Министерство образования Новосибирской области
государственное бюджетное профессиональное образовательное учреждение
Новосибирской области
«НОВОСИБИРСКИЙ ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»

Директор С.С. Лузан

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие

Новосибирск
2018

Содержание

Введение 4
Понятие информационной безопасности 5
Тема 1. Информационная безопасность. Основные положения 9
1.1 ИБ деятельности общества 9
1.1.2. Информация, основные свойства 11
1.2 Угрозы ИБ 13
1.3 Комплексное обеспечение ИБ 16
1.4 Источники угроз информационной безопасности РФ 18
Тема 2. Защита информации 19
2.1 Предмет защиты 19
2.2. Технологии обеспечения безопасности обработки информации 21
2.3. Классификация методов и средств защиты от угроз ИБ 23
Тема 3. Криптографические методы и средства защиты информации 27
3.1 Симметричные криптосистемы 29
3.2 Системы с открытыми ключами 35
3.3 Электронная (цифровая) подпись 36
3.4 Организация протоколирования связи и распределения ключей 36
Тема 4. Компьютерные вирусы и антивирусные программы 37
4.1 Компьютерные вирусы 37
4.2 Основные виды вирусов 38
4.3 Методы и технологии борьбы с компьютерными вирусами 39
4.4 Виды антивирусных программ 40
Тема 5. Защита информации в ПК 42
Тема 6. Технические средства и комплексное обеспечение безопасности 48
Тема 7. Организационно-правовое обеспечение ИБ 51
7.1 Отечественное организационное и нормативно-правовое обеспечение ИБ 51
7.2 Международные нормативно-правовые акты обеспечения ИБ 52
7.3 Организационное регулирование защиты информации 53
7.4 Ответственность за нарушение законодательства в информационной сфере 55
Литература 56

Введение

Данное методическое пособие предназначено для использования при изучении дисциплины «Информационная безопасность». Оно позволяет помочь студенту самостоятельно ознакомиться с основными понятиями информационной безопасности; угрозами информационной безопасности; методами и средствами защиты информационной безопасности; криптографическими методами и средствами; с видами компьютерных вирусов и антивирусных программ; техническими средствами обеспечения безопасности, а так же организационно-правовым обеспечением ИБ и нормативными документами.

Методическое пособие может быть полезным как при изучении данной дисциплины, так и для самостоятельных занятий. Для более глубокого изучения данной темы следует обратиться к дополнительной литературе.

Понятие информационной безопасности

Информационная безопасность не является залогом безопасности организации, информации и компьютерных систем. К сожалению, обеспечить надежную защиту "по взмаху волшебной палочки" нельзя. Но реализовать ее на должном уровне вполне реально, хотя концепции, лежащие в ее основе, не очень-то и просты.

Информационная безопасность - меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним.

Как следует из определения, информационная безопасность не обеспечивает абсолютную защиту, поэтому ***Информационная безопасность - это предупредительные действия***, которые позволяют защитить информацию и оборудование от угроз и использования их уязвимых мест.

Краткая история развития информационной безопасности

Способы защиты информации и других ресурсов постоянно меняются, как меняется наше общество и технологии. Очень важно понять это, чтобы выработать правильный подход к обеспечению безопасности. Надо знать историю, чтобы избежать ошибок.

Физическая безопасность

На заре цивилизации ценные сведения сохранялись в материальной форме: вырезались на ***каменных табличках***, позже записывались на бумагу. Для их защиты использовались такие же материальные объекты: стены, рвы и охрану.

Защита информации в процессе передачи

Важную или секретную информацию старались не сохранять на твердых носителях, наверное, поэтому до нас дошло так мало записей алхимиков. Они не обсуждали свои секреты ни с кем, кроме избранных учеников, ведь знание - это сила. Наверное, это и было самой лучшей защитой. Сунь Цзы говорил: "Секрет, который знает больше чем один, - уже не секрет".

Информация передавалась обычно с посыльным и в сопровождении охраны. И эти меры себя оправдывали, поскольку единственным способом получения информации было ее похищение.
К сожалению, физическая защита имела один ***недостаток***. При захвате сообщения враги узнавали все, что было написано в нем.

Еще в *V веке до нашей эры* спартанские полководцы использовали нехитрое шифровальное устройство для связи друг с другом. На палку круглого сечения (***скиталу***) наматывалась длинная полоска кожи, причем витки плотно прилегали один к другому. Поперек витков писали сообщение, затем кожаную полоску разматывали и передавали гонцу.

Перехваченное послание нельзя было прочесть: отдельные закорючки на витках кожи ничего не говорили противнику. А вот получатель, имея палку такого же диаметра, мог снова намотать на нее кожу и прочесть письмо.

Юлий Цезарь (*I век до нашей эры*) тоже прибегал к шифрованию. Он изобрел ***шифр Цезаря***.
Суть его проста: при написании послания буквы "сдвигались" вправо на три позиции. Для русского алфавита вместо "А" следовало бы писать "Г", вместо "Б" – "Д" и так далее. Разумеется, такой шифр, как и скиталу, нельзя было считать надежным, но, по крайней мере, он позволял скрыть содержание письма от случайного глаза. Варианты шифра Цезаря используются до сих пор.

Данная концепция получила свое развитие во время *Второй мировой войны*. Германия использовала машину под названием ***Enigma*** для шифрования сообщений, посылаемых воинским частям.

Немцы считали, что машину Enigma практически невозможно было взломать. Ее действительно было бы очень трудно взломать - если бы не ошибки операторов, позволившие союзникам прочитать некоторые сообщения.

Самое слабое звено в безопасности

Прежде всего, люди. Нельзя не вспомнить разведчиков бывшего Советского Союза и их одноразовые ключи. В любой системе безопасности самое слабое звено - это человеческие слабости.

После второй мировой войны Советский Союз использовал ***одноразовые ключи*** при передаче информации разведчиками. Эти ключи на самом деле представляли собой бумажные блокноты со случайным расположением цифр на каждой странице. Каждая страница предназначалась только для одного сообщения. Такая схема шифрования могла бы стать действительно уникальной, однако разовые ключи использовались не по одному разу, благодаря чему некоторые сообщения удавалось расшифровать.

Защита излучения

Если не считать ошибок при использовании шифровальных систем, сложный шифр очень трудно взломать. Поэтому шел ***постоянный поиск других*** способов перехвата информации, передаваемой в зашифрованном виде.

В 1950 г. было установлено, что доступ к сообщениям возможен посредством просмотра электронных сигналов, возникающих при их передаче по телефонным линиям.

Работа любых электронных систем сопровождается излучением, в том числе телетайпов и блоков шифрования, используемых для передачи зашифрованных сообщений. Блок шифрования посылает зашифрованное сообщение по телефонной линии, а вместе с ним передается и ***электрический сигнал от исходного сообщения***. Следовательно, при наличии хорошей аппаратуры исходное сообщение можно ***восстановить***.

Электронные сигналы "обходят" шифрование

Проблема защиты излучения привела к созданию в Соединенных Штатах Америки программы "TEMPEST". Эта программа разработала ***стандарты на электрическое излучение компьютерных систем***, используемых в секретных организациях. Целью программы было уменьшение уровня излучения, которое могло бы быть использовано для сбора информации.

Защита компьютера

При передаче сообщений по телеграфу достаточно было обеспечить защиту коммуникаций и излучения. Затем появились компьютеры, на которые были перенесены в электронном формате информационные ресурсы организаций. Спустя какое-то время работать на компьютерах стало проще, и многие пользователи научились общаться с ними в режиме интерактивного диалога. К информации теперь мог обратиться любой пользователь, вошедший в систему. Возникла потребность в защите компьютеров.

В начале 70-х гг. XX века Дэвид Белл и Леонард Ла Падула разработали модель безопасности для операций, производимых на компьютере. Эта модель базировалась на правительственной концепции уровней классификации информации (несекретная, конфиденциальная, секретная, совершенно секретная) и уровней допуска. Если человек (субъект) имел уровень допуска выше, чем уровень файла (объекта) по классификации, то он получал доступ к файлу, в противном случае доступ отклонялся. Эта концепция нашла свою реализацию в различных стандартах.

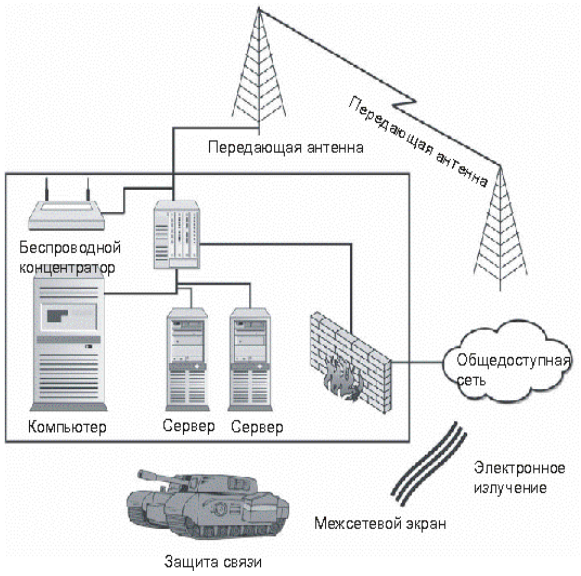
Технологии компьютерных систем ***слишком быстро развиваются*** по сравнению с программой сертификации. Возникают новые версии операционных систем и аппаратных средств и находят свои рынки сбыта еще до того, как более старшие версии и системы проходят сертификацию.

Защита сети

Одна из проблем, связанных с критериями оценки безопасности систем, заключалась в недостаточном понимании механизмов работы в сети. При объединении компьютеров к старым проблемам безопасности добавляются новые. Да, мы имеем средства связи, но при этом локальных сетей гораздо больше, чем глобальных. ***Скорости*** передачи стали ***выше***, появилось множество линий общего пользования. Шифровальные блоки иногда отказываются работать. Существует ***излучение от проводки***, проходящей по всему зданию. И, наконец, появились многочисленные ***пользователи, имеющие доступ*** к системам.
В наши дни проблемы стали еще серьезнее. Организации стали использовать ***беспроводные сети.***

Защита информации

В реальной жизни **надежная защита - это объединение всех способов защиты**.



1. ***Физическая защита*** необходима для обеспечения сохранности материальных активов - бумажных носителей и систем.
2. ***Защита коммуникаций*** отвечает за безопасность при передаче информации.
3. ***Защита излучения*** необходима, если противник имеет мощную аппаратуру для чтения электронной эмиссии от компьютерных систем.
4. ***Компьютерная безопасность*** нужна для управления доступом в компьютерных системах, а
5. ***Безопасность сети*** нужна для защиты локальных сетей.

В совокупности все виды защиты обеспечивают информационную безопасность.

Информационная безопасность включает множество **аспектов безопасности**

До настоящего времени не разработан процесс сертификации компьютерных систем, подтверждающий обеспечиваемую безопасность. Для большинства предлагаемых решений технологии слишком быстро ушли вперед.

Лабораторией техники безопасности США (Underwriters Laboratory) была предложена ***новая концепция*** безопасности, согласно которой необходимо создать ***центр сертификации***, удостоверяющий безопасность различных продуктов. Если совершено проникновение в систему, пользователи которой работали с несертифицированным продуктом, то это следует расценивать как халатное отношение к безопасности администраторов этой системы.

К сожалению, эта концепция ***создает две проблемы***.
Темп развития технологий ставит под сомнение тот факт, что центр представит самые лучшие сертифицированные продукты, прежде чем они станут устаревшими.

Тема 1. Информационная безопасность. Основные положения

1.1 ИБ деятельности общества

Информационная безопасность Российской Федерации - это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Интересы общества в информационной сфере заключается в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, духовном обновлении России.

Интересы личности в информационной сфере заключается в реализации конституционных прав человека и гражданина на доступ к информации, ее использовании в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите процессов переработки информации, обеспечивающей личную безопасность.

Выделяют **четыре основные составляющие национальных интересов Российской Федерации** в информационной сфере.

Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;
- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;
- обеспечить конституционные права и свободы человека и гражданина, свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
- гарантировать свободу массовой информации и запрет цензуры;
- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая представляет собой информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о самой государственной политике, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этих целей необходимо:

- укреплять государственные средства массовой информации (СМИ), расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
- интенсифицировать формирование открытых государственных информационных ресурсов, повышать эффективность их хозяйственного использования.

Третья составляющая предусматривает развитие современных информационных технологий (ИТ), отечественной индустрии информации (средств информатизации, телекоммуникации и связи); обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронного и компьютерного производства.

Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;
- поощрять отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
- способствовать производству в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая включает в себя защиту информационных ресурсов от несанкционированного доступа; обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Для достижения этих целей необходимо:

- повысить безопасность информационных систем, в том числе сетей связи, прежде всего сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты процессов переработки информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

1.1.2. Информация, основные свойства и характеристики безопасности ее применения

Информация, создаваемая, потребляемая и хранимая в процессе функционирования и взаимодействия социальных, технических и организационно-технических систем друг с другом и с внешней средой (чаще всего это одно и тоже), может быть разделена на два основных рода: внутреннюю и внешнюю.

