Основные вопросы:

1. Методы и средства обеспечения информационной безопасности.
2. Криптографические методы защиты информации.
   2.1. Основные сведения.
   2.2. Метод подстановки.
   2.3. Метод перестановки.
   2.4. Многоалфавитные шифры.
   2.5. Другие криптографические методы защиты информации.
3. Физическая защита информации.
4. Основные выводы.

Первый вопрос: Методы и средства обеспечения информационной безопасности.

Основные понятия, определения, методы и средства обеспечения информационной безопасности приведены при рассмотрении вопросов 1-5 Вводных сведений.

В дополнение к вышеназванным сведениям:

Антивирусная защита.

Методы защиты, как правило, используются в совокупности.

Инструменты организационно-правовой защиты.

Основным инструментом организационно-правовой защиты являются различные организационные мероприятия, осуществляемые в процессе формирования инфраструктуры, с помощью которой хранится информация. Данные инструменты применяются на этапе возведения зданий, их ремонта, проектирования систем. К инструментам организационно-правовой защиты относятся международные договоры, различные официальные стандарты.

Инструменты инженерно-технической защиты.

Инженерно-технические средства – это различные объекты, обеспечивающие безопасность. Их наличие обязательно нужно предусмотреть при строительстве здания, аренде помещения. Инженерно-технические инструменты обеспечивают такие преимущества, как:

- Защита помещения компании от действий злоумышленников.
- Защита хранилищ информации от действий заинтересованных лиц.
- Защита от удаленного видеонаблюдения, прослушивания.
- Предотвращение перехвата сведений.

- Создание доступа сотрудников в помещение компании.
- Контроль над деятельностью сотрудников.
- Контроль над перемещением работников на территории компании.
- Защита от пожаров.
- Превентивные меры против последствий стихийных бедствий, катаклизмов.

Все это – базовые меры безопасности. Они не обеспечат полную конфиденциальность, однако без них невозможна полноценная защита.

Криптографические инструменты защиты.

Шифрование – базовый метод защиты. При хранении сведений в компьютере используется шифрование. Если данные передаются на другое устройство, применяются шифрованные каналы. Криптография – это направление, в рамках которого используется шифрование. Криптография используется в следующих целях:

- Защита конфиденциальности сведений, которые передаются по открытым каналам.
- Возможность подтверждения подлинности сведений, которые передаются по различным каналам.
- Обеспечение конфиденциальности сведений в том случае, если они размещены на открытых носителях.
- Сохранение целостности данных при их передаче и хранении.
- Подтверждение отправки сообщения с информацией.
- Защита ПО от несанкционированного применения и копирования.

Программно-аппаратные инструменты для защиты сведений.

Программно-аппаратные инструменты включены в состав технических средств. К примеру, это могут быть:

- Инструменты для ввода сведений, нужных для идентификации (идентификация по отпечаткам пальцев, магнитные и пластиковые карты доступа).
- Инструменты для шифрования данных.
- Оборудование, предупреждающее несанкционированное использование систем (к примеру, электронные звонки, блокираторы).
- Инструменты для уничтожения сведений на носителях.
- Сигнализация, срабатывающая при попытках несанкционированных манипуляций.

В качестве этих инструментов могут выбираться разные программы. Предназначаются они для идентификации пользователей, ограничения доступа, шифрования. Для полноценной защиты применяются и аппаратные, и программные инструменты. Комплекс мер обеспечивает наивысшую степень

защиты. Однако руководитель должен помнить, что добиться стопроцентной защиты невозможно. Всегда остаются слабые места, которые нужно выявлять.

Второй вопрос: Криптографические методы защиты информации.

2.1. Основные сведения.

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos - тайный, logos - наука). Криптология разделяется на два направления - криптографию и криптоанализ. Цели этих направлений прямо противоположны:

- криптография занимается поиском и исследованием математических методов преобразования информации.
- сфера интересов криптоанализа - исследование возможности расшифровывания информации без знания ключей.

Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа. В качестве информации, подлежащей шифрованию и дешифрованию, рассматриваются тексты, построенные на некотором алфавите. Алфавит - конечное множество используемых для кодирования информации знаков. Примеры алфавитов, используемых в современных информационных системах:

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

Шифрование – процесс преобразования исходного или открытого текста в зашифрованный. Выполняется на основе ключа и используется для защиты сообщений от несанкционированного прочтения. Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов. Обычно ключ представляет собой последовательный ряд символов того же алфавита, в котором набрано информационное сообщение

По характеру используемого ключа криптографические методы делятся на:

- симметричные: для шифрования и дешифрования используется один и тот же секретный ключ;

- асимметричные: для шифрования и дешифрования используют разные ключи, открытый – для шифрования, секретный – для дешифрования.

