетей. Описываются функции межсетевых экранов. Рассматриваются технологии обнаружения и предотвращения вторжений в корпоративные информационные системы. Обсуждаются технологии защиты от вредоносных программ и спама. Рассматриваются методы управления средствами обеспечения информационной безопасности.

Данная книга представляет интерес для пользователей и администраторов компьютерных систем и сетей, менеджеров, руководителей предприятий, заинтересованных в безопасности своих корпоративных информационных систем и сетей. Книга может быть использована в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению «Информатика и вычислительная техника», а также для аспирантов и преподавателей вузов соответствующих специальностей.

Шаньгин Владимир Федорович

Защита информации
в компьютерных системах и сетях

Главный редактор Мовчан Д. А.
dm@dmk-press.ru
Корректор Синяева Г. И.
Верстка Паранская Н. В.
Дизайн обложки Мовчан А. Г.

Подписано в печать 26.03.2012. Формат 70×100 1/16 .
Гарнитура «Петербург». Печать офсетная.
Усл. печ. л. 48,1. Тираж 200 экз.
Заказ №
Web-сайт издательства: www.dmk-press.ru
Электронный адрес издательства: books@dmkpress.ru

ISBN 978-5-94074-833-5

Оглавление

ГЛАВА 1 Основные понятия и анализ угроз информационной безопасности

Непостижимо все, что в мире есть.
К тому ж изъянов в том, что есть, не счесть.

Омар Хайям «Рубаи»

Новые информационные технологии активно внедряются во все сферы человеческой деятельности. Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности для оперативного обмена информацией. Развитие Интернета привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий.

1.1. Основные понятия информационной безопасности и защиты информации

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Рассмотрим основные понятия информационной безопасности и защиты информации компьютерных систем и сетей с учетом определений стандарта ГОСТ Р 50922-96 [10, 45].

Под *информационной безопасностью* понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищен-

ность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной. Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, и стихийные бедствия (землетрясение, ураган, пожар и т. п.).

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты – информация, или носитель информации, или информационный процесс, в отношении которого необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение нанесения ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на нее.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки – деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к ней и от получения защищаемой информации злоумышленниками.

Защита информации от несанкционированного воздействия – деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия – деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информации, сбоя технических и программных средств информационных систем, а также природных явлений или иных не направленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, которые приводят к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения – деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа (*НСД*) – деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим несанкционированный

доступ к защищаемой информации, может выступать государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, которые установлены соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Современная *автоматизированная информационная система* (*ИС*) представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. *Компоненты ИС* можно разбить на следующие группы:

- *аппаратные средства* – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры, кабели, линии связи и т. д.);
- *программное обеспечение* – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;
- *данные* – информация, хранимая временно и постоянно на магнитных носителях, печатная, архивы, системные журналы и т. д.;
- *персонал* – обслуживающий персонал и пользователи.

Одной из особенностей обеспечения информационной безопасности в ИС является то, что таким абстрактным понятиям, как информация, объекты и субъекты системы, ставятся в соответствие физические представления в компьютерной среде:

- *для представления информации – машинные носители информации* в виде внешних устройств компьютерных систем (терминалов, печатающих устройств, различных накопителей, линий и каналов связи), оперативной памяти, файлов, записей и т. д.;
- под *объектами системы* понимают пассивные компоненты системы, хранящие, принимающие или передающие информацию. Доступ к объекту означает доступ к содержащейся в нем информации;
- под *субъектами системы* понимают активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

Перечисленные выше *базовые свойства информации* нуждаются в более полном толковании.

Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальным данным можно отнести, например, следующие: личную информацию пользователей; учетные записи (имена и пароли); данные о кредитных картах; данные о разработках и различные внутренние документы; бухгалтерские сведения. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Установление градаций важности защиты защищаемой информации (объекта защиты) называют *категорированием защищаемой информации*.

Под *целостностью информации* понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, то есть если не произошло их случайного или преднамеренного искажения или разрушения. Обеспечение целостности данных является одной из сложных задач защиты информации.

Достоверность информации – свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Юридическая значимость информации означает, что документ, являющийся носителем информации, обладает юридической силой.

Доступность данных – работа пользователя с данными возможна только в том случае, если он имеет к ним доступ.

Доступ к информации – получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Субъект доступа к информации – участник правоотношений в информационных процессах.

Оперативность доступа к информации – это способность информации или некоторого информационного ресурса быть доступными для конечного пользователя в соответствии с его оперативными потребностями.