Внутренняя информация - это структурная, или преобразующая, информация (последнее название адекватно для частного вида организационно-технических структур - автоматических систем управления (АСУ)). Внутренняя структурная информация создается, потребляется и распространяется самой системой. Ее использование санкционировано только для внутреннего потребления, т.е. для управления элементами и подсистемами, обеспечения основного и вспомогательных производственных процессов и т.п. эту информацию содержат массивы данных, документы и файлы, не предназначенные для передачи во внешнюю среду.

Внешняя информация - циркулирует в каналах обмена с иными системами, в совокупности составляющими внешнюю среду. В процессе информационного обмена с внешней средой может участвовать информация, являющаяся основным продуктом деятельности системы, также контрольная информация о состоянии системы (финансовая, отчетная, плановая и т.п.), правовая и нормативная информация, регламентирующая условия функционирования системы, рекламная информация и др.

Информации присущи следующие свойства.

1. Доступность (если информация содержится на информационном носителе). Необходимо защищать материальные носители информации, так как с их помощью можно обезопасить материальные объекты и людей.

2. Ценность. Ценность информации определяется степенью ее полезности для владельца. Обладание истинной (достоверной) информацией дает ее владельцу определенные преимущества. Истинной, или достоверной, является та информация, которая с достаточной для владельца (пользователя) точностью отображает объекты и процессы окружающего мира в определенных временных и пространственных рамках.

Информация, искаженно представляющая действительность (недостоверная информация), может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышленно, то ее называют ***дезинформацией***.

Если доступ к информации ограничивается, то такая информация является ***конфиденциальной***. Эта информация может содержать государственную или коммерческую тайну.

Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме. *Государственную* тайну могут содержать сведения, принадлежащие государству.

Информацию правомочно рассматривать как товар, имеющий определённую цену. Цена, как и ценность информации, связана с полезностью информации для конкретных людей, организаций, государств.

Информация может быть получена тремя путями:

- проведением научных исследований;
- покупкой;
- противоправным добыванием.

3. Количественная характеристика информации. В большинстве работ по теории информации основное внимание уделяется той ее характеристике, которая получила название *объем информации.* Основными методами определения объема информации являются: комбинаторный, статистический, алгоритмический и метрический.

Например: при *комбинаторном* методе используют разнообразие множества характеристик объекта X по признакам его элементов x. В соответствии с определением Р.Хартли считается, что объём информации I тем больше, чем выше разнообразие их возможных состояний: $I = K \ln N$ (K - коэффициент пропорциональности, N - число возможных состояний).

В *статистическом* методе используют энтропийный подход. При этом объём информации оценивается мерой уменьшения неопределённости (энтропии) ожидания событий после получения информации. Объём тем больше, чем ниже вероятность события. По формуле К.Шеннона объём информации I равен:

$$I = N\sum_{i=1}^{k} P_i \log_2 P_i$$

где N – количество символов в сообщении, k – число символов в алфавите языка, P_i – вероятность появления в сообщении символа i

Алгоритмическая мера информационной сложности основывается на модели по А.Н.Колмогорову. Другая разновидность определения информации – *тезаурусный* подход. Согласно этому подходу, предложенному Ю.А.Шрейдером, объём информации, извлекаемый человеком из сообщения, можно оценить степенью изменения его знаний. И так далее. В настоящее время известно несколько более или менее удачных попыток введения и использования количественных показателей для оценки информации.

1.2 Угрозы ИБ

При комплексном подходе к классификации угроз ИБ их можно подразделить,
во-первых, на случайные и преднамеренные,
во-вторых, на пассивные и активные,
в-третьих, на организационные, физико-технические, информационные и программно-математические (смотреть рисунок 1)

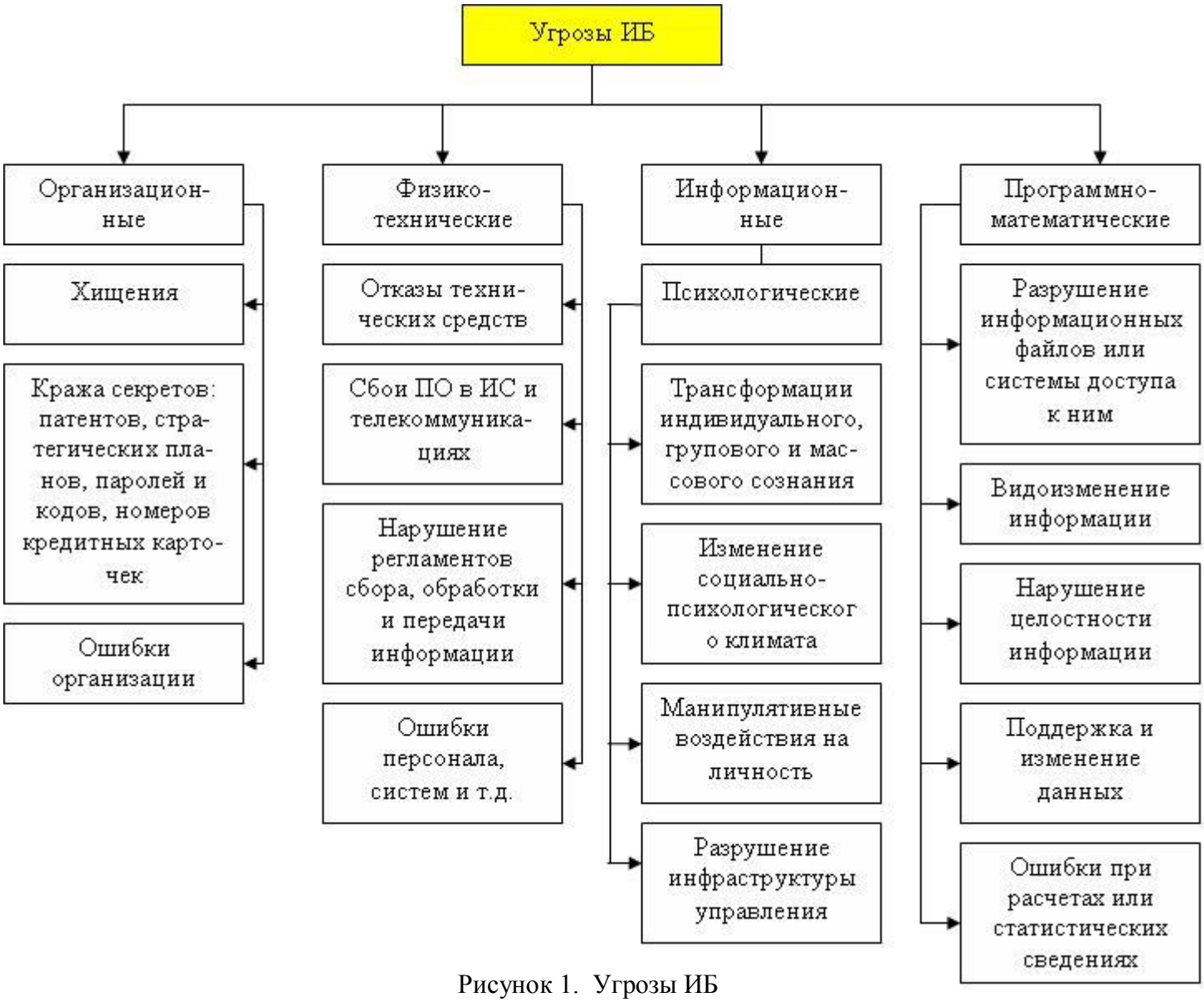


Рисунок 1. Угрозы ИБ

По своей общей направленности угрозы ИБ РФ подразделяют на следующие виды:
1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности;
2. Угрозы информационному обеспечению государственной политики РФ;
3. Угрозы развитию отечественной индустрии информации, а также обеспечению эффективного использования отечественных информационных ресурсов;
4. Угрозы безопасности информационных и телекоммуникационных средств и систем.

1. Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов РФ нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение органами власти, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение Российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

2. Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики РФ вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

3. Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

4. Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникаций и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств перехвата информации в средства обработки информации, а также в служебные помещения органов власти и организаций;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информатизации, телекоммуникации и связи;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

1.3 Комплексное обеспечение ИБ

Комплексное обеспечение информационной безопасности - это взаимосвязанный комплекс организационно-правовых, физических, социальных, духовных, информационных, программно-математических и технических методов, мероприятий и средств, обеспечивающих нормальное функционирование государства, его структур, населения, фирм, предприятий как на его территории и в его пространстве, так и в межгосударственных отношениях, независимо от состояний государства - мирного труда или военного времени.

Государственная политика обеспечения ИБ РФ основывается на следующих основных принципах:

1. Соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению ИБ РФ;
2. Открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;
3. Правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации;
4. Приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Так как международное сотрудничество в области ИБ является неотъемлемой составляющей взаимодействия всех стран мира, то

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения ИБ являются:

1. Запрещение разработки, распространения и применения "информационного оружия";
2. Обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным сетям и каналам связи;
3. Координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;
4. Предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

Основными элементами организационной основы системы обеспечения ИБ РФ являются:

- Президент РФ
- Совет Федерации
- Федеральное собрание РФ
- Государственная Дума Федерального собрания РФ
- Правительство РФ
- Совет безопасности РФ
- Федеральные органы исполнительной власти
- Межведомственные и государственные комиссии
- Органы исполнительной власти субъектов РФ
- Органы местного самоуправления
- Органы судебной власти
- Общественные организации
- Общественные объединения
- Граждане, принимающие участие в решении задач (в соответствии с законом)

Общие методы обеспечения ИБ РФ подразделяют на правовые, организационно-технические и экономические

- К *правовым методам* обеспечения ИБ РФ относится:

- разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения ИБ РФ.

- *Организационно- техническими* методами обеспечения ИБ РФ являются:

- создание и совершенствование системы обеспечения ИБ РФ;
- предупреждение и пресечение правонарушений в информационной сфере, а также привлечение к ответственности лиц, совершивших преступления в этой сфере;
- разработка, использование и совершенствование средств защиты процессов переработки информации и методов контроля эффективности этих средств;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты процессов переработки информации;
- сертификация средств защиты процессов переработки информации, стандартизация способов и средств защиты;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения ИБ РФ;
- формирование системы мониторинга показателей и характеристик ИБ РФ в наиболее важных сферах жизни и деятельности общества и государства.

- *Экономические методы* обеспечения ИБ РФ включают в себя:

- разработку программ обеспечения ИБ РФ и определение порядка их финансирования;
- совершенствование системы финансирования методов защиты процессов переработки информации, создание системы страхования информационных рисков физических и юридических лиц.

1.4 Источники угроз информационной безопасности РФ

Источники угроз ИБ РФ подразделяют на внешние и внутренние.

К внешним источникам угроз ИБ относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам угроз ИБ РФ относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения ИБ РФ; недостаточная разработанность нормативно-правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению ИБ РФ;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения ИБ;
- отставание России от ведущих стран мира по уровню информатизации органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Тема 2. Защита информации

2.1 Предмет защиты

Под защитой информации АСОД понимается регулярное использование в них средств и методов, принятия мер с целью обеспечения надежности информации (смотреть рисунок 2).

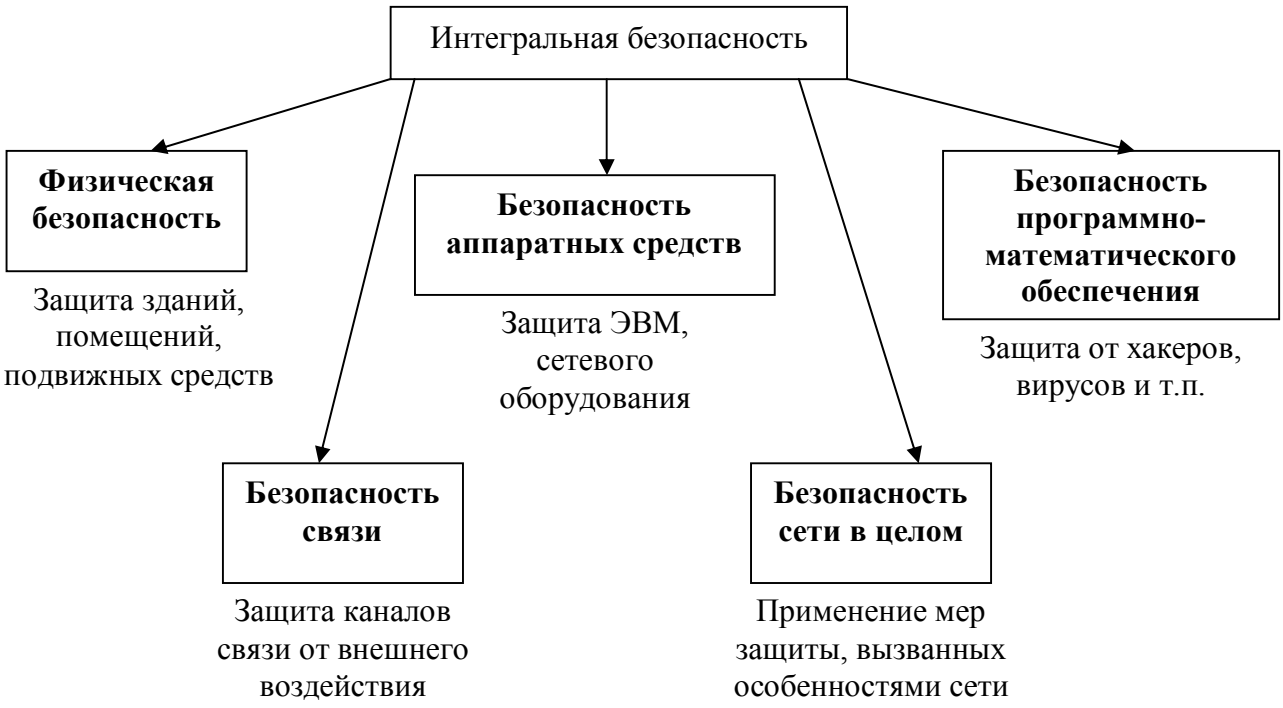


Рисунок 2. Интегральная безопасность

Объекты защиты ИБ

1. Информационные ресурсы - содержащие данные, составляющие государственную тайну и другие конфиденциальные сведения.
В соответствии с Федеральным законом "Об информации, информатизации и защите информации" от 25.01.95 №24-ФЗ под информационными ресурсами понимаются отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах).

