Лабораторная работа №4

Оформление текста

Белорукова Елизавета

2017

Оглавление

[***Информационная безопасность*** *1*](#_Toc500783844)

[***Основные угрозы информационной безопасности*** *2*](#_Toc500783845)

[***Обеспечение информационной безопасности*** *4*](#_Toc500783846)

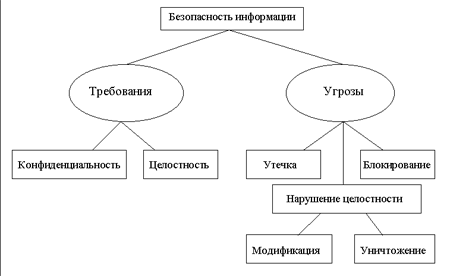
[***Аппаратно-программные средства защиты информации*** *5*](#_Toc500783847)

**Статься по теме:**

**Информационная безопасность**

Быстро развивающиеся компьютерные информационные технологии вносят заметные изменения в нашу жизнь. Информация стала товаром, который можно приобрести, продать, обменять. При этом стоимость информации часто в сотни раз превосходит стоимость компьютерной системы, в которой она хранится.

От степени безопасности информационных технологий в настоящее время зависит благополучие, а порой и жизнь многих людей. Такова плата за усложнение и повсеместное распространение автоматизированных систем обработки информации.

Под [***информационной безопасностью***](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

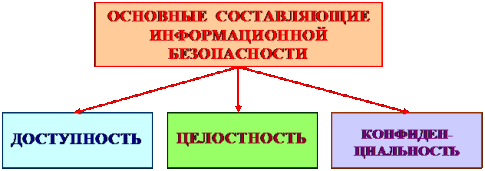
* ***доступность*** (возможность за разумное время получить требуемую информационную услугу);
* ***целостность*** (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
* ***конфиденциальность*** (защита от несанкционированного прочтения).

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

# **Основные угрозы информационной безопасности**

Современная информационная система 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 автоматизированной информационной системы можно разбить на следующие группы:

* [***аппаратные средства***](https://ru.wikipedia.org/wiki/%D0%90%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)- компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства - дисководы, принтеры, контроллеры, кабели, линии связи и т.д.);
* [***программное обеспечение***](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)- приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;
* [***данные***](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5)- хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
* ***персонал*** - обслуживающий персонал и пользователи.



Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами ***случайных воздействий*** при эксплуатации могут быть:

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

***Преднамеренные воздействия*** [[1]](#footnote-1) . В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

* недовольством служащего своей карьерой;
* взяткой;
* любопытством;
* конкурентной борьбой;
* стремлением самоутвердиться любой ценой.

Можно составить гипотетическую модель потенциального нарушителя:

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

Наиболее распространенным и многообразным видом компьютерных нарушений является [***несанкционированный доступ***](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF)(НСД). НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов НСД, по которым можно осуществить хищение, изменение или уничтожение информации:

* Через человека:
  + хищение носителей информации;
  + чтение информации с экрана или клавиатуры;
  + чтение информации из распечатки.
* Через программу:
  + перехват паролей;
  + дешифровка зашифрованной информации;
  + копирование информации с носителя.
* Через аппаратуру:
  + подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
  + перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые ***удаленные атаки***[[2]](#footnote-2). Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

# **Обеспечение информационной безопасности**

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. законодательный (законы, нормативные акты, стандарты и т.п.);
2. морально-этический (всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации);
3. административный (действия общего характера, предпринимаемые руководством организации);
4. физический (механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей);
5. аппаратно-программный (электронные устройства и специальные программы защиты информации).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют ***систему защиты***.

Надежная система защиты должна соответствовать следующим принципам:

* Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.
* Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.
* Защита тем более эффективна, чем проще пользователю с ней работать.
* Возможность отключения в экстренных случаях.
* Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать.
* Под защитой должна находиться вся система обработки информации.
* Разработчики системы защиты, не должны быть в числе тех, кого эта система будет контролировать.
* Система защиты должна предоставлять доказательства корректности своей работы.
* Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.
* Объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других.
* Надежная система защиты должна быть полностью протестирована и согласована.
* Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.
* Система защиты должна разрабатываться, исходя из предположения, что пользователи будут совершать серьезные ошибки и, вообще, имеют наихудшие намерения.
* Наиболее важные и критические решения должны приниматься человеком.
* Существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

# **Аппаратно-программные средства защиты информации**

Несмотря на то, что современные ОС для персональных компьютеров, такие, как Windows 2000, Windows XP и Windows NT, имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется. Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами, например, при сетевом информационном обмене.