Собственник информации – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Владелец информации – субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Пользователь (*потребитель*) *информации* – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Право доступа к информации – совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.

Правило доступа к информации – совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации – это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ (*НСД*) к информации характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Ответственным за защиту компьютерной системы от несанкционированного доступа к информации является *администратор защиты.*

Доступность информации подразумевает также *доступность компонента или ресурса* компьютерной системы, то есть свойство компонента или ресурса быть доступным для законных субъектов системы. Вот примерный перечень ресурсов, которые должны быть доступны: принтеры; серверы; рабочие станции; данные пользователей; любые критические данные, необходимые для работы.

Целостность ресурса или компонента системы – это свойство ресурса или компонента быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений либо разрушающих воздействий.

С допуском к информации и ресурсам системы связана группа таких важных понятий, как идентификация, аутентификация, авторизация.

С каждым субъектом системы (сети) связывают некоторую информацию (число, строку символов), идентифицирующую субъект, Эта информация является *идентификатором* субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, является *законным* (*легальным*) *субъектом.*

Идентификация субъекта – это процедура распознавания субъекта по его идентификатору. Идентификация выполняется при попытке субъекта войти в систему (сеть).

Следующим шагом взаимодействия системы с субъектом является аутентификация субъекта.

Аутентификация субъекта – это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил.

После идентификации и аутентификации субъекта выполняют процедуру авторизации.

Авторизация субъекта – это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Под *угрозой безопасности* ИС понимаются возможные действия, способные прямо или косвенно нанести ущерб ее безопасности. *Ущерб безопасности* под-

разумевает нарушение состояния защищенности информации, содержащейся и обрабатываемой в системе (сети).

С понятием угрозы безопасности тесно связано понятие уязвимости компьютерной системы (сети). *Уязвимость компьютерной системы* – это присущее системе неудачное свойство, которое может привести к реализации угрозы.

Атака на компьютерную систему – это поиск и/или использование злоумышленником той или иной уязвимости системы. Иными словами, атака – это реализация угрозы безопасности.

Противодействие угрозам безопасности является целью средств защиты компьютерных систем и сетей.

Защищенная система – это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные либо используемые для защиты информации.

Комплекс средств защиты (*КСЗ*) представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети). КСЗ создается и поддерживается в соответствии с принятой в данной организации политикой безопасности.

Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Корпоративные сети относятся к распределенным информационным системам (ИС), осуществляющим обработку информации. Обеспечение безопасности ИС предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования ИС, а также попыткам модификации, хищения, выведения из строя или разрушения ее компонентов, то есть защиту всех компонентов ИС – аппаратных средств, программного обеспечения, данных и персонала. Конкретный подход к проблеме обеспечения безопасности основан на политике безопасности, разработанной для ИС.

Политика безопасности – это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы от заданного множества угроз. Более подробные сведения о видах политики безопасности и процессе ее разработки приводятся в главе 2.

1.2. Анализ угроз информационной безопасности

Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты. Обычно под *угрозой* (в общем смысле) понимают потенциально возможное со-

бытие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам. Далее под *угрозой безопасности* информационной системы будем понимать возможность воздействия на ИС, которое прямо или косвенно может нанести ущерб ее безопасности.

В настоящее время известен достаточно обширный перечень угроз безопасности ИС, содержащий сотни позиций. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты ИС. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз безопасности ИС обусловлена тем, что хранимая и обрабатываемая информация в современных ИС подвержена воздействию чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Поэтому для защищаемой системы обычно определяют не полный перечень угроз, а перечень классов угроз.

Принято считать, что, вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации, ИС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие важные свойства информации и систем ее обработки: *доступность, целостность и конфиденциальность информации*. Иными словами, информационная безопасность ИС обеспечена в случае, если для информационных ресурсов в системе поддерживаются определенные уровни:

- доступности (возможности за разумное время получить требуемую информацию);
- целостности (невозможности несанкционированной или случайной модификации информации);
- конфиденциальности (невозможности несанкционированного получения информации).

Соответственно, для автоматизированных информационных систем угрозы следует классифицировать прежде всего по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого они направлены в первую очередь:

- *угрозы нарушения доступности (отказ в обслуживании)*, направленные на создание таких ситуаций, когда определенные действия либо блокируют доступ к некоторым ресурсам ИС, либо снижают ее работоспособность. Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным;

- *угрозы нарушения целостности информации*, хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на ее изменение либо искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена преднамеренно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации – компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (например, таким изменением является периодическая коррекция какой-либо базы данных);
- *угрозы нарушения конфиденциальности*, направленные на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой.

