В связи с широким распространением персональных компьютеров не только как средств обработки информации, но также как оперативных средств коммуникации (электронная, телефаксная почта), возникают проблемы, связанные с обеспечением защиты информации от преднамеренных или случайных искажений.

Актуальность этих проблем подчеркивается также тем обстоятельством, что персональный компьютер или автоматизированное рабочее место (АРМ) является частью систем обработки информации, систем коллективного пользования, вычислительных сетей. В таких случаях предъявляются достаточно жесткие требования по надежности и достоверности передаваемой информации.

Любой канал связи характеризуется наличием в нем помех, приводящих к искажению информации, поступающей на обработку. С целью уменьшения вероятности ошибок принимается ряд мер, направленных на улучшение технических характеристик каналов, на использование различных видов модуляции, на расширение пропускной способности и т. п. При этом также должны приниматься меры по защите информации от ошибок или несанкционированного доступа.

*Доступ –* это получение возможности использовать информацию, хранящуюся в ЭВМ (системе).

Всякая информация в машине или системе требует той или иной *защиты,* под которой понимается совокупность методов, позволяющих управлять доступом выполняемых в системе программ к хранящейся в ней информации.

«Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

в отношении сведений, отнесенных к государственной тайне, уполномоченными органами на основании Закона Российской Федерации «О государственной тайне»;

в отношении конфиденциальной документированной информации собственник информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

в отношении персональных данных – федеральным законом».[[1]](#footnote-1)

«Целями защиты являются:

предотвращение утечки, хищения, утраты, искажения, подделки информации;

предотвращение угроз безопасности личности, общества, государства;

предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

предотвращение других форм незаконного вмешательства в информационные системы, обеспечение правового режима документированной информации как объекта собственности;

защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения».[[2]](#footnote-2)

Задача защиты информации в информационных вычислительных системах решается, как правило, достаточно просто: обеспечиваются средства контроля за выполнением программ, имеющих доступ к хранимой в системе информации. Для этих целей используются либо списки абонентов, которым разрешен доступ, либо *пароли,* что обеспечивает защиту информации при малом количестве пользователей. Однако при широком распространении вычислительных и информационных систем, особенно в таких сферах, как обслуживание населения, банковское дело, этих средств оказалось явно недостаточно. Система, обеспечивающая защиту информации, не должна позволять доступа к данным пользователям, не имеющим такого права. Такая система защиты является неотъемлемой частью любой системы коллективного пользования средствами вычислительной техники, независимо от того, где они используются. Данные экспериментальных исследований различных систем коллективного пользования показали, что пользователь в состоянии написать программы, дающие ему доступ к любой информации, находящейся в системе. Как правило, это обусловлено наличием каких-то ошибок в программных средствах, что порождает неизвестные пути обхода установленных преград.

В процессе разработки систем защиты информации выработались некоторые общие правила, которые были сформулированы Ж. Солцером и М. Шредером (США):

1. *Простота механизма защиты.* Так как средства защиты усложняют и без того сложные программные и аппаратные средства, обеспечивающие обработку данных в ЭВМ, естественно стремление упростить эти дополнительные средства. Чем лучше совпадает представление пользователя о системе защиты с ее фактическими возможностями, тем меньше ошибок возникает в процессе работы.
2. *Разрешения должны преобладать над запретами.* Нормальным режимом работы считается отсутствие доступа, а механизм защиты должен быть основан на условиях, при которых доступ разрешается. Допуск дается лишь тем пользователям, которым он необходим.
3. *Проверка полномочий любого обращения к любому объекту информации.* Это означает, что защита выносится на общесистемный уровень и предполагает абсолютно надежное определение источника любого обращения.
4. *Разделение полномочий* заключается в определении для любой программы и любого пользователя в системе минимального круга полномочий. Это позволяет уменьшить ущерб от сбоев и случайных нарушений и сократить вероятность преднамеренного или ошибочного применения полномочий.
5. *Трудоемкость проникновения в систему.* Фактор трудоемкости зависит от количества проб, которые нужно сделать для успешного проникновения. Метод прямого перебора вариантов может дать результат, если для анализа используется сама ЭВМ.
6. *Регистрация проникновений в систему.* Иногда считают, что выгоднее регистрировать случаи проникновения, чем строить сложные системы защиты.[[3]](#footnote-3)

Обеспечение защиты информации от несанкционированного доступа – дело сложное, требующее широкого проведения теоретических и экспериментальных исследований по вопросам системного проектирования. Наряду с применением разных приоритетных режимов и систем разграничения доступа разработчики информационных систем уделяют внимание различным криптографическим методам обработки информации.

*Криптографические методы* можно разбить на два класса:

1. обработка информации путем замены и перемещения букв, при котором объем данных не меняется (шифрование);
2. сжатие информации с помощью замены отдельных сочетаний букв, слов или фраз (кодирование).

По способу реализации криптографические методы возможны в аппаратном и программном исполнении.

Для защиты текстовой информации при передачах на удаленные станции телекоммуникационной сети используются аппаратные способы шифрования и кодирования. Для обмена информацией между ЭВМ по телекоммуникационной сети, а также для работы с локальными абонентами возможны как аппаратные, так и программные способы. Для хранения информации на магнитных носителях применяются программные способы шифрования и кодирования.

*Аппаратные способы шифрования информации* применяются для передачи защищенных данных по телекоммуникационной сети. Для реализации шифрования с помощью смешанного алфавита используется перестановка отдельных разрядов в пределах одного или нескольких символов.