2. Информационные системы различных классов: библиотеки, архивы, базы и банки данных, процедура сбора, обработки и хранения, передачи.

3. Информационная инфраструктура и ее элементы, центры переработки информации, каналы обмена, механизмы обеспечения функционирования телекоммуникационной системы, сами средства защиты перерабатываемой информации.

4. Общественное сознание – информация, распространяемая СМИ, воздействующая на политические взгляды, моральные ценности и поведение людей.

5. Компьютерная система (КС) – это комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.
АСОД (автоматизированная система обработки данных).

Элементы защиты - это та совокупность данных, которая может содержать подлежащие защите сведения (смотреть рисунок 3).

Рисунок 3. Основные элементы и объекты защиты в АСОД

ЭВМ – аппаратные средства (процессор, память, устройства ввода/вывода и т. д.) и системы программного обеспечения (ОС, программы технического обслуживания, пакеты прикладных программ)

Вычислительные комплексы – многомашинные и многопроцессорные являющиеся базовыми средствами для создания систем обмена данными различного назначения

Вычислительные системы (ВС) - системы обработки данных, включающие аппаратные средства и программное обеспечение, ориентированные на решение определенных задач.

Каналы связи - через которые передаются блоки данных (данные и служебная информация)

Вычислительные сети - сети передачи данных (СПД) и локальные вычислительные сети (ЛВС)

АСУ (автоматизированные системы управления) - системы управления процессами

АСОУ (автоматизированные системы организационного управления) - сложный комплекс, состоящий из коллектива специалистов, автоматизированных и технических средств

2.2. Технологии обеспечения безопасности обработки информации

Методы защиты включают в себя:

Препятствие (ограничение доступа) **-** метод физического преграждения пути злоумышленнику к защищаемой информации;

Управление доступом (контроль доступа, разделение доступа) **–** метод защиты путём регулирования использования всех ресурсов компьютерной информационной системы;

- Идентификация пользователей, персонала и ресурсов
- Опознание (установление подлинности) объекта по идентификатору
- Проверка полномочий (соответствия дня недели)
- Разрешение и создание условий работы в пределах регламента
- Регистрация (протокол) обращений к ресурсам
- Реагирование (сигнализация) при попытке несанкционированного доступа

Регламентация (разграничение доступа) **-** процесс переработки информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемых процессов обработки информации, при которых возможности несанкционированного доступа к ней сводятся к минимуму;

Маскировка (криптография) **–** метод защиты информации путем ее криптографического закрытия;

Принуждение (законодательные меры) **-** метод, при котором пользователи и персонал вынуждены соблюдать правила обработки, передачи и использования защищаемых процессов обработки информации под угрозой материальной, административной или уголовной ответственности;

Побуждение **-** метод защиты процессов переработки информации, который побуждает пользователя и персонал системы не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Все эти методы реализуются за счёт **средств** и **механизмов**

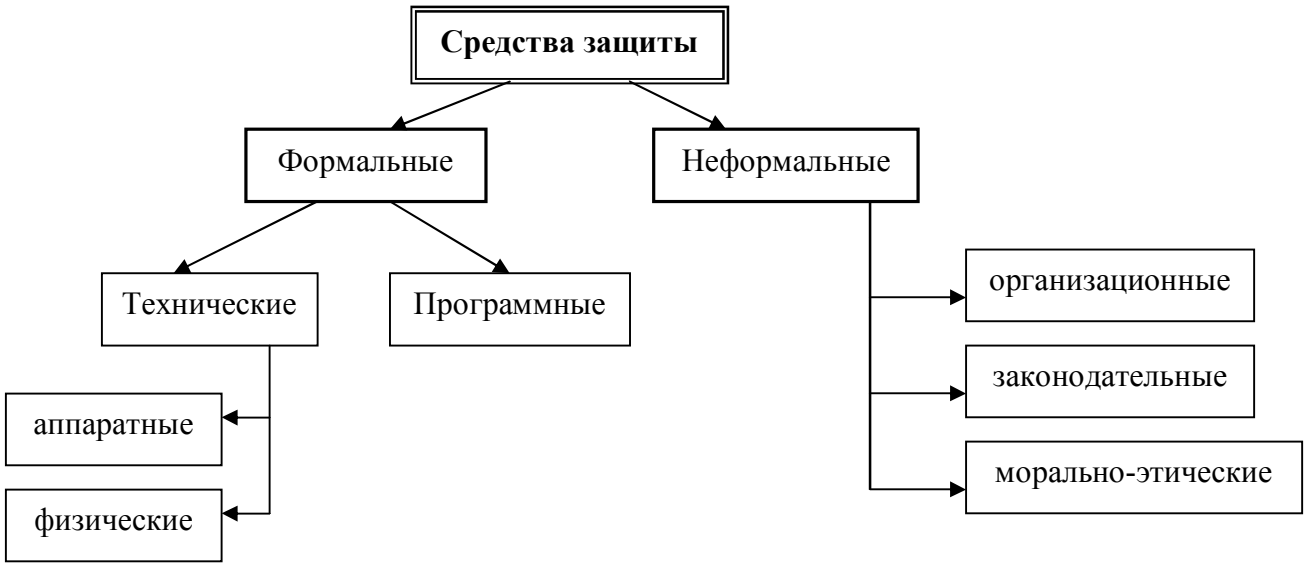


Рисунок 4. Средства защиты ИБ

Технические – электрические, электромеханические, электронные устройства

аппаратные – встраиваемые в вычислительную технику устройства
физические – автономные устройства и системы (замки, решётки)

Программные – программное обеспечение, специальное для защиты процессов обработки информации

Организационные – организационно-технические, организационно-правовые в процессе создания и эксплуатации

Законодательные – законодательные акты страны, которыми определяются правила пользования, обработки и передачи информации

Морально-этические – всевозможные меры, не являющиеся обязательными, несоблюдение которых ведёт к потере авторитета и престижа человека

Механизмы безопасности

1. Криптография (шифровани**е**) – обеспечение секретности (аутентичности, подлинности) передаваемых сообщений;

2. Цифровая подпись – это присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство;

3. Контроль доступа – осуществление проверки полномочий объектов на доступ к ресурсам;

4. Обеспечение целостности данных – как к блоку данных, так и к потоку;

5. Обеспечение аутентификации – установление односторонней или взаимной подлинности;

6. Постановка трафика (для засекреченного потока данных) – механизм заполнения текста. Это генерация фиктивных блоков для нейтрализации возможности получения информации посредством наблюдения;

7. Управление маршрутизацией – для исключения передачи информации по ненадёжным каналам;

8. Арбитраж (освидетельствование) – подтверждение данных третьей стороной (арбитром).

2.3. Классификация методов и средств защиты от угроз ИБ

Методы и средства защиты от угроз ИБ можно представить общей классификацией, в соответствии с которой процессы защиты можно разделить на три большие группы: **предотвращение, парирование и нейтрализацию угроз.**

1. <u>Предотвращение</u> – упреждение возможности проникновения на начальном этапе

- организационно-правовые методы
- предотвращение угроз несанкционированного изменения инфраструктур
- предотвращение угроз шпионажа и диверсий
- предотвращение угроз несанкционированного доступа к КС
- методы и средства предотвращения случайных угроз
- криптографические методы предотвращения угроз

2. <u>Парирование</u> – препятствие или ограничение воздействия на объект

- защита от электромагнитных излучений и наводок
- комплексная защита сетей
- обеспечение безопасности процессов переработки информации в защищаемой КС

3. <u>Нейтрализация</u> – устранение, ликвидация в случае диверсии

- борьба с компьютерными вирусами
- защита хранения и обработки информации в базах данных
- комплексные организационно-технические методы и средства устранения и нейтрализации угроз

1. Предотвращение угроз ИБ включает в себя технологии, осуществляющие упреждение и предупреждение возможного проникновения, а также организацию и реализацию защиты объекта на начальном этапе нападения.

- **К организационным и правовым методам и средствам предотвращения угроз ИБ относятся:**
  - Государственная политика безопасности информационных технологий (ИТ)
  - Правовой статус КС, информации, систем защиты информации владельцев и пользователей информации и т.д.
  - Иерархическая структура государственных органов политики безопасности ИТ
  - Система стандартизации, лицензирования и сертификации средств защиты информации
  - Воспитание патриотизма и бдительности, повышение уровня образования и ответственности граждан в области ИТ

Вопросы ИБ РФ изложены:

- в «Концепции национальной безопасности» утверждённой Указом Президента 17.12.1997 №1300
- в Федеральном законе «Об информации, информатизации и защите информации» от 25.01.1995 №24-ФЗ
- в законе «О Государственной тайне» от 21.07.1993 №5485-1

В УК РФ гл.28 – уголовная ответственность за преступления в области ИТ

- ст. 272 – неправомерный доступ к информации (от штрафа 2000 мрот до 5 лет)
- ст. 273 – ответственность за создание вредительских программ (от штрафа в 1 мрот до заключения 2 мес – 7 лет)
- ст. 274 – ответственность за нарушение прав эксплуатации (запрет на деятельность)

- **К методам предотвращения угроз несанкционированного изменения инфраструктур относятся:**
  - Выявление и устранение закладок (непреднамеренные ошибки разработчиков, сбои и отказы аппаратуры и программных средств)
  - Применение стандартных блочных структур
  - Дублирование разработки КС (независимая разработка одного и того же блока)
  - Контроль адекватности функционирования (тестирование)
  - Многослойная фильтрация (поэтапное выявление ошибок)
  - Автоматизация процесса разработки КС (применение типовых решений)
  - Контроль порядка разработки
  - Сертификация готового продукта

- **К методам предотвращения угроз шпионажа и диверсий относятся:**
  - Создание системы охраны объекта (СОО) (инженерные конструкции, охранная сигнализация, средства наблюдения, подсистемы доступа на объект, дежурная смена охраны и т.д.)
  - Организация работ с конфиденциальными ресурсами (сбор, уничтожение, учёт, выдача конфиденциальных документов)
  - Противодействие наблюдению (в оптическом и инфракрасном диапазоне; использование стекла с односторонней проводимостью, жалюзи; разворот мониторов; ложные тепловые поля)
  - Противодействие подслушиванию
    а) защита речевой информации при передаче по каналам связи с помощью аналогового скремблирования[1] и дискретизации речи[2] с последующим шифрованием
    б) защита акустической информации в помещениях (звукоизоляция, зашумление, защита от несанкционированной записи, обнаружение закладных устройств)
  - Предотвращение злоумышленных действий персонала (в 80% случаев этому способствует образ жизни персонала, микроклимат в коллективе, охрана сотрудников и разграничение доступа к информации)

- **К методам предотвращения угроз несанкционированного доступа к КС относятся:**

Наиболее практичные злоумышленники не используют программно-аппаратные средства, а используют знания о КС, сведения о системе защиты, сбои и отказы программных средств, ошибки и небрежность обслуживающего персонала.