К симметричным криптографическим алгоритмам относят простейшие методы шифрования (подстановки, перестановки), потоковые и блочные шифры.

2.2. Метод подстановки.

Метод подстановки

Шифр подстановки или замены - наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие символы того же либо другого алфавита по определенному правилу.

Историческим примером шифра подстановки является шифр Цезаря, в котором каждый символ открытого текста заменяется другой буквой, которая определяется путем смещения по алфавиту от исходной буквы влево или вправо на k букв. При достижении конца алфавита выполняется циклический переход к его началу. Цезарь использовал шифр замены при смещении вправо при $k = 3$.

Для произвольного ключа k шифр имеет вид:

$$x_i \to y_j, \qquad i = (j + k) mod\ n, \qquad i = \overline{1,n} \tag{1.1}$$

где j – номер в алфавите символа открытого текста,

j –номер зашифрованного символа,

k –величина смещения - ключ,

n –количество букв в алфавите.

Обратная подстановка осуществляется по правилу

$$i = (j + n - k) mod\ n \tag{1.2}$$

Условием для успешной реализации этого метода является совпадение размера множеств открытого текста и шифротекста. Это условие в современных криптосистемах называется гомоморфизмом.

Другим вариантом метода подстановки является задание соответствия между буквами исходного алфавита и буквами подстановочного алфавита. Это позволяет заменять буквы в открытом тексте буквами из подстановочного алфавита Подстановочный алфавит может задаваться как множество символов, либо составляться по определенному правилу.

Пусть подстановочный алфавит составлен по следующему правилу:

$$y_{2k-1} = x_{2k}, y_{2k} = x_{33-2k} \quad k = \overline{1,16} \tag{1.3}$$

где x- исходный подстановочный алфавит; y - подстановочный алфавит;

В формуле (1.3) буквы с четными и нечетными номерами в алфавите, заменяются по разным правилам.

Воспользуемся новым алфавитом для шифрования фразы:

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Каждая буква в этой фразе имеет порядковый номер в исходном алфавите. При шифровании методом подстановки необходимо заменить буквы исходного алфавита соответствующими буквами подстановочного алфавита (О - П, С - О, Н - Т и т.д.). Так буква О в исходном алфавите имеет номер 16, k=8. По правилу $x(2\cdot8)=y(33-2\cdot8)$ буква О заменяется буквой с номером 17, т.е. П.

В шифрованном виде эта фраза примет следующий вид:

ПОТПГЭ ШБЖЙУЭ ЙТХПСНЬЧЙЙ.

Шифрование простой подстановкой на коротких алфавитах обеспечивает слабую защиту открытого текста. Подстановочные криптограммы можно раскрыть, составляя частотные таблицы для букв, пар букв (биграмм) и троек букв (триграмм). Большие частоты появления одних букв и малые других, а также частые ассоциации гласных с согласными позволяют найти буквы открытого текста. С увеличением размера алфавита применение частотного анализа становится все более дорогим, однако, принцип подстановки теряет свою практическую значимость.

2.3. Метод перестановки.

При шифровании этим методом переставляются не буквы алфавита, а буквы открытого текста в пределах группы, называемой таблицей перестановки. Например, сообщение разбито на группы знаков, включая пробелы, и в каждой группе буквы переставлены в соответствии с правилом:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}$$

В этом случае вторая буква исходного текста буде стоять на первом месте, четвертая – на втором и т.д. Если сообщение не кратно количеству символов в группе перестановки, последняя группа дополняется определенными символами, чаще всего пробелами.

Если задана фраза: ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ, то после шифрования она примет вид: СООНЫЗВ ЩТАИ НЫИОМФРИАИ.

В случае перестановки таблицы частот для пар и трех букв показывают наличие стандартных буквенных пар, позволяя реконструировать открытый текст путем поиска тех перестановок, которые их воссоединяют. Следовательно, ключ, используемый для преобразования открытого текста, может быть восстановлен по одной криптограмме. Используется, как правило, в сочетании с другими методами.

2.4. Многоалфавитные шифры.