*Программные способы* применяются для шифрования информации, хранящейся на магнитных носителях (дисках, лентах). Это могут быть данные различных информационно-справочных систем АСУ, АСОД и др. программные способы шифрования сводятся к операциям перестановки, перекодирования и сложения по модулю 2 с ключевыми словами. При этом используются команды ассемблера TR (перекодировать) и XC (исключающее ИЛИ).

 Особое место в программах обработки информации занимают операции кодирования. Преобразование информации, в результате которого обеспечивается изменение объема памяти, занимаемой данными, называется *кодированием.* На практике кодирование всегда используется для уменьшения объема памяти, так как экономия памяти ЭВМ имеет большое значение в информационных системах. Кроме того, кодирование можно рассматривать как криптографический метод обработки информации.

Естественные языки обладают большой избыточностью для экономии памяти, объем которой ограничен, имеет смысл ликвидировать избыточность текста или уплотнить текст.

Существуют несколько способов уплотнения текста.

1. *Переход от естественных обозначений к более компактным.* Этот способ применяется для сжатия записи дат, номеров изделий, уличных адресов и т.д. Идея способа показана на примере сжатия записи даты. Обычно мы записываем дату в виде 10. 05. 01. , что требует 6 байтов памяти ЭВМ. Однако ясно, что для представления дня достаточно 5 битов, месяца- 4, года- не более 7, т.е. вся дата может быть записана в 16 битах или в 2-х байтах.
2. *Подавление повторяющихся символов.* В различных информационных текстах часто встречаются цепочки повторяющихся символов, например пробелы или нули в числовых полях. Если имеется группа повторяющихся символов длиной более 3, то ее длину можно сократить до трех символов. Сжатая таким образом группа повторяющихся символов представляет собой триграф S P N , в котором S – символ повторения; P – признак повторения; N- количество символов повторения, закодированных в триграфе. В других схемах подавления повторяющихся символов используют особенность кодов ДКОИ, КОИ- 7, КОИ-8 , заключающуюся в том , что большинство допустимых в них битовых комбинаций не используется для представления символьных данных.
3. *Кодирование часто используемых элементов данных.* Этот способ уплотнения данных также основан на употреблении неиспользуемых комбинаций кода ДКОИ. Для кодирования, например, имен людей можно использовать комбинации из двух байтов диграф PN, где P – признак кодирования имени, N – номер имени. Таким образом может быть закодировано 256 имен людей, чего обычно бывает достаточно в информационных системах. Другой способ основан на отыскании в текстах наиболее часто встречающихся сочетании букв и даже слов и замене их на неиспользуемые байты кода ДКОИ.
4. *Посимвольное кодирование.* Семибитовые и восьмибитовые коды не обеспечивают достаточно компактного кодирования символьной информации. Более пригодными для этой цели являются 5 - битовые коды, например международный телеграфный код МГК-2. Перевод информации в код МГК-2 возможен с помощью программного перекодирования или с использованием специальных элементов на основе больших интегральных схем (БИС). Пропускная способность каналов связи при передаче алфавитно - цифровой информации в коде МГК-2 повышается по сравнению с использованием восьмибитовых кодов почти на 40%.
5. *Коды переменной длины.* Коды с переменным числом битов на символ позволяют добиться еще более плотной упаковки данных. Метод заключается в том, что часто используемые символы кодируются короткими кодами, а символы с низкой частотой использования - длинными кодами. Идея такого кодирования была впервые высказана Хаффманом, и соответствующий код называется кодом Хаффмана. Использование кодов Хаффмана позволяет достичь сокращения исходного текста почти на 80%.

Использование различных методов уплотнения текстов кроме своего основного назначения – уменьшения информационной избыточности – обеспечивает определенную криптографическую обработку информации. Однако наибольшего эффекта можно достичь при совместном использовании как методов шифрования, так и методов кодирования информации.

Надежность защиты информации может быть оценена временем, которое требуется на расшифрование (разгадывание) информации и определение ключей.

Если информация зашифрована с помощью простой подстановки, то расшифровать ее можно было бы, определив частоты появления каждой буквы в шифрованном тексте и сравнив их с частотами букв русского алфавита. Таким образом определяется подстановочный алфавит и расшифровывается текст.

«Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством Российской Федерации».[[4]](#footnote-4)

«За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и субъектов Российской Федерации.

Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные третейские суды.

Третейский суд рассматривает конфликты и споры сторон в порядке, установленном законодательством о третейских судах.».[[5]](#footnote-5)

«Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях».[[6]](#footnote-6)

**СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ:**

1. Федеральный закон Российской Федерации «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ
2. Савельев А. Я. Основы информатики: Учебник для вузов. – М.: Издательство МГТУ им. Н. Э. Баумана, 2001 .
3. Правовая информатика и управление в сфере предпринимательства. Учебное пособие. – М.: Юристъ, 1998.
1. Федеральный закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ (ст.21). [↑](#footnote-ref-1)
2. Там же. (ст. 20). [↑](#footnote-ref-2)
3. Савельев А. Я. Основы информатики: Учебник для вузов. – М.: Издательство МГТУ им. Н. Э. Баумана, 2001. С. 216. [↑](#footnote-ref-3)
4. Федеральный закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ (ст. 21 п.2). [↑](#footnote-ref-4)
5. Там же (ст. 23 п. 3). [↑](#footnote-ref-5)
6. Там же (ст. 24 п. 3). [↑](#footnote-ref-6)