Данные виды угроз можно считать первичными, или непосредственными, поскольку их реализация ведет к непосредственному воздействию на защищаемую информацию.

Классификация возможных угроз безопасности ИС может быть проведена также по ряду других признаков [54, 59].

1. *По природе возникновения* различают:
   - *естественные угрозы*, вызванные воздействиями на ИС объективных физических процессов или стихийных природных явлений;
   - *искусственные угрозы* безопасности ИС, вызванные деятельностью человека.
2. *По степени преднамеренности* проявления различают:
   - *угрозы, вызванные ошибками или халатностью* персонала, например некомпетентное использование средств защиты; ввод ошибочных данных и т. п.;
   - *угрозы преднамеренного действия*, например действия злоумышленников.
3. *По непосредственному источнику угроз*. Источниками угроз могут быть:
   - *природная среда*, например стихийные бедствия, магнитные бури и пр.;
   - *человек*, например вербовка путем подкупа персонала, разглашение конфиденциальных данных и т. п.;
   - *санкционированные программно-аппаратные средства*, например удаление данных, отказ в работе операционной системы;
   - *несанкционированные программно-аппаратные средства*, например заражение компьютера вирусами с деструктивными функциями.
4. *По положению источника угроз*. Источник угроз может быть расположен:
   - *вне контролируемой зоны ИС*, например перехват данных, передаваемых

по каналам связи, перехват электромагнитных, акустических и других излучений устройств;
- *в пределах контролируемой зоны ИС*, например применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т. п.;
- *непосредственно в ИС*, например некорректное использование ресурсов ИС.

5. *По степени зависимости от активности ИС*. Угрозы проявляются:
   - *независимо от активности ИС*, например вскрытие шифров криптозащиты информации;
   - *только в процессе обработки данных*, например угрозы выполнения и распространения программных вирусов.
6. *По степени воздействия на ИС* различают:
   - *пассивные угрозы*, которые при реализации ничего не меняют в структуре и содержании ИС, например угроза копирования секретных данных;
   - *активные угрозы*, которые при воздействии вносят изменения в структуру и содержание ИС, например внедрение троянских коней и вирусов.
7. *По этапам доступа пользователей или программ к ресурсам ИС* различают:
   - угрозы, проявляющиеся *на этапе доступа к ресурсам ИС*, например угрозы несанкционированного доступа в ИС;
   - угрозы, проявляющиеся *после разрешения доступа к ресурсам ИС*, например угрозы несанкционированного или некорректного использования ресурсов ИС.
8. *По способу доступа к ресурсам ИС* различают:
   - *угрозы с использованием стандартного пути доступа* к ресурсам ИС, например незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя;
   - *угрозы с использованием скрытого нестандартного пути доступа* к ресурсам ИС, например несанкционированный доступ к ресурсам ИС путем использования недокументированных возможностей ОС.
9. *По текущему месту расположения информации, хранимой и обрабатываемой в ИС*, различают:
   - угрозы доступа к информации *на внешних запоминающих устройствах*, например несанкционированное копирование секретной информации с жесткого диска;
   - угрозы доступа к информации *в оперативной памяти*, например чтение остаточной информации из оперативной памяти; доступ к системной области оперативной памяти со стороны прикладных программ;
   - угрозы доступа к информации, *циркулирующей в линиях связи*, например незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений; незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений;

– угрозы доступа к информации, *отображаемой на терминале или печатаемой на принтере*, например запись отображаемой информации на скрытую видеокамеру.

Как уже отмечалось, опасные воздействия на ИС подразделяют на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации ИС показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни и функционирования ИС.

Причинами *случайных воздействий* при эксплуатации ИС могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Ошибки в программном обеспечении (ПО) являются распространенным видом компьютерных нарушений. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, поэтому оно практически всегда содержит ошибки. Чем выше сложность подобного программного обеспечения, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляют никакой опасности, некоторые же могут привести к серьезным последствиям, таким как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (использование компьютера в качестве плацдарма для атаки и т. п.). Обычно подобные ошибки устраняются с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких пакетов является необходимым условием безопасности информации.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник и т. д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т. п.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить *гипотетическую модель потенциального нарушителя*:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

К таким нарушителям относятся, в частности, инсайдеры. Инсайдер – это человек, допущенный к работе с информацией, которая предназначена для строго

ограниченного круга лиц. Используя свое положение, инсайдеры крадут информацию. Они могут пересылать ее по электронной почте, копировать на различные USB-устройства и КПК, записывать в ноутбуки, распечатывать и выносить на бумаге, выкладывать на всевозможные файлообменные ресурсы.