Слабая криптостойкость моноалфавитных подстановок преодолевается с применением подстановок многоалфавитных. Для защиты от частотного анализа были разработаны многоалфавитные шифры, в которых для шифрования сообщения периодически используется несколько различных подстановочных алфавитов. Если задано r подстановочных алфавитов, то исходное сообщение разбивается на группы по r символов, для шифрования i-го символа группы используется i-ый подстановочный алфавит. Например, для r=4 буквы с номерами 1,5,9,13, ... шифруются 1 алфавитом, буквы с номерами 2,7,10,14, ... - 2 алфавитом, и т.д.

Для получения открытого текста выделяются повторяющиеся группы знаков, и определяется период повторения. Предполагаемый период проверяется составлением частотного распределения для каждой n-й буквы зашифрованного текста. Если каждое из n частотных распределений имеет сильную неоднородность, характерную для моноалфавитной подстановки, то предполагаемый период является правильным. Затем задача решается как n различных простых подстановок.

2.5. Другие криптографические методы защиты информации.

Сведения о других криптографических методах защиты информации представлены в приложении к данному план-конспекту.

Третий вопрос: Физическая защита информации.

Физические средства защиты – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий (рисунок).

Эти средства применяются для охраны:

1) территории предприятия и наблюдение за ней;
2) зданий, внутренних помещений и контроль за ними;
3) оборудования, продукции, финансов и информации;
4) осуществление контролируемого доступа в здания и помещения.

Все физические средства защиты объектов можно разделить на **три категории**:

- средства предупреждения,
- средства обнаружения и
- системы ликвидации угроз.

Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов – это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов). Средства пожаротушения относятся к системам ликвидации угроз.

По физической природе и функциональному назначению средства защиты объектов можно разделить на следующие группы:

– охранные и охранно-пожарные системы;
– охранное телевидение;
– охранное освещение;
– средства физической защиты.

Охранные системы предназначены для

– обнаружения попыток проникновения на объект защиты;
– оповещения сотрудников охраны о появлении угроз.

К элементам охранных систем относятся датчики, принципы работы которых определяют возможности охранных систем. Уже разработано и широко используется значительное количество самых разнообразных датчиков, как по принципам обнаружения различных физических полей, так и по тактическому использованию. Датчики посредством тех или иных каналов связи соединены с

контрольно-приемным устройством пункта (или поста) охраны и средствами тревожного оповещения.

Охранное телевидение позволяет контролировать обстановку как на объекте, так и вокруг него в динамике ее развития, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя.

Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры. Через объектив изображение злоумышленника попадает на светочувствительный элемент камеры, в котором оно преобразуется в электрический сигнал, поступающий затем по специальному коаксиальному кабелю на монитор и при необходимости – на видеомагнитофон.

Видеокамера является наиболее важным элементом системы охранного телевидения, так как от ее характеристик зависит эффективность и результативность всей системы контроля и наблюдения. В настоящее время разработаны и выпускаются самые разнообразные модели, различающиеся как по габаритам, так и по возможностям, и по конструктивному исполнению.

Обязательной составной частью системы защиты любого объекта является **охранное освещение**. Различают дежурное и тревожное охранное освещение.

К средствам **физической защиты** относятся:

– естественные и искусственные барьеры;

– особые конструкции периметров, оконных и дверных переплетов,;

– зоны безопасности.

Важным средством физической защиты является планировка объекта, его зданий и помещений по **зонам безопасности**, которые учитывают степень важности различных частей объекта, с точки зрения нанесения ущерба от различного вида угроз.

Среди средств **физической защиты** особо следует отметить **средства защиты ПЭВМ** от хищения и проникновения к их внутренним компонентам. Для этого используют металлические конструкции с клейкой подставкой, которая обеспечивает сцепление с поверхностью стола с силой в 2500-2700 кг/см. Это исключает изъятие или перемещение ПЭВМ без нарушения целостности поверхности стола. Перемещение ПЭВМ возможно только с использованием специальных ключей и инструментов.

Физическая защита данных.

Физическая защита данных включает в себя защиту

1. Кабельной системы
2. Системы электроснабжения
3. Системы архивирования и дублирования информации
4. Защиту от стихийных бедствий

1. Кабельная система остается главной "ахиллесовой пятой" большинства локальных вычислительных сетей: по данным различных исследований, именно кабельная система является причиной более чем половины всех отказов сети. В связи с этим кабельной системе должно уделяться особое внимание с самого момента проектирования сети.