[1] Аналоговое скремблирование – изменение речевого сигнала таким образом, что полученный сигнал, обладая свойством неразборчивости, занимает ту же полосу частот, что и исходный

[2] Дискретизация – преобразование речевой информации, представленной в цифровой форме в соответствии с выбранными алгоритмами (обеспечивает наивысшую степень защиты)

- Для защиты процессов переработки информации – система разграничения доступа, реализующая процессы идентификации и аутентификации
- Для защиты от копирования программных средств – средства, обеспечивающие целостность структуры КС (копирование – наиболее привлекательно для злоумышленников, т.к. сначала создается копия, а потом проводится исследование)
- Для блокирования несанкционированного исследования – комплекс средств и мер, объединённых в систему защиты от исследования и копирования (СЗИК)

- **К методам и средствам предотвращения случайных угроз относятся:**
  - Дублирование информации (самый эффективный)
  - Повышение надёжности КС (корректная постановка задачи на этапах разработки)
  - Оптимизация взаимодействия пользователей (НОТ, воспитание и обучение персонала, оборудование рабочих мест, режим труда и отдыха)
  - Минимизация ущерба от аварий (правильный выбор места строительства, использование источников бесперебойного питания, организация оповещения, обучение персонала)
  - Блокировка ошибочных операций
  - Применение отказоустойчивых КС (резервирование, помехоустойчивое кодирование)

- **К криптографическим методам предотвращения угроз относятся:**
  - Кодирование (замена исходной информации кодами)
  - Сжатие-расширение (сокращение объёма информации)
  - Стенография (позволяет скрыть не только смысл передаваемой информации, но и сам факт хранения и передачи её)
  - Шифрование-дешифрование (процесс преобразования открытой информации в закрытую)

2. Парирование угроз включает в себя методы и приемы, препятствующие или ограничивающие воздействие на защищенный объект

- **К методам парирования угроз от электромагнитных излучений и наводок относятся:**

Пассивные методы:
- Экранирование поля (электрического, магнитного и электромагнитного). Этот метод защиты от электромагнитных излучений является одним из самых эффективных методов
- Снижение мощности излучений и наводок (изменение электрических схем, использование оптических каналов связи, изменение конструкции, использование фильтров)
- Снижения информативности сигналов (схемные решения при обработке алгоритмов и конструкций преобразователей и процессоров, кодирование информации)

Активные методы:
- Пространственное зашумление
- Линейное зашумление (антенна рядом)

которые предполагают применение генераторов шумов, различающихся принципами формирования маскирующих помех.

- **К методам комплексной защиты КС относятся:**
  - Реализация принципа системности (модульное построение)
  - Применение многоуровневой Компьютерной Системы Защиты Информации (КСЗИ)
  - Централизованнее управление КСЗИ
  - Использование блочной аппаратуры

- **К методам и средствам обеспечения безопасности обработки информации в защищённой КС относятся:**
  - Обеспечение безопасности информации в пользовательской подсистеме и спец.коммуникациях КС
  - Защита обработки информации на уровне подсистемы управления сетью
  - Защита передачи и преобразования информации в каналах связи
  - Обеспечение контроля подлинности взаимодействия процессов

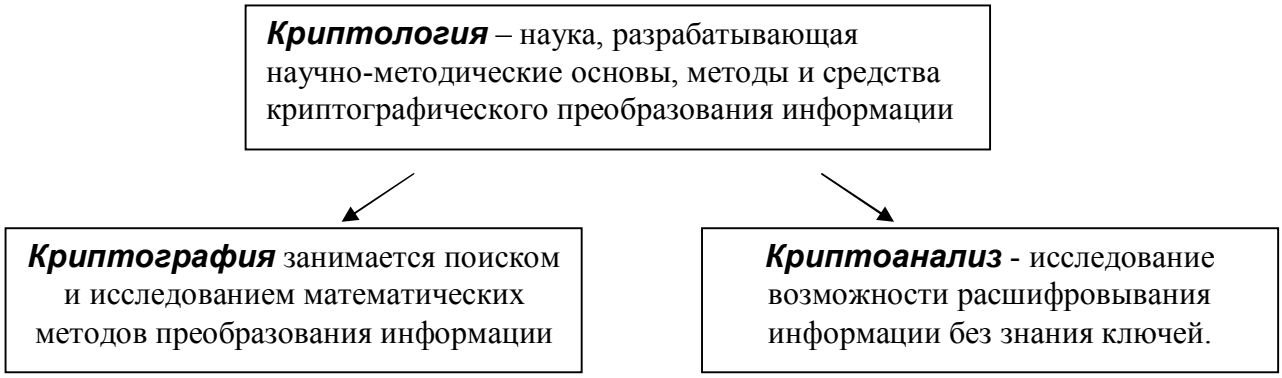
3. Нейтрализация угроз предусматривает применение средств устранения и ликвидации угроз, частичной или полной их нейтрализации в случае проникновения на объект либо диверсии

- **Борьба с компьютерными вирусами**
  - обнаружение вирусов (использование сканирования, нахождение изменений с помощью программ-ревизоров, программные антивирусные средства)
  - профилактика заражения вирусами (использование официального программного обеспечения, дублирование информации, антивирусные средства, программы-сканеры, проверка сменных носителей)
  - удаление и ликвидация последствий (восстановление системы, восстановление загрузочных файлов, создание резервных копий, использование дистрибутивов)

- **Защита хранения и обработки информации в базах данных**
  - Блокировка ответа (при неправильном числе запросов - отказ)
  - Коррекция и искажение ответа (путём округления, незначительного изменения ответа)
  - Случайный выбор записи для обработки (не позволяет отследить множество запросов)
  - Контекстно-ориентированная защита (назначение атрибутов доступа)
  - Контроль поступающих запросов (анализ попыток выявляет каналы)

- **Комплексные организационно-технические методы и средства устранения и нейтрализации угроз**
  - Применение современных технологий программирования
  - Организация защиты аппаратных средств на этапах разработки
  - Применение стандартных модулей

Тема 3. Криптографические методы и средства защиты информации



Основные понятия и определения криптографии

Алфавит - конечное множество используемых для кодирования информации знаков. В качестве примеров алфавитов, используемых в современных ИС, можно привести следующие:

алфавит Z_{33}-32 буквы русского алфавита и пробел;
алфавит Z_{256}-символы, входящие в стандартные коды ASCII и КОИ-8;
бинарный алфавит-Z_2=(0,1);
восьмеричный или шестнадцатеричный алфавит.

Текст - упорядоченный набор из элементов алфавита.

Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

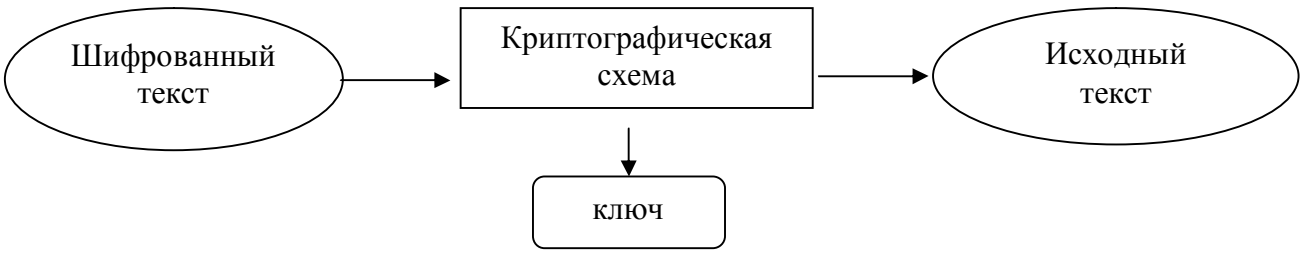


Рисунок 5. Процедура шифрования текста

Дешифрование – процесс, обратный шифрованию. На основе ключа шифрованный текст преобразуется в исходный.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрирования текстов.

Криптографическая система представляет собой семейство T преобразований открытого текста. Члены этого семейства индексируются или обозначаются символом k; параметр k является ключом.

Пространство ключей K – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы подразделяют на симметричные и с открытым ключом.

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

В ***системах с открытым*** ключом используют два ключа – *открытый и закрытый*, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины ***"распределение ключей"*** и ***"управление ключами"*** относятся к процессам системы обработки информации, содержанием которых являются составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другими пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

- количество всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищённость и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Современная криптография включает в себя **четыре крупных раздела**:

- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- системы электронной подписи;
- управление ключами.

Основными направлениями использования криптографических методов являются: передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

3.1 Симметричные криптосистемы

Классификация методов криптографического закрытия

1. <u>Шифрование</u> – вид криптографического закрытия, при котором преобразуется каждый символ

- Замена (подстановка) – замена одного символа на другой
  (простая, многоалфавитная, монофоническая)
- Перестановка – несложный метод, использующийся в сочетании с другими
  (простая, усложнённая)
- Аналитическое преобразование – использование алгебры матриц по особым зависимостям
- Гаммирование – наложение на исходный текст некоторой случайной последовательности (с конечной короткой и длинной гаммой, с бесконечной гаммой)
- Комбинированные методы – сочетание разных методов
  Используются в блочных шифрах.
  К определённому блоку текста применяется определённый метод.
  Замена и перестановка
  Замена и гаммирование
  Перестановка и гаммирование
  Гаммирование и гаммирование

<u>2. Кодирование</u> – вид криптографического закрытия, когда некоторые элементы защищаемых данных заменяются заранее выбранными кодами

- Смысловое – по специальным таблицам
  (элементы имеют вполне определённый смысл)
- Символьное – по кодовому алфавиту (кодируется каждый символ)

3. <u>Другие виды</u>

- Рассечение-разнесение – массив делится на элементы, каждый из которых, по отдельности, не позволяет раскрыть содержание защищаемой информации
- Сжатие-расширение

1. Шифрование

1.1 Шифрование методом замены (подстановка)

Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов.

Самой простой разновидностью является ***прямая*** (простая) замена, когда буквы шифруемого сообщения заменяются другими буквами того же самого или другого алфавита (смотреть рисунок 6).

Исходные символы шифруемого текста	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Заменяющие символы	S	P	X	L	R	Z	I	M	A	Y	E	D	W	T	B	G	V	N	J	O	C	F	H	Q	U	K

Рисунок 6. Таблица простой замены

При ***полиалфавитной подстановке*** для замены символов исходного текста используется несколько алфавитов.

Другой разновидностью метода замены является ***схема шифрования Вижинера***.

Она представляют собой квадратную матрицу с n^2 элементами, где n – число символов используемого алфавита. Каждая строка получена циклическим сдвигом алфавита на один символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования. При этом из полной таблицы выбирается первая и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается первая строка, а под нее – строки, соответствующие буквам ключа в порядке следования этих букв в ключе (смотреть рисунок 7).

Исходный текст - **безопасность**

а	**б**	**в**	**г**	**д**	**е**	**ё**	**ж**	**з**	**и**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ь**	**ы**	**ъ**	**э**	**ю**	**я**
и	**й**	к	л	м	н	о	п	р	с	т	у	ф	х	ц	**ч**	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ё	ж	з
н	о	п	р	с	**т**	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	**я**	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м
т	у	ф	х	ц	ч	ш	щ	**ь**	ы	ъ	э	ю	я	а	б	в	г	д	**е**	ё	ж	з	и	й	к	л	м	н	о	п	р	с
е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	**у**	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	**я**	а	б	в	г	д
г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	**т**	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	**щ**	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к

Ключ: **интеграл**

шифротекст - **йтьутрсщчяея**

Рисунок 7. Шифрование по таблице Вижинера

1.2 Шифрование методами перестановки

Этот вид шифрования подразумевает, что символы шифруемого текста внутри шифруемого блока символов переставляются по определенным правилам.

- **Метод простой перестановки**

Написать исходный текст задом наперёд и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО

Тогда шифрограмма, несмотря на столь незначительное изменение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке появятся серьезные неудобства.

- **Усложнённая перестановка по таблице**

Исходную фразу следует писать в несколько строк, например, по пятнадцать букв в каждой, дополнив последнюю строку свободно выбранными буквами.

Символы шифрования при усложненной замене по строкам

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
П	У	С	Т	Ь	Б	У	Д	Е	Т	Т	А	К	К	А
К	М	Ы	Х	О	Т	Е	Л	И	К	Л	М	Н	О	П

Затем вертикальные столбцы разбивают на пятерки букв и последовательно записывают в строку. Получают зашифрованный текст:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Другой вариант этого шифра предусматривает предварительную процедуру записи исходной фразы в столбцы

Символы шифрования при усложненной замене по столбцам

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
П	С	Ь	У	Е	Т	К	А	М	Х	Т	Л	А	В	Д
У	Т	Б	Д	Т	А	К	К	Ы	О	Е	И	Б	Г	Е

Затем строки разбивают на пятерки букв:

ПСЬУЕ ТКАМХ ТЛАВД УТБДТ ААЫО ЕИБГЕ

- **Матричный шифр перестановки**

Нужно укоротить строки, соответственно увеличив их количество в таблице. В результате получиться решетка, в которую записывают исходный текст.

П	У	С	Т	Ь
Б	У	Д	Е	Т
Т	А	К	К	А
К	М	Ы	Х	О
Т	Е	Л	И	А

В этом случае необходимо сформулировать условия для записи и дешифрования (длина и высота **(5x5)**).

Записывать текст в решетку можно по строкам, столбцам, прямой или обратной спирали, диагоналям, причем шифровать и дешифровать можно в различных направлениях.

В данном случае нужно переписать буквы по диагонали, а потом разбить на пятёрки.

Получится:

ПУБСУ ТТДАК ЬЕКМТ ТКЫЕА ХЛОИА

Нужно отметить, что в данном случае требуется предварительная договорённость между адресатом и отправителем по вопросу размера матрицы.