Наиболее распространенным и многообразным видом компьютерных нарушений является *несанкционированный доступ* (НСД). Суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами ИС, так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам ИС и осуществить хищение, модификацию и/или разрушение информации:

- штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными средствами ИС;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

Из всего разнообразия способов и приемов несанкционированного доступа остановимся на следующих распространенных и связанных между собой нарушениях:

- перехват паролей;
- маскарад;
- незаконное использование привилегий;
- вредоносные программы.

Перехват паролей осуществляется специально разработанными программами. При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы-перехватчика, после чего на экран выводится сообщение об ошибке и управление возвращается операционной системе. Пользователь предполагает, что допустил ошибку при вводе пароля. Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя и пароль законного пользователя, может теперь использовать их в своих целях. Существуют и другие способы перехвата паролей.

Маскарад – это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями. Целью маскарада является приписывание каких-либо действий другому пользователю

либо присвоение полномочий и привилегий другого пользователя. Примерами реализации маскарада являются:

- вход в систему под именем и паролем другого пользователя (этому маскараду предшествует перехват пароля);
- передача сообщений в сети от имени другого пользователя.

Маскарад особенно опасен в банковских системах электронных платежей, где неправильная идентификация клиента из-за маскарада злоумышленника может привести к большим убыткам законного клиента банка.

Незаконное использование привилегий. Большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций. Каждый пользователь получает свой набор привилегий: обычные пользователи – минимальный, администраторы – максимальный. Несанкционированный захват привилегий, например, посредством маскарада, приводит к возможности выполнения нарушителем определенных действий в обход системы защиты. Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

Вредоносные программы. К таким программам относятся компьютерные вирусы, сетевые черви, программа «троянский конь». Особенно уязвимы к этим программам рабочие станции конечных пользователей. Дадим краткую характеристику этих распространенных угроз безопасности ИС.

Компьютерный вирус представляет собой своеобразное явление, возникшее в процессе развития компьютерной и информационной техники. Суть этого явления состоит в том, что программы-вирусы обладают рядом свойств, присущих живым организмам, – они рождаются, размножаются и умирают. Термин «вирус» в применении к компьютерам предложил Фред Коэн из университета Южной Калифорнии. Исторически первое определение вируса было дано Ф. Коэном: «Компьютерный вирус – это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Компьютерные вирусы наносят ущерб системе за счет быстрого размножения и разрушения среды обитания.

Сетевой червь является разновидностью программы-вируса, которая распространяется по глобальной сети.

«Троянский конь» представляет собой программу, которая наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам. Аналогия такой программы с древнегреческим троянским конем вполне оправданна, так как в обоих случаях не вызывающая подозрений оболочка таит серьезную угрозу. Радикальный способ защиты от этой угрозы заключается в создании замкнутой среды исполнения программ, которые должны защищаться от несанкционированного доступа.

Следует отметить, что троянские кони, компьютерные вирусы и сетевые черви относятся к весьма опасным угрозам ИС. Особенностью современных вредоносных программ является их ориентация на конкретное прикладное ПО, ставшее стандартом де-факто для большинства пользователей, в первую очередь это Microsoft Internet Explorer и Microsoft Outlook. Массовое создание вирусов под продукты Майкрософт объясняется не только низким уровнем безопасности и надежности программ, важную роль играет глобальное распространение этих продуктов. Авторы вредоносного программного обеспечения все активнее начинают исследовать «дыры» в популярных СУБД, связующих ПО и корпоративных бизнес-приложениях, построенных на базе этих систем.

Вредоносные программы постоянно эволюционируют, основной тенденцией их развития является полиморфизм. Сегодня уже довольно сложно провести границу между вирусом, червем и троянской программой – они используют практически одни и те же механизмы, небольшая разница заключается лишь в степени этого использования. Устройство вредоносного программного обеспечения стало сегодня настолько унифицированными, что, например, отличить почтовый вирус от червя с деструктивными функциями практически невозможно. Даже в троянских программах появилась функция репликации (как одно из средств противодействия антивирусным средствам), так что при желании их вполне можно назвать вирусами (с механизмом распространения в виде маскировки под прикладные программы).

Для защиты от вредоносных программ необходимо применение ряда мер:

- исключение несанкционированного доступа к исполняемым файлам;
- тестирование приобретаемых программных средств;
- контроль целостности исполняемых файлов и системных областей;
- создание замкнутой среды исполнения программ.