Наилучшим способом избавить себя от "головной боли" по поводу неправильной прокладкй кабеля является использование получивших широкое распространение в последнее время так называемых структурированных кабельных систем, использующих одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, передачи видеоинформации или сигналов от датчиков пожарной безопасности или охранных систем. К структурированным кабельным системам относятся, например, SYSTIMAX SCS фирмы AT&T, OPEN DECconnect компании Digital, кабельная система корпорации IBM.

Понятие "структурированность" означает, что кабельную систему здания можно разделить на несколько уровней в зависимости от назначения и месторасположения компонентов кабельной системы. Например, кабельная система SYSTIMAX SCS состоит из:

- Внешней подсистемы (campus subsystem)
- Аппаратных (equipment room)
- Административной подсистемы (administrative subsystem)
- Магистрали (backbone cabling)
- Горизонтальной подсистемы (horizontal subsystem)

Внешняя подсистема состоит из медного и оптоволоконного кабеля, устройств электрической защиты и заземления и связывает коммуникационную и обрабатывающую аппаратуру в здании. В эту подсистему входят устройства сопряжения внешних кабельных линий с внутренними.

Аппаратные служат для размещения различного коммуникационного оборудования, предназначенного для обеспечения работы административной подсистемы.

Административная подсистема предназначена для быстрого и легкого управления кабельной системой SYSTIMAX SCS при изменении планов размещения персонала и отделов. В ее состав входят кабельная система (неэкранированная витая пара и оптоволокно), устройства коммутации и сопряжения магистрали и горизонтальной подсистемы, соединительные шнуры.

Магистраль состоит из медного кабеля или комбинации медного и оптоволоконного кабеля и вспомогательного оборудования. Она связывает между собой этажи здания или большие площади одного и того же этажа.

Горизонтальная система на базе витого медного кабеля расширяет основную магистраль от входных точек административной системы этажа к розеткам на рабочем месте.

И, наконец, оборудование рабочих мест включает в себя соединительные шнуры, адаптеры, устройства сопряжения и обеспечивает механическое и электрическое соединение между оборудованием рабочего места и горизонтальной кабельной подсистемой.

Наилучшим способом защиты кабеля от физических (а иногда и температурных и химических воздействий, например, в производственных цехах) является прокладка кабелей с использованием в различной степени защищенных коробов. При прокладке сетевого кабеля вблизи источников электромагнитного излучения необходимо выполнять следующие требования:

а) неэкранированная витая пара должна отстоять минимум на 15-30 см от электрического кабеля, розеток, трансформаторов.

б) требования к коаксиальному кабелю менее жесткие - расстояние до электрической линии или электроприборов должно быть не менее 10-15 см.

Другая важная проблема правильной инсталляции и безотказной работы кабельной системы - соответствие всех ее компонентов требованиям международных стандартов.

Наибольшее распространение в настоящее время получили следующие стандарты кабельных систем:

Спецификации корпорации IBM, которые предусматривают девять различных типов кабелей. Наиболее распространенным среди них является кабель IBM type 1 - экранированная витая пара (STP) для сетей Token Ring.

Система категорий Underwriters Labs (UL) представлена этой лабораторией совместно с корпорацией Anixter. Система включает пять уровней кабелей. В настоящее время система UL приведена в соответствие с системой категорий EIA/TIA.

Стандарт EIA/TIA 568 был разработан совместными усилиями UL, American National Standards Institute (ANSI) и Electronic Industry Association/Telecommunications Industry Association, подгруппой TR41.8. 1 для кабельных систем на витой паре (UTP).

В дополнение к стандарту EIA/TIA 568 существует документ DIS 1 180i, разработанный International Standard Organisation (ISO) и International Electrotechnical Commission (IEC). Данный стандарт использует термин "категория" для отдельных кабелей и термин "класс" для кабельных систем.

2. Системы электроснабжения. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка **источников бесперебойного питания**. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства - серверы, концентраторы, мосты и т. д. - оснащены собственными дублированными системами электропитания.

3. Системы архивирования и дублирования информации. Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер. Среди наиболее распространенных моделей архивационных серверов можно выделить Storage Express System корпорации Intel, ARCserve for Windows, производства фирмы Cheyenne и ряд других.

Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия. Для обеспечения восстановления данных при сбоях магнитных дисков в последнее время чаще всего применяются системы дисковых массивов - группы дисков, работающих как единое устройство, соответствующих стандарту RAID

(Redundant Arrays of Inexpensive Disks). Эти массивы обеспечивают наиболее высокую скорость записи/считывания данных, возможность полного восстановления данных и замены вышедших из строя дисков в "горячем" режиме (без отключения остальных дисков массива).

Организация дисковых массивов предусматривает различные технические решения, реализованные на нескольких уровнях.

Уровень 0 предусматривает простое разделение потока данных между двумя или несколькими дисками. Преимущество подобного решения заключается в увеличении скорости ввода/вывода пропорционально количеству задействованных в массиве дисков. В то же время такое решение не позволяет восстановить информацию при выходе из строя одного из дисков массива.

RAID уровня 1 заключается в организации так называемых "зеркальных" дисков. Во время записи данных информация основного диска системы дублируется на зеркальном диске, а при выходе из строя основного диска в работу тут же включается "зеркальный".

Уровни 2 и 3 предусматривают создание так называемых параллельных дисковых массивов, при записи на которые данные распределяются по дискам на битовом уровне. Специальный диск выделяется для сохранения избыточной информации, которая используется для восстановления данных при выходе из строя какого-либо из дисков массивов.

Уровни 4 и 5 представляют собой модификацию нулевого уровня, при котором поток данных распределяется по дискам массива. Отличие состоит в том, что на уровне 4 выделяется специальный диск для хранения избыточной информации, а на уровне 5 избыточная информация распределяется по всем дискам массива. Организация дисковых массивов в соответствии со стандартом 5 уровня обеспечивает высокую скорость считывания/записи информации и позволяет восстанавливать данные при сбое какого-либо диска без отключения всего дискового массива.

Среди всех вышеперечисленных уровней дисковых массивов уровни 3 и 5 являются наиболее предпочтительными и предполагают меньшие по сравнению с организацией "зеркальных" дисков материальные затраты при том же уровне надежности.

4. Основной и наиболее распространенный **метод защиты информации** и оборудования от различных **стихийных бедствий** - пожаров, землетрясений, наводнений и т.д. - состоит в хранении архивных копий информации или в размещении некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других зданиях или, реже, даже в другом районе города или в другом городе.

Четвёртый вопрос: <u>Основные выводы.</u>

Методы и средства обеспечения безопасности информации в автоматизированных информационных технологиях представлены на рисунке (представлен ниже). К ним относятся: **препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение.**

Методы защиты информации представляют собой основу механизмов защиты.

Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. д.).

Управление доступом — метод защиты информации с помощью использования всех ресурсов информационной технологии. Управление доступом включает следующие функции зашиты:

- идентификация специалистов, персонала и ресурсов информационной технологии (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверка полномочий (соответствие дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрация (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытке несанкционированных действий.

Маскировка — метод защиты информации путем ее криптографического закрытия. Этот метод сейчас широко применяется как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности данный метод является единственно надежным.

Регламентация — метод защиты информации, создающий по регламенту в информационных технологиях такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Принуждение — метод защиты, когда специалисты и персонал информационной технологии вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение — метод защиты, побуждающий специалистов и персонал автоматизи-рованной информационной технологии не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Рассмотренные методы обеспечения безопасности в информационных технологиях реализуются на практике за счет применения различных средств защиты.

Все средства защиты информации делятся на следующие виды:

Формальные средства защиты – это средства, выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека

Неформальные средства защиты – это средства защиты, которые определяются целенаправленной деятельностью человека, либо регламентируют эту деятельность.

К основным формальным средствам защиты, которые используются в информационных технологиях для создания механизмов защиты, относятся следующие:

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Все технические средства делятся на следующие виды:

Аппаратные, представляющие собой устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу.

Физические, представляющие собой автономные устройства и системы, создающие физические препятствия для злоумышленников (замки, решетки, охранная сигнализация и т.д.)

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций зашиты информации.

К основным неформальным средствам защиты относятся:

Организационные средства.
Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации в информационных технологиях. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство и оборудование помещений экономического объекта, проектирование информационной технологии, монтаж и наладка оборудования, испытания, эксплуатация и т. д.).

Морально-этические средства. Реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи. Эти нормы большей частью не являются обязательными как законодательные меры, однако несоблюдение их ведет к утечке информации и нарушению секретности.

Законодательные средства определяются законодательными актами страны, в которых регламентируются правила пользования, обработки и передачи

информации ограниченного доступа и устанавливаются меры ответственности за нарушения этих правил.