- **Перестановка символов с ключом**

Р	*А*	*Д*	*И*	*А*	*Т*	*О*	*Р*
6	**1**	**3**	**4**	**2**	**8**	**5**	**7**
П	У	С	Т	Ь	Б	У	Д
Е	Т	Т	А	К	К	А	К
М	Ы	Х	О	Т	Е	Л	И

В данном случае правила заполнения решетки и шифрования из нее упрощаются.

Единственное, что используется - это ключ, которым может быть любое слово.

Возьмем, например, слово РАДИАТОР. Применяем следующий алгоритм кодировки букв. По алфавиту буква А получает номер 1, вторая буква А-2, следующая по алфавиту буква Д -3, потом И-4, О-5, первая буква Р-6, вторая Р-7 и буква Т-8.

Переписываем столбики в соответствии с номерами букв ключа:

УТЫ ЬКТ СТХ ТАО УАЛ ПЕМ ДКИ БКЕ

1.3 Шифрование методом аналитических преобразований

Это умножение матрицы на вектор по следующему правилу:

$\overline{C} = A \times \overline{B}$ Матрица **A**=(a_{ij}) – в качестве ключа, Вектор **B**=(b_j) – символы шифруемого текста

C - символы зашифрованного текста

$$A = \begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix}$$

КЛЮЧ

Заменим буквы алфавита цифрами, соответствующим их порядковому номеру в алфавите: А=0, Б=1, В=2 и т.д. Тогда отрывку текста ВАТАЛА будет соответствовать последовательность чисел 2, 0, 19, 0, 12, 0.

По принятому алгоритму выполним действия:

$$\overline{C} = A \times \overline{B} = \begin{vmatrix} 14 & 8 & 5 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix} \text{ x } \begin{vmatrix} 2 \\ 0 \\ 19 \end{vmatrix} = \begin{vmatrix} 85 \\ 54 \\ 25 \end{vmatrix}$$

При этом зашифрованный текст будет иметь следующий вид:
85, 54, 25 96, 60, 24.

$$\overline{C} = A \times \overline{B} = \begin{vmatrix} 14 & 8 & 5 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix} \text{ x } \begin{vmatrix} 0 \\ 12 \\ 0 \end{vmatrix} = \begin{vmatrix} 96 \\ 60 \\ 24 \end{vmatrix}$$

$A_{ij} = (-1)^{i+j} \Delta_{ij,}$, где Δ_{ij} - определитель матрицы, получаемой вычеркиванием i-й строки и j-ого столбца исходной матрицы А.

$$A^{-1} \text{ x } C = \begin{vmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{vmatrix} \text{ x } \begin{vmatrix} 85 \\ 54 \\ 25 \end{vmatrix} = \begin{vmatrix} 1\bullet 85 - 2\bullet 54 + 1\bullet 25 \\ -2\bullet 85 + 5\bullet 54 - 4\bullet 25 \\ 1\bullet 85 - 4\bullet 54 + 6\bullet 25 \end{vmatrix} = \begin{vmatrix} 2 \\ 0 \\ 19 \end{vmatrix}$$

$$A^{-1} \text{ x } C = \begin{vmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{vmatrix} \text{ x } \begin{vmatrix} 94 \\ 60 \\ 24 \end{vmatrix} = \begin{vmatrix} 1\bullet 96 - 2\bullet 60 + 1\bullet 24 \\ -2\bullet 96 + 5\bullet 60 - 4\bullet 24 \\ 1\bullet 96 - 4\bullet 60 + 6\bullet 24 \end{vmatrix} = \begin{vmatrix} 0 \\ 12 \\ 0 \end{vmatrix}$$

1.4 Шифрование аддитивными методами (гаммирование)

Этот вид шифрования предусматривает последовательное сложение символов шифруемого текста с символами некоторой специальной последовательности, которая называется *гаммой*.

Существует два способа. При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю k, где k – число символов в алфавите, т.е.

$$R_i – (S_i + G) \text{mod}(k - 1)$$

где R_i, S_i, G – символы соответственно зашифрованного, исходного текста и гаммы.

При втором символы исходного текста представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю.

		Текст	
		0	1
Гамма	0	0	1
	1	1	0

	Б	У	Д	Ь ….
Шифруемый текст	010010	100000	10010	100000
Знаки гаммы	7	1	8	2 …..
	000111	000001	001000	000010
Шифрованный текст	010101	100001	111010	100010

1.5 Комбинированные методы шифрования

заключаются в применении различных способов шифрования одновременно или последовательно.

2. Кодирование

вид криптографического закрытия, при котором некоторые элементы защищаемых данных заменяются заранее выбранными кодами.

Символьное – кодируется каждый символ

A	1	1	1	1						
O	1	1	1	0						
N	1	1	0							
D	1	1	0	1	1					
P	1	1	0	1	0	1				
V	1	1	0	1	0	0	1			
K	1	1	0	1	0	0	0	1	1	
Q	1	1	0	1	0	0	0	1	0	1
Z	1	1	0	1	0	0	0	1	0	0
X	1	1	0	1	0	0	0	0	1	
J	1	1	0	1	0	0	0	0	0	
R	1	0	1	1						
I	1	0	1	0						
E	1	0	0							
S	0	1	1	0						
W	0	1	1	1	0	1				
B	0	1	1	1	0	0				
H	0	1	0	1						
F	0	1	0	0	1					
C	0	1	0	0	0					
M	0	0	0	1	1					
U	0	0	0	1	0					
G	0	0	0	0	1					
Y	0	0	0	0	0					

Рисунок 8. Коды Хаффмена

Смысловое – элементы имеют вполне определённый смысл

Например:

Автоматизированные системы управления 001
Автоматизация управления 002
Осуществляет 415
Позволяет 632

3. Другие виды криптографического преобразования

К ним относятся рассечение-разнесение и сжатие данных. Рассечение-разнесение данных состоит в том, что массив делится на элементы, каждый из которых, по отдельности, не позволяет раскрыть содержание защищаемой информации, и выделенные таким образом элементы размещаются в различных зонах ЗУ. Обратная процедура называется сборкой данных.

3.2 Системы с открытыми ключами

В системах с открытым ключом используют ***два ключа*** - открытый и закрытый, которые математически связаны друг с другом.

СУТЬ процесса: информация шифруется с помощью ***открытого ключа***, который доступен всем желающим, а расшифровывается с помощью ***закрытого ключа***, известного только получателю сообщения (смотреть рисунок 9).

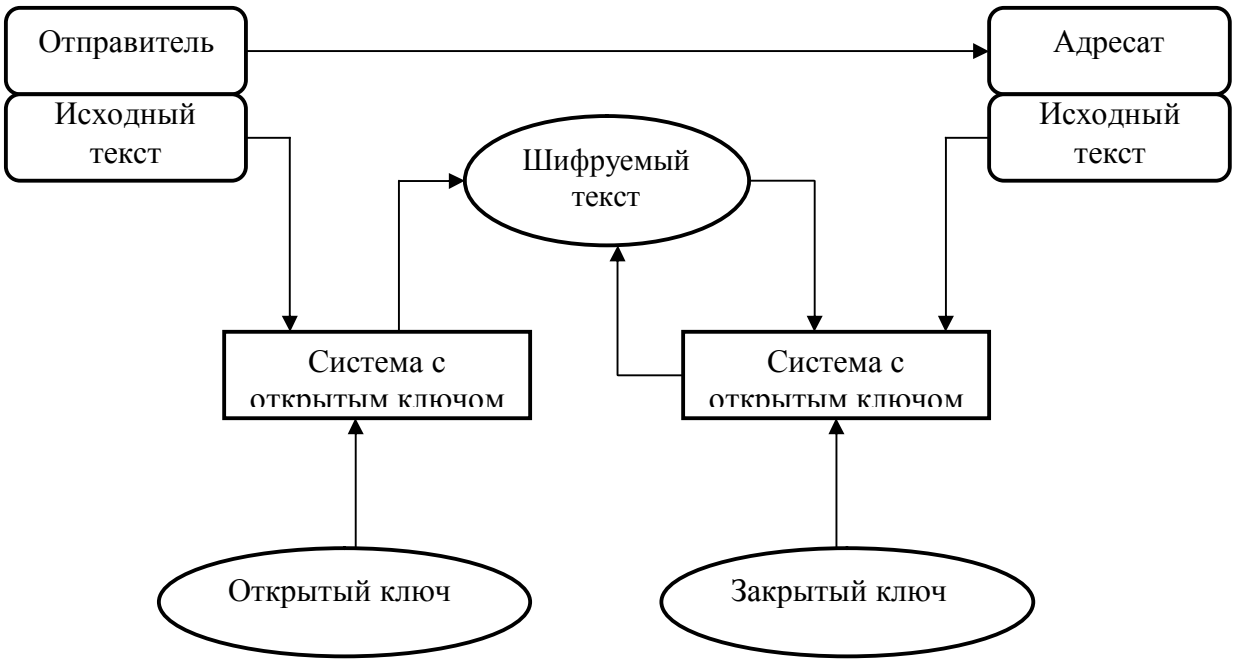


Рисунок 9. Схема шифрования с открытым ключом

В этих криптографических системах используются необратимые, односторонние функции.

Под ***необратимостью*** понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Например: по произведению множителей невозможно вычислить сами множители.

Очевидные требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.
2. Определение закрытого ключа на основе открытого также должно быть невозможным при современном уровне развития технологии.

Типы необратимых преобразований:

- разложение больших чисел на простые множители;
- вычисление логарифма в конечном поле;
- вычисление корней алгебраических уравнений.

Назначения криптосистем СОК:

1. Как самостоятельные средства защиты передаваемых и хранимых данных;
2. Средства для распределения ключей;
3. Средства аутентификации пользователей (электронная подпись).

Алгоритм шифрования **RSA** является мировым стандартом для открытых систем.

3.3 Электронная (цифровая) подпись

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Впервые идея цифровой подписи как законного средства подтверждения подлинности авторства электронного документа была предложена в работе Диффи и Хеллмана в 1976 году.

При передаче сообщения по линиям связи или хранении его в памяти должны быть обеспечены вместе или по отдельности следующие требования:

1. Соблюдение конфиденциальности сообщения - злоумышленник не должен иметь возможности узнать содержание передаваемого (или хранимого) сообщения.
2. Удостоверение в подлинности полученного (или считанного из памяти) сообщения, которая включает в себя два понятия:

- *целостность* - сообщение должно быть защищено от случайного или умышленного изменения по пути его следования (или во время хранения в памяти);
- *идентификация* отправителя (проверка авторства) - получатель должен иметь возможность проверить, кем отправлено (или составлено) сообщение.

3.4 Организация протоколирования связи и распределения ключей

Большие трудности возникают при формировании механизмов распределения ключей криптографического преобразования. Одним из принципов, которого придерживаются специалисты, является несекретность используемого способа закрытия. Предполагается. Что необходимая защита обеспечивается за счёт сохранения в тайне ключей. Отсюда следует принципиальная важность формирования протоколов ключей, их распределения и доставки. Здесь существенными являются следующие соображения:

- ключи должны выбираться случайно;
- выбранные ключи должны распределяться таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю;
- механизм распределения ключей должен обеспечивать тайну ключей на всех этапах функционирования системы;
- должна быть предусмотрена достаточно частая смена ключей, причём частота их изменения должна определяться двумя факторами: временем действия и объемом закрытой с их использованием информации.

Таким образом, в жизни, используемые в системе ключи, подразделяются на ключи для шифрования данных и ключи для шифрования ключей. Последние должны быть устойчивыми и для их генерации используют случайные процессы.

Программно-аппаратная реализация криптографических средств и систем

Программно-аппаратная реализация криптографических средств в мире основывается на стандартах DES (Data Encryption Standart 1974 год) и ГОСТ 28147-89.
Это широко известные алгоритмы блочного шифрования, принятые в качестве государственных стандартов в США и России.

Тема 4. Компьютерные вирусы и антивирусные программы

4.1 Компьютерные вирусы

Компьютерным вирусом называется специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.

Массовое применение персональных компьютеров, к сожалению, связано с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации. Проникнув в один компьютер, вирус способен распространиться на другие компьютеры.

Основными путями проникновения вирусов в компьютер являются съемные диски, а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке компьютера с дискеты, содержащей вирус. На дискету вирус может попасть, например, при считывании ее оглавления на зараженном компьютере.

После запуска программы, содержащей вирус, возможно заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширение EXE, COM, SYS, или BAT. Крайне редко заражаются текстовые и графические файлы.

При заражении компьютера вирусом очень важно своевременно его обнаружить. Для этого следует знать об **основных признаках проявления вирусов**. К ним можно отнести следующие:

- прекращение работы или неправильная работа раннее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Следует заметить, что перечисленные явления необязательно вызываются наличием вируса, а могут быть следствием других причин.