Борьба с вирусами, червями и троянскими конями ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и на уровне сети. По мере появления новых вирусов, червей и троянских коней нужно обновлять базы данных антивирусных средств и приложений. Подробная классификация и характеристика вредоносных программ приводится в главе 13, посвященной защите от них.

К непрограммным угрозам относится спам. *Спам* (spam) – это массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, не выражавшим желания их получать. Спам, объем которого сейчас превышает 80% от общего объема почтового трафика, может создавать угрозу доступности информации, блокируя почтовые серверы, либо использоваться для распространения вредоносного программного обеспечения.

Как уже отмечалось, угрозы нарушения доступности, целостности и конфиденциальности информации являются первичными, или непосредственными, поскольку реализация этих угроз ведет к непосредственному воздействию на защищаемую информацию.

Для современных информационных технологий подсистемы защиты являются неотъемлемой частью ИС обработки информации. Атакующая сторона должна преодолеть эту подсистему защиты, чтобы нарушить, например, конфиденциальность ИС. Однако нужно сознавать, что не существует абсолютно стойкой системы защиты, – вопрос лишь во времени и средствах, требующихся на ее преодоление. Исходя из данных условий, рассмотрим следующую модель: защита информационной системы считается преодоленной, если в ходе исследования этой системы определены все ее уязвимости.

Преодоление защиты также представляет собой угрозу, поэтому для защищенных систем можно рассматривать четвертый вид угрозы – *угрозу раскрытия параметров ИС*, включающей в себя подсистему защиты. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которого определяются основные параметры системы, ее характеристики и т. п. Результатом этого этапа является уточнение поставленной задачи, а также выбор наиболее оптимального технического средства.

Угрозу раскрытия параметров ИС можно считать опосредованной. Последствия ее реализации не причиняют какого-либо ущерба обрабатываемой информации, но дают возможность реализовать первичные, или непосредственные, угрозы, перечисленные выше.

При рассмотрении вопросов защиты ИС целесообразно использовать четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой ИС информации. Такая градация доступа поможет систематизировать как возможные угрозы, так и меры по их нейтрализации и парированию, то есть даст возможность систематизировать весь спектр методов обеспечения защиты, относящихся к информационной безопасности.

Это следующие уровни доступа:

- уровень носителей информации;
- уровень средств взаимодействия с носителем;
- уровень представления информации;
- уровень содержания информации.

Введение данных уровней обусловлено следующими соображениями.

Во-первых, информация для удобства манипулирования чаще всего фиксируется на материальном носителе, которым может быть дискета или что-нибудь подобное.

Во-вторых, если способ представления информации таков, что она не может быть непосредственно воспринята человеком, возникает необходимость в преобразователях информации в доступный для человека способ представления. Например, для чтения информации с дискеты необходим компьютер, оборудованный дисководом соответствующего типа.

В-третьих, как уже было отмечено, информация может быть охарактеризована способом своего представления, или тем, что еще называется языком в обиходном смысле. Язык символов, язык жестов и т. п. – все это способы представления информации.

В-четвертых, человеку должен быть доступен смысл представленной информации, ее семантика.

К основным направлениям реализации злоумышленником информационных *угроз* относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства ИС программных или технических механизмов, нарушающих предполагаемую структуру и функции ИС.

В табл. 1.1 перечислены основные методы реализации угроз информационной безопасности.

Таблица 1.1. Основные методы реализации угроз информационной безопасности

Уровень доступа к информации в ИС	Методы реализации угроз информационной безопасности			
	Угроза раскрытия параметров системы	**Угроза нарушения конфиденциальности**	**Угроза нарушения целостности**	**Угроза отказа служб (отказа доступа к информации)**
Уровень носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Уровень средств взаимодействия с носителем	Получение информации о программно-аппаратной среде. Получение детальной информации о функциях, выполняемых ИС. Получение данных о применяемых системах защиты	Несанкционированный доступ к ресурсам ИС. Совершение пользователем несанкционированных действий. Несанкционированное копирование программного обеспечения. Перехват данных, передаваемых по каналам связи	Внесение пользователем несанкционированных изменений в программы и данные. Установка и использование нештатного программного обеспечения. Заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонентов ИС. Обход механизмов защиты ИС
Уровень представления информации	Определение способа представления информации	Визуальное наблюдение. Раскрытие представления информации (дешифрование)	Внесение искажения в представление данных. Уничтожение данных	Искажение соответствия синтаксических и семантических конструкций языка
Уровень содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержания информации	Внедрение дезинформации	Запрет на использование информации