Аппаратно-программные средства защиты информации можно разбить на пять групп:

1. Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.
2. Системы шифрования дисковых данных.
3. Системы шифрования данных, передаваемых по сетям.
4. Системы аутентификации электронных данных.
5. Средства управления криптографическими ключами.

**1. Системы идентификации и аутентификации пользователей**

Применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы таких систем заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

При построении этих систем возникает проблема выбора информации, на основе которой осуществляются процедуры идентификации и аутентификации пользователя. Можно выделить следующие типы:

* секретная информация, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.); пользователь должен запомнить эту информацию или же для нее могут быть применены специальные средства хранения;
* физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.).

Системы, основанные на первом типе информации, считаются ***традиционными***. Системы, использующие второй тип информации, называют ***биометрическими***. Следует отметить наметившуюся тенденцию опережающего развития биометрических систем идентификации.

**2. Системы шифрования дисковых данных**

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая ***криптографией*** [от греч. ***kryptos***- скрытый и ***grapho*** - пишу].

Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков. К программам первого типа можно отнести архиваторы типа ARJ и RAR, которые позволяют использовать криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities, Best Crypt.

Другим классификационным признаком систем шифрования дисковых данных является способ их функционирования. По способу функционирования системы шифрования дисковых данных делят на два класса:

* системы "прозрачного" шифрования;
* системы, специально вызываемые для осуществления шифрования.

В системах прозрачного шифрования (шифрования "на лету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Системы второго класса обычно представляют собой утилиты, которые необходимо специально вызывать для выполнения шифрования. К ним относятся, например, архиваторы со встроенными средствами парольной защиты.

Большинство систем, предлагающих установить пароль на документ, не шифрует информацию, а только обеспечивает запрос пароля при доступе к документу. К таким системам относится MS Office, 1C и многие другие.

**3. Системы шифрования данных, передаваемых по сетям**

Различают два основных способа шифрования: канальное шифрование и оконечное (абонентское) шифрование.

В случае [***канального шифрования***](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы. Однако у данного подхода имеются и существенные недостатки:

* шифрование служебных данных осложняет механизм маршрутизации сетевых пакетов и требует расшифрования данных в устройствах промежуточной коммуникации (шлюзах, ретрансляторах и т.п.);
* шифрование служебной информации может привести к появлению статистических закономерностей в шифрованных данных, что влияет на надежность защиты и накладывает ограничения на использование криптографических алгоритмов.

***Оконечное (абонентское) шифрование*** позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся служебная информация остается открытой. Недостатком является возможность анализировать информацию о структуре обмена сообщениями, например об отправителе и получателе, о времени и условиях передачи данных, а также об объеме передаваемых данных.

**4. Системы аутентификации электронных данных**

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации данных применяют код аутентификации сообщения (имитовставку) или электронную подпись.

***Электронная цифровая подпись*** представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

***Имитовставка*** вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных. Имитовставка проверяется получателем, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными

Таким образом, для реализации имитовставки используются принципы симметричного шифрования, а для реализации электронной подписи - асимметричного. Подробнее эти две системы шифрования будем изучать позже.

**5. Средства управления криптографическими ключами**

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети.

Различают следующие виды функций управления ключами: генерация, хранение, и распределение ключей.

Способы ***генерации ключей*** для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами. Подробнее на этом вопросе остановимся при изучении симметричных и асимметричных криптосистем.

Функция ***хранения*** предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (т.е. мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключа является критическим вопросом криптозащиты.

***Распределение*** - самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

* с помощью прямого обмена сеансовыми ключами;
* используя один или несколько центров распределения ключей.

Сравнение способов интерполяции.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование | Способ интерполяции | Размах вариации (сообщ.) | Среднее отклонение (сообщ.) | Коэффициент осцилляции | Линейный коэффициент вариации |
| Оценка мат. ожидания кол-ва сообщ. ИБ | Линейная | 9.3 | 1.5 | 0.083 | 0.013 |
| Квадратичная | 5.3 | 0.7 | 0.048 | 0.006 |
| Кубическая | 5.2 | 0.7 | 0.047 | 0.006 |
| Оценка дисперсии кол-ва сообщ. ИБ | Линейная | 1.1 | 0.2 | 0.088 | 0.013 |
| Квадратичная | 0.6 | 0.1 | 0.052 |  |
| Кубическая | 0.7 | 0.1 | 0.047 |  |

1. ***Преднамеренные воздействия***- это целенаправленные действия нарушителя. [↑](#footnote-ref-1)
2. **Удалённая атака** — информационное разрушающее воздействие на распределённую вычислительную систему (ВС), осуществляемое программно по каналам связи. [↑](#footnote-ref-2)