4.2 Основные виды вирусов

Компьютерные вирусы – это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения в КС

Основные классы вирусов

По среде обитания:	сетевые	распространяются по компьютерной сети.
	файловые	внедряются в выполняемые файлы и активизируются при запуске. Лечение затруднено т.к. они резидентные (в ОП).
	загрузочные	внедряются в загрузочный сектор диска (Boot-сектор). Принцип действия основан на алгоритмах запуска и перезагрузки ОС.
По способу заражения:	резидентные	после включения ПК перемещаются из среды обитания в оперативную память ЭВМ, используют привилегированные режимы работы в ОС.
	нерезидентные	попадают в оперативную память только на время активности заражения, а затем покидают, оставаясь в среде обитания.
По степени опасности:	безвредные	не наносят особенного ущерба.
	неопасные	уменьшают свободную память, создают звуковые, графические и прочие эффекты.
	опасные	могут привести к серьезным сбоям в работе.
	очень опасные	могут привести к потере программ или системных данных, форматируют диски, шифруют данные, разрушают электронные устройства.
По особенностям алгоритма вируса:	вирусы-«спутники»	не изменяют файлы, создают для EXE-файлов файлы-спутники с расширением COM.
	«черви»	распространяются по сети, рассылают свои копии, вычисляя сетевые адреса.
	«паразитические»	изменяют содержимое дисковых секторов или файлов.
	«студенческие»	примитив, содержат большое количество ошибок.
	«стелс»-вирусы (невидимки)	перехватывают обращения DOS к пораженным файлам или секторам и подставляют вместо себя незараженные участки.
	вирусы-призраки (полиморфные)	не имеют ни одного постоянного участка кода, труднообнаруживаемы, основное тело вируса зашифровано.
	макровирусы	Пишутся не в машинных кодах, а на WordBasic, переписывают себя в Normal.dot. Ограниченно резидентные. Заражают документы пока открыто приложение.
	троянские	Выполняют несанкционированную пользователем передачу управления компьютером удалённому пользователю.

4.3 Методы и технологии борьбы с компьютерными вирусами

Для защиты от вирусов используют:

- Общие средства защиты (копирование, разграничение доступа)
- Профилактику
- Специализированные программы защиты

Антивирусные средства применяются для решения задач (смотреть рисунок 10):

- Обнаружение вируса в КС (на стадии внедрения)
- Блокирование работы программ-вирусов
- Устранение последствий воздействия вирусов (удаление, восстановление).

Методы обнаружения

1. ***Сканирование*** – самый простой. Программа-сканер просматривает файлы в поисках сигнатур (опознавательной части вирусов).
2. ***Обнаружение изменений*** – базируется на использовании программ-ревизоров. Эти программы определяют и запоминают характеристики всех областей на дисках и сравнивают их с текущими.
3. ***Эвристический анализ*** – позволяет определить неизвестные вирусы, не требует предварительного сбора информации. Сущность: проверка возможных сред обитания и выявление в них команд, характерных для вирусов.
4. ***Использование резидентных сторожей*** – основан на применении программ, которые постоянно находятся в оперативной памяти и отслеживают все действия остальных программ. Недостаток – значительный % ложных тревог.
5. ***Вакцинация программ –*** создание специального модуля для контроля целостности. В качестве характеристики – контрольная сумма. Достоинство - обнаруживают все вирусы, кроме «стелс-вирусов».
6. ***Применение программно-аппаратных антивирусных средств –*** в настоящее время используют специальные контроллеры и программное обеспечение. Контроллер устанавливается в разъём и имеет доступ к общей шине. Достоинство – работают постоянно, блокируют неразрешённые действия. Недостаток – зависят от аппаратных средств ЭВМ.

Методы удаления последствий

Первый метод предполагает восстановление системы после воздействия *известных* вирусов. Разработчики программы, удаляющей вирус, должны знать структуру вируса и его характеристики размещения.

Второй метод позволяет восстанавливать файлы и загрузочные сектора, зараженные *неизвестными* вирусами. Для этого программа восстановления должна заблаговременно создать и хранить информацию о файлах, полученную в условиях отсутствия вирусов.

Если изменения необратимы, то восстановление возможно только при использовании резервной копии или дистрибутива.

В крайнем случае – переустановка Операционной системы.

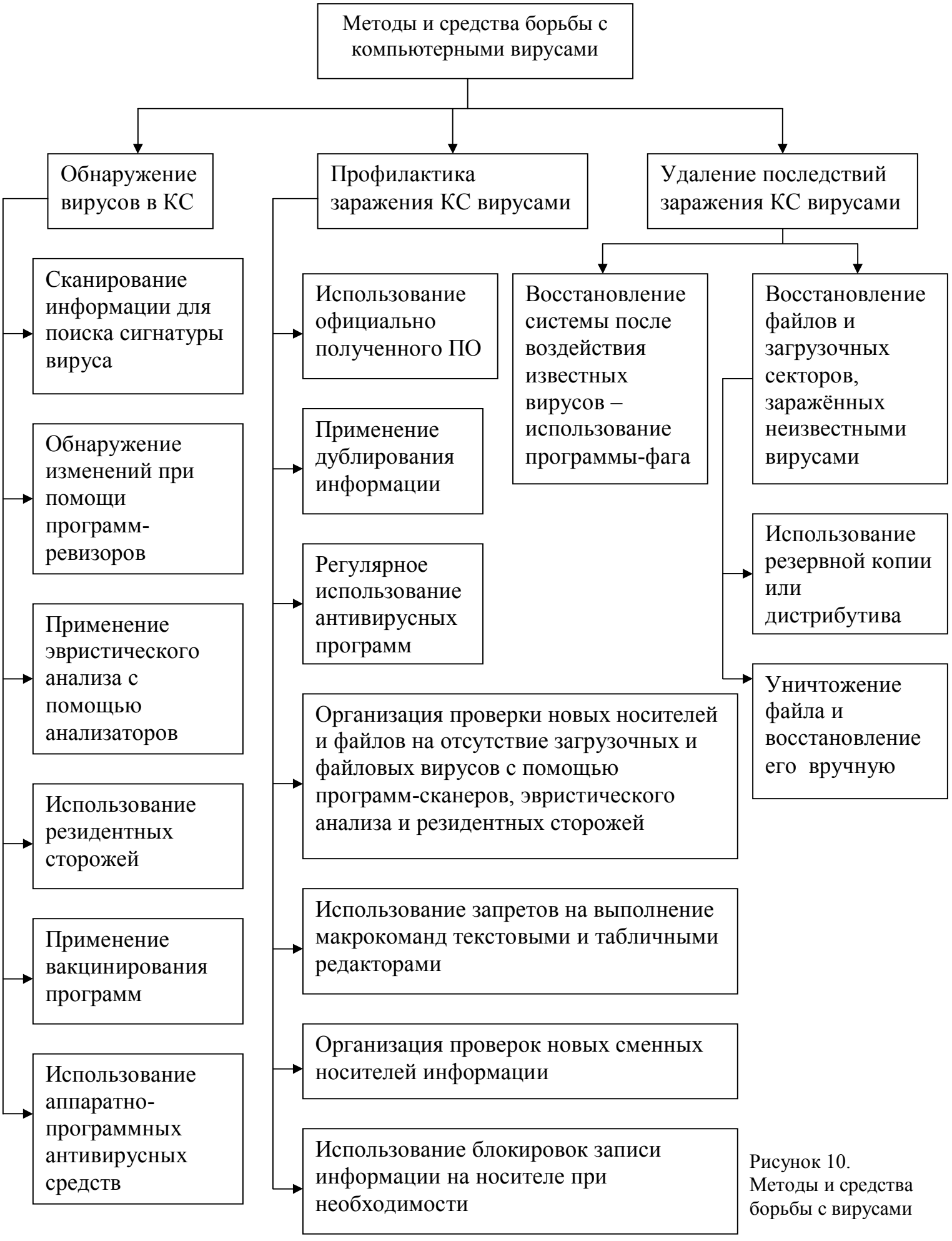


Рисунок 10. Методы и средства борьбы с вирусами

4.4 Виды антивирусных программ

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называют антивирусными.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение вирусов позволяют избежать распространения эпидемии на другие компьютеры.

Программы-детекторы – осуществляют поиск характерного для конкретного вируса кода (сигнатуры) в оперативной памяти и файлах. При обнаружении вируса они выдают соответствующее сообщение.

Недостаток: находят только вирусы, известные разработчикам.

Программы-доктора – или фаги, а также ***программы-вакцины*** не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние.

В них находится эвристический анализатор – набор подпрограмм, анализирующих код исполняемых файлов для обнаружения вирусов. Основная часть его – эмулятор кода, задача которого не выполнять код, а выявлять в нём события (действия программ). Если действия укладываются в определённую схему – то это вирус. Doctor Web – наиболее мощный анализатор.

Программы-ревизоры – запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражён вирусом, а затем периодически сравнивают текущее состояние с исходным состоянием. Обнаруженные изменения выводятся на экран монитора.

Достоинство: обнаруживают вирусы всех типов.

Недостаток: лечат только те файлы, которые не были заражены до начальной проверки.

Программы-фильтры или «сторожа» - представляют собой небольшие программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов, и сообщают об этом пользователю.

Тема 5. Защита информации в ПК

Определяющее влияние оказывают следующие факторы

1) Цели защиты
2) Способы защиты
3) Средства защиты

Основные цели защиты

- ***Обеспечение физической целостности***

Целостность дискет, информации на дисках

- ***Обеспечение логической целостности***

Малоактуально

- ***Предупреждение несанкционированного получения***

Актуальна в случаях, когда информация содержит государственную и коммерческую тайну.

- ***Предупреждение несанкционированной модификации***

Разновидностью модификации является действие вредоносных программ.

- ***Предупреждение несанкционированного копирования***

Актуальность определяется тем, что массивы информации становятся товаром, торговля компьютерными программами, наличие дисководов способствует.

Основные механизмы защиты ПК от несанкционированного доступа

1. Физическая защита ПК и носителей информации.
2. Опознавание (аутентификация) пользователей и используемых компонентов обработки информации.
3. Разграничение доступа к элементам защищаемой информации.
4. Криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных).
5. Регистрация всех обращений к защищаемой информации.

1. Физическая защита

ПК необходимо размещать надёжно запираемом помещении. ПК должен быть под наблюдением пользователя. При обработке закрытой информации в помещении должны быть только допущенные.

2. Опознавание (аутентификация) пользователей и используемых компонентов

Система должна определять законность каждого обращения к ресурсам, а законный пользователь должен убедиться, что ему предоставляются именно те компоненты, которые ему необходимы.

Для опознавания пользователей

Следующие способы:

1) *С использованием простого пароля*

Каждому зарегистрированному пользователю выдается персональный пароль, который он должен держать в тайне и вводить при каждом обращении к ПК. Специальная программа сравнивает его с эталоном, хранящимся в ЗУ ПК.

Недостаток: пароль м/б утерян, подобран, можно проникнуть к ту область ЗУ где хранятся эталоны

2) *В диалоговом режиме с использованием нескольких паролей и/или персональной информации пользователя*

В файлах механизмов защиты создаются записи, содержащие персонифицирующие данные пользователя (рост, имена и даты рождения и т.д.) или набор паролей. Каждый раз разные вопросы.

3) *По индивидуальным особенностям человека (отпечатки пальцев, геометрия руки, голос, персональная роспись, структура сетчатки глаз, фотография и т.д.)*

Весьма надёжно, но требует специальной аппаратуры. Заманчивым по простоте является опознавание пользователя по его параметрам работы на клавиатуре ПК (скорость, интервалы между нажатием клавиш).

4) *С использованием радиокодовых устройств*

Изготавливаются специальные устройства, генерирующие радиосигналы, имеющие индивидуальные характеристики. ПК улавливает

Недостаток: устройство может быть похищено.

5) *С использованием электронных карточек*

Изготавливаются карточки, на которые наносятся данные, персонифицирующие пользователя (код, шифр).

Для опознавания компонентов

Следующие средства:

1) *Специальные аппаратные блоки-приставки (для опознавания ЭВМ, терминалов и ВУ)*

Технические устройства оснащаются специальными устройствами, генерирующими индивидуальные сигналы. Они могут быть зашифрованными.

2) *Специальные программы, реализующие процедуру «запрос-ответ»*

Заранее в ЗУ вносятся массивы данных, которые запрашиваются и сравниваются с соответствующими данными из своего массива.

3) Контрольные суммы (для опознавания программ и массивов данных)
Для программ и массивов заблаговременно вычисляются контрольные суммы, зависящие от содержания объектов.

3. Разграничение доступа к элементам защищаемой информации
Заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможность беспрепятственного доступа к информации в пределах его полномочий и исключить повышение его полномочий.
Само разграничение осуществляется несколькими способами:

1) По уровням (кольцам) секретности
Защищаемые данные распределяются по массивам (базам) таким образом, чтобы в каждом массиве содержались только данные одного уровня секретности (только «конфиденциально или только «секретно»). Каждому пользователю предоставляется только определённый уровень доступа.

2) По специальным спискам
Для каждого элемента защищаемых данных составляется список всех пользователей, которым предоставлен доступ к этому элементу или список элементов, для каждого зарегистрированного пользователя.

3) По матрицам полномочий
Предполагает формирование двумерной матрицы, по строкам которой идентификаторы зарегистрированных пользователей, по столбцам идентификаторы защищаемых элементов данных.

	Каталог D:\WORK	Каталог D:\BOOK	Каталог D:\TEST
Пользователь WER9	10	01	10
Пользователь YUI3	00	10	11

00 - доступ запрещён;
01 – разрешено чтение;
10 – разрешена запись;
11 – разрешена и запись и чтение.

4) По специальным мандатам
Каждому защищаемому элементу присваивается уникальная персональная метка, которую выдает администратор защиты или владелец элемента.

4. Криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных)

Для информации, долговременно хранящейся в ЗУ и для одновременного уменьшения объёмов. Классический пример – Коды Хаффмена, где для кодирования часто встречающихся символов используются короткие кодовые комбинации, а, для редко встречающихся, длинные.

Серия криптографических устройств **КРИПТОН** – это ряд выполненных в виде одноплатных устройств программно-аппартных комплексов, обеспечивающий шифрование и дешифрование информации в ЭВМ и сетях позволяет осуществлять:

- Шифрование и дешифрование файлов
- Разграничение и контроль доступа
- Защиту информации, передаваемой по открытым каналам связи и сетям
- Электронную подпись документов
- Прозрачное шифрование жестких и гибких дисков

Для криптографического преобразования использован алгоритм отечественного стандарта ГОСТ 28147 – 89. Длина ключа – 256 бит, причем предусмотрено 7 типов ключевых систем, по усмотрению. КРИПТОН работает в среде DOS и выше.

Н его базе разработана система **КРИПТОНИК**, обеспечивающая чтение, запись и защиту данных хранящихся в идентификационных карточках.

5. Регистрация всех обращений к защищаемой информации

Для решения задач:

- Контроль использования защищаемой информации
- Выявление попыток несанкционированного доступа
- Накопление статистических данных

Наиболее распространённая система защиты информации «Снег – 2.0». Система состоит из подсистем управления доступом, регистрации и учета и криптографической.

Общие положения по применению системы «Снег 2.0»

Предназначен для применения в ПК IBM PC/AT с ОС MS DOS/ Система «Снег» обеспечивает конфиденциальность и защиту от НСД к информации В ПК до уровня «Совершенно секретно». Но предприятие обязано обеспечить:

1) введение и организацию работы службы безопасности информации;
2) ведение журнала учёта работы ПК;
3) организацию учета носителей информации;
4) обеспечение физической сохранности оборудования;
5) исключение возможности загрузки ОС с дискет пользователя при помощи специальной платы КРИПТОН-3, опечатывания корпуса ПК и контроля сохранности печатей;
6) запрещение доступа пользователей к программам, имеющим доступ к оперативной памяти.
7) обеспечение уникальности ключевых дискет (по группам пользователей и т.д.)

Защита информации от копирования

Это предупреждение снятия информации из ОЗУ или на МД. Для защиты авторских и коммерческих интересов.

В настоящее время используются общесистемные и специализированные программные средства.

К ***общесистемным*** относится утилита Setup, входящая в состав BIOS и предназначенная для настройки аппаратных параметров компьютера.

Необходимо установить:

- Порядок загрузки ОС, задающий первичную загрузку жесткого диска
- Запрос пароля перед загрузкой ОС

Недостаток: защита может быть преодолена путем принудительного обнуления содержимого энергонезависимой памяти компьютера (CMOS-памяти) после вскрытия его корпуса.

К ***специализированным*** относится система «Кобра»

- Ввод пароля с клавиатуры
- Ввод пароля с дискеты
- Вход в систему при условии раздельного ввода независимыми субъектами разных паролей

Каждый следующий уровень является мощнее предыдущего.
При вводе пароля с клавиатуры его длина может достигать 64 символа. Т.к. пароль должен быть нетривиальным и длинным, то запоминание проблематично. Поэтому «Кобра» позволяет записать его на дискету и использовать дискету в дальнейшем как электронный аутентификатор. Кроме этого система позволяет создать ключевую дискету, без которой невозможна загрузка ОС. В этом случае появляется возможность организации входа в компьютер только при условии раздельного ввода двух разных паролей – пароля, хранящегося на ключевой дискете, и пароля, используемого для подтверждения подлинности.

Защита от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы
Хранитель экрана: недостаток в том, что отсутствует возможность принудительной блокировки клавиатуры, экрана и мыши без завершения сеанса работы.
В «Кобре» обеспечивается эта возможность.

Защита в среде MS-DOS
Защиту от НСД при его оставлении можно осуществить с помощью утилиты Discreet, входящей в состав пакета Norton Utility 7-ой или 8-ой версии. Для этого необходимо:

- Подключить драйвер Discreet.sys и включить в файл Config.sys строку DEVICE = d:\path\DISKREET.SYS, где d и path – соответственно логический привод и путь файла Discreet.sys;
- Перезагрузить ОС;
- Запустить утилиту Diskreet.exe;
- Нажатием клавиши F10 войти в меню, выбрать пункт **Options** и ввести команду Driver. Раскрыть список «Hot key» с помощью комбинации клавиш <Ctrl+!> и выбрать комбинацию клавиш для блокирования клавиатуры, мыши и экрана; установить нажатием клавиши пробела флажок **Keyboard**/Screen Lock и нажать Ok.
- Использую команду Master Password из пункта меню Options, ввести главный пароль и выйти из утилиты.

При забывании главного пароля единственным выходом является удаление файла Diskreet.ini. Когда данный файл отсутствует, считается, что главный пароль не установлен.

Защита в среде Windows

В окне «Свойства: экран» на закладке **Заставка** выбрать хранитель экрана и установить флажок **Пароль**.

Защита ПК от вредоносных закладок

К основным разновидностям относятся:

- воздействие на информацию (уничтожение, искажение, модификация);
- воздействие на систему (вывод из строя, ложное инициирование действия, модификация выполняемых функций, создание помех в работе).

Известные сейчас закладки осуществляются программным и аппаратным путём.

Аппаратные могут быть осуществлены в процессе изготовления ПК, ремонта или проведения профилактических работ. Особая опасность в том, что они длительное время могут себя не проявлять.

Программные закладки (РПС) представляются особо опасными в силу простоты их осуществления, высокой динамичности распространения и повышенной трудности защиты. В отличие от аппаратных, которые обнаруживаются в результате плановых проверок, эти могут появиться в любое время, чему способствуют: флэшки, копирование, подключение к сети.

Принципиальные подходы и общая схема защиты

Основу составляют следующие функции:

1) Создание условий, при которых дестабилизирующие факторы не могут появляться;
2) Предупреждение появления;
3) Обнаружение появления;
4) Предупреждение воздействия на информацию;
5) Обнаружение негативного воздействия на информацию;
6) Локализация негативного воздействия на информацию;
7) Ликвидация последствий воздействия.

Методы и средства защиты

Методы: анализа, синтеза, организационно-правовые, программные и аппаратные.

Средства:

Юридические – сводятся к установлению ответственности. На Западе эти нормы разработаны гораздо лучше, чем в России.

Организационно-административная защита – заключается в выработке и осуществлении организационно-технических мероприятий, направленных на предупреждение, обнаружение и ликвидацию последствий.

Из *аппаратных* средств рекомендуются:

1) Форматирование диска;
2) Физическая блокировка ключом клавиатуры ЭВМ;
3) Запрет и регистрация попыток записи в файлы ОС в области памяти, занятые системной информацией.

А антивирусные программы делятся на 4 класса

- класс А – предупреждение заражения;
- класс Б – выявление последствий заражения;
- класс В – минимизация причиненного ущерба;
- класс Г – общего характера.

Тема 6. Технические средства и комплексное обеспечение безопасности

Комплексный подход основан на интеграции различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

Современный комплекс защиты должен включать:

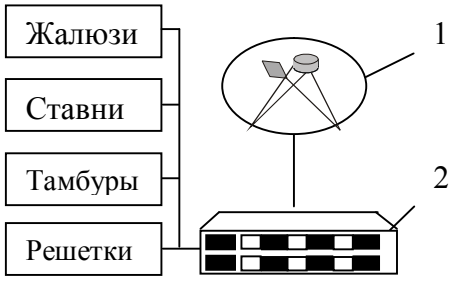
- Механическую систему защиты
- Управление доступом
- Систему оповещения о попытках проникновения
- Отображения и оценки обстановки
- Оборонительную систему
- Связную инфраструктуру
- Центральный пост охраны
- Персонал охраны

1. Механические системы защиты

Реальное физическое препятствие.

Это стены, ограды, колючая проволока, а также средства контроля доступа.

(смотреть рисунки 11, 12)



1 — приемопередатчик
2 — контроллер

Рисунок 11. Функциональная схема механической системы защиты объекта

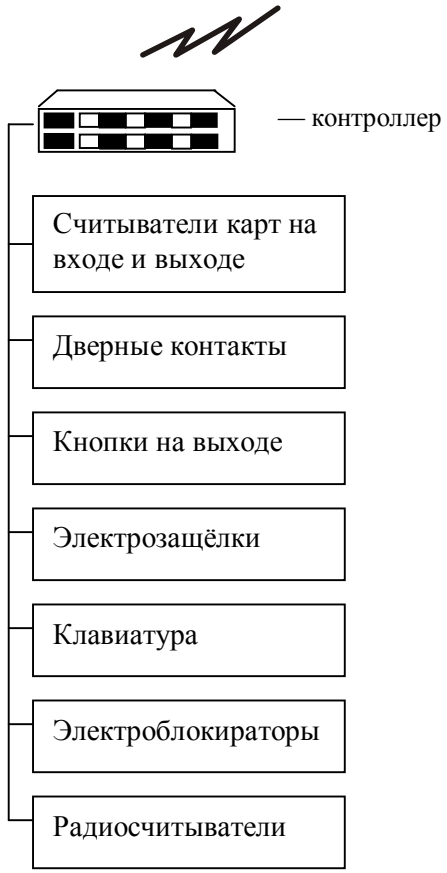


Рисунок 12. Структурная схема управления доступом

2. Системы оповещения (тревожный сигнал)

Здесь находят применение различные датчики (смотреть рисунок 13).

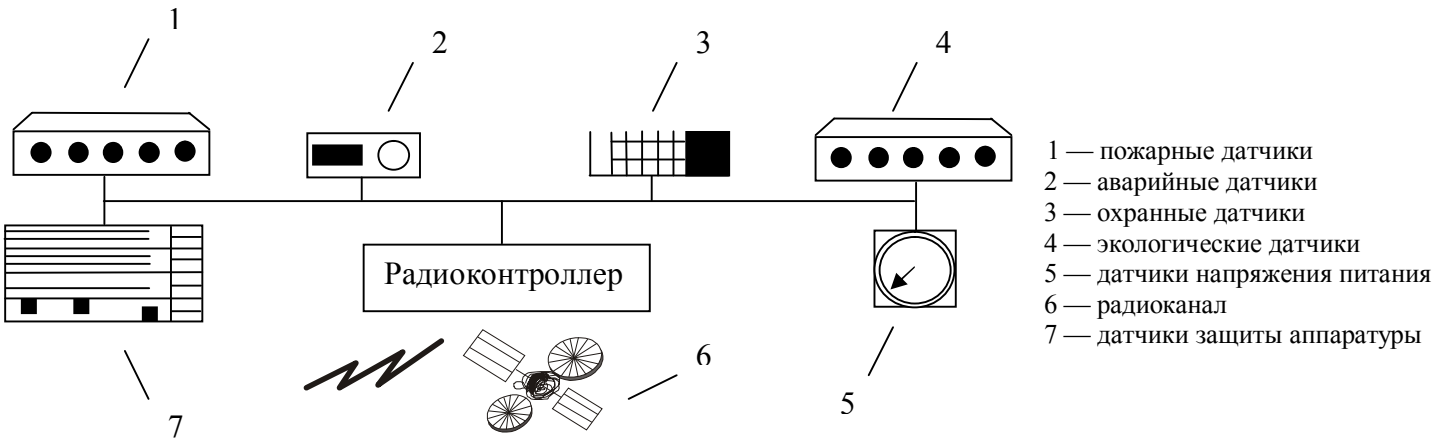


Рисунок 13. Функциональная схема аварийной, пожарной и охранной сигнализации системы

В системах защиты периметра без ограды применяются:

- ***Микроволновые***

  Действие основано на контроле интенсивности излучения датчика. Срабатывает при прерывании.
- ***Инфракрасные***

  Между передатчиком и приёмником монохромное световое излучение в невидимой области спектра. Срабатывает при прерывании.
- ***Емкостные***

  Работа основывается на формировании электростатического поля между параллельно расположенными передающими и принимающими проволочными элементами специального ограждения
- ***Электрические***

  Базируются на использовании специального ограждения с токопроводящими элементами
- ***Магнитные***

  Предполагают контроль параметров магнитного поля. Срабатывают при регистрации искажения поля.

При наличии механической защиты находят применение:

- ***Вибрационные датчики***

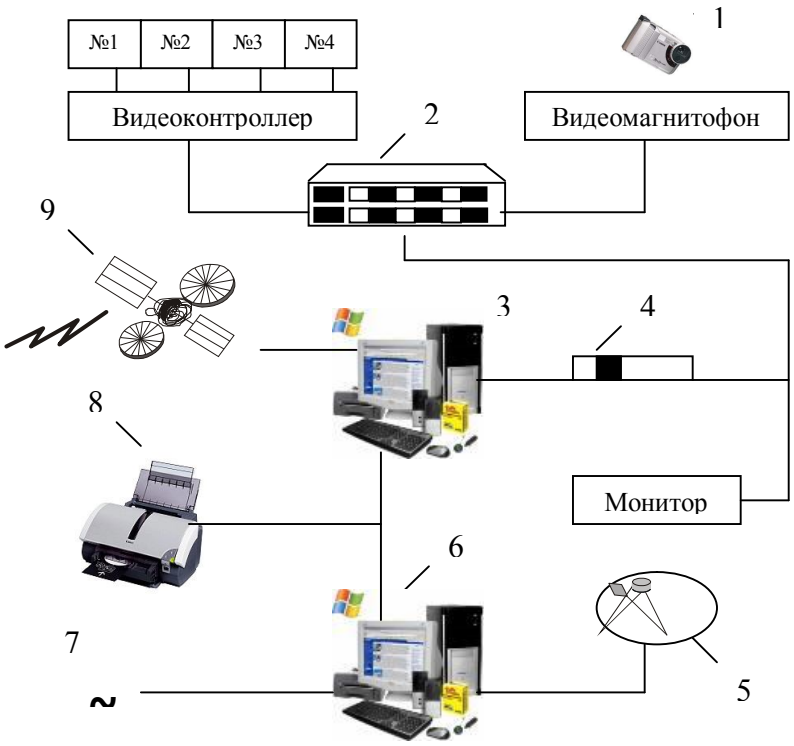
  Закрепляются непосредственно на ограде
- ***Звуковые***

  Закрепляются на ограде. Срабатывают при шумах прикосновения.
- ***Акустические***

  Контролируют звуковые колебания, передающиеся через воздух.

3. Системы опознавания

Телевизионные установки дистанционного наблюдения (смотреть рисунок 14)



1 — телевизионная камера, 2 — контроллер, 3 — рабочая станция,
4 — интерфейсный модуль, 5 — средства связи и управления,
6 — резервная рабочая станция, 7 — аварийное питание,
8 — принтер, 9 — радиоинтерфейс

Рисунок 14. Функциональная схема телевизионной системы опознавания нарушителей и центрального поста охраны объекта

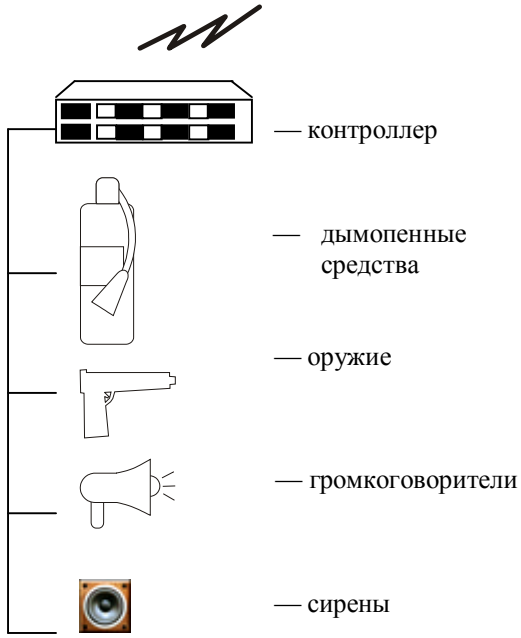


Рисунок 15. Функциональная схема оборонительной системы защиты

4. Оборонительные системы

Для предотвращения вторжения на охраняемую территорию (смотреть рисунок 15). Обнаруженный объект информируется, подаётся свет, звук, вызывается милиция.

5. Охранное освещение

2 вида: дежурное (предназначено для постоянного использования по всей охраняемой зоне), тревожное (включается вручную сотрудниками охраны при поступлении сигнала тревоги - прожектор 1000 Вт)

6. Центральный пост

К нему ведут каналы связи – специально проложенные линии связи, многожильные экранированные кабели, которые помещаются в пластмассовые трубы. Пост имеет возможность автоматического подключения к резервному энергоисточнику.

Примером комплексного решения охранной защиты и обеспечения контроля доступа является охранная система **МИККОМ AS 101**, которая представляет собой компьютеризированную автономную систему и предназначена для защиты от несанкционированного доступа в производственные и служебные помещения.

Тема 7. Организационно-правовое обеспечение ИБ

7.1 Отечественное организационное и нормативно-правовое обеспечение ИБ

Законодательные меры по защите процессов переработки информации заключаются в исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц – пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

Цель законодательных мер – предупреждение и сдерживание потенциальных нарушителей.

Основным документом, лежащим в основе информационной политики нашей страны является ***Доктрина информационной безопасности Российской Федерации***, в которой раскрыто содержание принципов, закреплённых в ***Федеральном законе «Об информации, информатизации и защите информации»*** от 25.01.95 № 24-ФЗ.

В Российской Федерации действуют девять государственных стандартов по защите информации: ГОСТ 28147-89, ГОСТ Р 34.10-94. ГОСТ Р 34.11-94, ГОСТ 29.339-92, ГОСТ Р 50752-95, ГОСТ РВ 50170-92, ГОСТ Р 50600-93, ГОСТ Р 50739-95, ГОСТ Р 50922-96. Они относятся к различным группам по классификатору стандартов и, к сожалению, не являются функционально полными.

Комплексный характер защиты процессов переработки информации достигается за счёт использования унифицированного алгоритмического обеспечения для средств криптографической защиты в соответствии с российскими государственными стандартами:

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма»;

ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

Проблема обеспечения безопасности носит комплексный характер. Для её решения необходимо сочетание, как правовых мер, так и организационных (где руководство должно выработать политику безопасности) и программно-технических (идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование).

7.2 Международные нормативно-правовые акты обеспечения ИБ

В международной практике обеспечения ИБ основными направлениями являются:

- нормирование компьютерной безопасности;
- стандартизация процессов создания безопасных информационных систем.

Ещё в 1983 году Агентством компьютерной безопасности Министерства обороны США был разработан стандарт "Trusted Computing System Evaluation Criteria" ***TCSEC*** ("Критерий оценки безопасности компьютерных систем"). Из-за цвета обложки он получил название *"Оранжевая книга"*. "Оранжевая книга" ранжировала компьютерные системы в соответствии со следующей шкалой:

D - Минимальная защита (ненормируемая)
C1, C2 - избирательное управление доступом
B1, B2, B3 - полное удовлетворение доступом
A1 - Гарантируемая защита

"Оранжевая книга" определяла для каждого раздела функциональные требования и требования гарантированности. Система должна была удовлетворять этим требованиям, чтобы соответствовать определенному уровню сертификации.

Для оценки компьютерных систем Министерства обороны США Национальный центр компьютерной безопасности МО США выпустил инструкции NCSC-TG-005 и NCSC-TG-011, известные как *«Красная книга»*.

В свою очередь, Агентство информационной безопасности ФРГ подготовило *"Зеленую книгу"*, где сделаны попытки разделить функциональные требования и требования гарантированности. В 1990г. «Зелёная книга» была одобрена ФРГ, Великобританией, Францией и Нидерландами и ЕС, где на её основе были подготовлены ITSEC (критерии оценки защищённости информационных технологий) или *«Белая Книга»*, как европейский стандарт, определяющий критерии, требования и процедуры для создания безопасных информационных систем, имеющий две схемы оценки: по эффективности и функциональности.

Согласно европейским критериям ITSEC информационная безопасность включает в себя шесть основных элементов детализации:

1) цели безопасности и функции ИБ;
2) спецификация функций безопасности;
3) конфиденциальность информации (защита от несанкционированного получения информации);
4) целостность информации (защита от несанкционированного изменения информации);
5) доступность информации (защита от несанкционированного или случайного удержания информации и ресурсов системы);
6) описание механизмов безопасности.

7.3 Организационное регулирование защиты процессов переработки информации

Законы и нормативные акты исполняются только в том случае, если они подкреплены организаторской деятельностью соответствующих структур, создаваемых в государстве, в ведомствах, учреждениях и организациях.

Организационные методы включают в себя меры, которые должны осуществлять должностные лица в процессе создания и эксплуатации КС для обеспечения заданного уровня ИБ.

В соответствии с законами и нормативными актами в организациях для защиты процессов переработки информации создаются специальные службы безопасности. Эти службы подчиняются руководству учреждения. Руководители служб организуют создание и функционирование систем защиты. Решаются следующие задачи:

- Организация работ по разработке системы защиты процессов переработки информации;
- Ограничение доступа на объект и к ресурсам КС;
- Разграничение доступа к ресурсам КС;
- Планирование мероприятий;
- Разработка документации;
- Воспитание и обучение обслуживающего персонала и пользователей;
- Сертификация средств защиты информации;
- Лицензирование деятельности по защите информации;
- Аттестация объектов защиты;
- Совершенствование системы защиты информации;
- Оценка эффективности функционирования системы защиты информации;
- Контроль выполнения установленных правил работы в КС.

Организационные методы являются стержнем комплексной защиты процессов переработки информации. Только с помощью них возможно объединение на правовой основе технических, программных и криптографических средств в единую комплексную систему.

Основными направлениями защиты информационной собственности является охрана государственной, коммерческой, служебной, банковской и интеллектуальной собственности, а также профессиональных тайн и данных.

Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Коммерческая тайна – это информация, которая имеет действительную или потенциальную коммерческую ценность, в силу её неизвестности третьим лицам, к которой нет свободного доступа на законном основании и к которой принимаются меры по охране конфиденциальности. Она охраняется при содействии государства.

Банковская тайна – это сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

К числу объектов ***интеллектуальной собственности*** относятся:
- произведения науки, литературы и искусства;
- результаты творчества;
- звукозаписи и изображения;
- передача радио- и телевизионных сигналов;
- профессиональные секреты;
- селекционные достижения;
- товарные знаки и знаки обслуживания;
- наименования мест происхождения товаров и т.д.

Профессиональная тайна – защищаемая по закону информация, доверенная или ставшая известной лицу, исключительно в силу исполнения им своих профессиональных обязанностей, распространение которой может нанести ущерб правам и законным интересам держателя или другого лица доверившего эти сведения.

Можно выделить следующие объекты профессиональной тайны:
Врачебная тайна – сведения о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе заболевания, сведения о наличии психического расстройства;
Нотариальная тайна – сведения, доверенные нотариусу;
Адвокатская тайна – сведения, сообщенные адвокату гражданином;
Тайна связи – тайна переписки, телефонных переговоров, почтовых, телеграфных сообщений;
Тайна усыновления – сведения об усыновлении ребёнка;
Тайна страхования – сведения о страхователе, застрахованном лице и выгодоприобретателе, а также об имущественном положении этих лиц;
Тайна исповеди – сведения, доверенные священнослужителю на исповеди;

Служебная тайна – это защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей. Для осуществления её правовой охраны и защиты необходим Закон РФ «О тайне» от 21.07.93 № 5485-1.

В Европе для охраны и защиты права на неприкосновенность частной жизни в условиях автоматизированной обработки личных данных о гражданах более 25 лет назад был введён *институт защиты персональных данных*. Во всех странах Европейского Союза с 1998 года создана единая унифицированная система защиты персональных данных, в том числе в секторе телекоммуникаций.

Федеральный закон «Об информации, информатизации и защите информации» от 25.01.95 № 24-ФЗ вводит понятие «персональные данные», относит их к конфиденциальной информации и устанавливает, что перечни персональных данных должны быть закреплены федеральных законом.

К ***персональным данным*** могут быть отнесены сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам.

7.4 Ответственность за нарушение законодательства в информационной сфере

В Уголовном кодексе Российской Федерации, введённом в действие 13.06.96, предусмотрена ответственность за не предоставление информации гражданам, палатам Федерального собрания РФ и Счётной палате РФ (ст.140 и 287), а также за сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст.237).

Защита права может осуществляться в *административном порядке* – через подачу жалобы и в *судебном* порядке – лицо может выбрать любой способ защиты прав через подачу иска для рассмотрения в судопроизводстве.

При рассмотрении иска потерпевший вправе использовать ст.12 Гражданского кодекса РФ от 30.11.96 и требовать:

- признания права;
- прекращения действий, нарушающих право;
- признания недействительным акта государственного органа;
- восстановления права;
- возмещения убытков;
- компенсации морального ущерба.

Литература

1. Мельников В.П. Информационная безопасность: Учеб. пособие для сред. проф. образования / В.П.Мельников, С.А.Клеймёнов, А.М.Петраков; Под ред. С.А.Клеймёнова. – М.: Издательский центр «Академия», 2005. – 336 с.

2. Партыка Т.Л., Попов И.И. Информационная безопасность [Текст]: учебное пособие для студентов учреждений среднего профессионального образования.– 5-е изд., перераб. и доп. - М.: ФОРУМ: ИНФРА – М, 2016. – 432 с.: ил. – (Профессиональное образование).

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА – М», 2016. – 416 с.: ил. – (Профессиональное образование).

4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ В.А. Галатенко. – Режим доступа: http://www.intuit.ru/studies/courses - Загл. с экрана