**Недостатки криптографической системы**

|  |  |  |
| --- | --- | --- |
| Тип шифрования | Преимущества | Недостатки |
| Шифрование с симметричным ключом | Скорость, легкость аппаратной реализации | Оба ключа одинаковы, трудно распространять ключи, не поддерживает цифровые подписи |
| Шифрование с открытым ключом | Используется два различных ключа, просто распространять ключи, обеспечивает целостность и невозможность отказа от авторства (за счет цифровой подписи) | Работает медленно, требует больших вычислительных мощностей |

Алгоритмы защиты информации

Алгоритмы можно реализовать как программным, так и аппаратным методом. Аппаратный шифратор представляет собой компьютерное “железо” чаще всего, это плата расширения, вставляемая в разъём системной платы в пк. Производители аппаратных шифраторов стараются насытить их дополнительными возможностями, среди которых:

1. Генерация случайных чисел – (Это нужно для получения криптографических ключей).
2. Контроль входа в компьютер – (При включении пк устройство требует от пользователя ввести персональную информацию, например вставить диск с ключами. Работа будет разрешена только после опознания предъявленных ключей, в противном случае придется разбирать системный блок и вынимать оттуда шифратор, чтобы загрузить пк.
3. Контроль целостности файлов операционной системы – (Это не позволит злоумышленнику в ваше отсутствие изменить файлы. Шифратор хранит в себе список всех важных файлов с заранее рассчитанными для каждого контрольными суммами, и если при следующей загрузке не совпадает эталонная сумма хотя бы одного из них – компьютер блокируется).

Плата со всеми перечисленными возможностями называется устройством криптографической защиты данных.

Шифратор выполняющий контроль входа на пк и проверяющий целостность операционной системы называют так же электронным замком.

Понятно что с электронным замком должно использоваться соответствующее программное обеспечение – утилита с помощью которой формируются ключи для пользователей и ведется их список для распознавания “свой/чужой”.

Эти программы обычно доступны только администратору по безопасности, который должен предварительно настроить все указы D для пользователей.

Структура шифраторов

Для выполнения ……. Это основной модуль шифратора, который заведует работой всех остальных.

Контролер системной шины пк – через него осуществляется основной обмен данными между указами D и компьютером.

Энергозависимое запоминающее устройство – должно быть емким (несколько мегабайт) и допускать большое число треков записи. Здесь размещается программное обеспечивание микроконтроллера.

Память журнала – представляет собой энергозависимое ЗУ.

Шифропроцессор – это специализированная микросхема, которая занимается шифрованием данных.

Генератор случайных чисел, блок ввода ключевой информации, блок коммутаторов.

Система криптографической защиты информации (СКЗИ) – “Верба-OW”

Используемые в “Верба” методы шифровая гарантируют не только высокую секретность и эффективное обнаружение искажений или ошибок передаваемой информации.

Ключ шифрования – это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных.

При зашифрования сообщения криптографическое преобразование использует ключ.

Для расшифрования нужен соответствующий ключ, в Верба-OW использует пару ключей: Открытые и секретные ключи шифрования.

Верба-OW использует алгоритм шифрования, основанный на принципе комбинирования, который подразумевает процесс наложения по определенному закону гаммы шифра на открытые данные.

Верба является системой с открытым распределением ключей, каждый пользователь вырабатывает свой секретный ключ, из которого формируется открытый ключ.

В вербе реализован алгоритм подписи на базе криптографического алгоритма.

Открытый ключ подписи вычисляется как значение некоторой функции от секретного ключа.

При работе с СКЗИ-Верба каждый пользователь, обладающий правом подписи, самостоятельно формирует личные секретный и открытый ключи подписи. Открытые ключи объединяются в справочники. В СКЗИ-Верба реализована система ЭЦП (электронной цифровой подписи) на базе ассиметричного криптографического алгоритма. При проверке подписи проверяющий должен располагать открытым ключом пользователя, поставившего подпись. Процедура проверки подписи состоит из вычисления КЭШ-значения документов и проверки некоторых соотношений, связывающих КЭШ-значения документа, подпись под этим документом и открытый ключ.

Автоматизированное рабочее место администратора системы безопасности предназначено для работы с ключевой информации.

На основе исходной ключевой информации, находящейся на лицензионной дискете, вырабатывать ключи, секретные и открытые, создавать рабочие копии цифровых дискет.

ПО Верба предусматривает возможность хранения секретных ключей на жестком диске. Смена ключей возможна:

1. При плановой смене ключей
2. Компрометации ключей или ключа
3. Ввод в действие нового ключа
4. Удаление ключа

Плановую схему ключей рекомендуется менять не реже одного раза в год.

После уничтожения ключевой информации вводятся в действие секретные ключи

**Защита информации в интернете**

Платой за использование интернета являются следующие угрозы:

1. …
2. Несанкционированный доступ к сети организации со стороны рабочих станций удаленных и передающих серверов, включенных в сеть интернет
3. Потеря информации в каналах связи интернет в результате заражения вредоносными программами, некомплектности сотрудников, отказа канала связи, стихийных бедствий
4. Несанкционированный программно-аппаратный доступ к информации, находящейся в канале связи интернет
5. Несанкционированный доступ к информации через электромагнитные излучения каналов связи
6. Сбор и мониторинг сетевой информации в интересах третьих лиц
7. Переизбыток ненужной и вредоносной и вредоносной информации в системе

Из всего выше сказанного следует что строго необходимо соблюдать рекомендации:

1. Проводить тщательный анализ и изъятие конфиденциальной информации из подключаемой сети или пк.
2. Использование прокси и условно анонимных серверов позволяет снизить риски, связанные со сбором и мониторингом сетевой информации.
3. Использование автоматизированных средств проверки сети.
4. Использование систем ограничения доступа сотрудников к сетевым ресурсам интернет.
5. Выполнять рекомендации до подключения к интернету:
6. При работе в сети интернет на первое место выходит межсетевой экран или брандмауэр. Он позволяет снизить число эффективных внешних атак, несанкционированный доступ к сети организации, блокировать доступ ненужной и вредоносной информации в систему. Использование VPN-технологий, дублирование канала интернет и т.д.

Проблема межсетевого экранирования формируется следующим образом, пусть имеется две информационные системы.

О: Экран – это средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.

Экран выполняет свои функции контролируя все информационные потоки между двумя множествами информационных систем, работая как некоторая информационная мембрана.

**Лекция 6**

В этом смысле экран можно представлять себе как набор фильтров, анализирующих проходящую через них информацию и на основе заложенных в них алгоритмов, принимающих решение пропустить информацию или отказать в ее пересылке. Такая система может выполнять регистрацию событий связанных с процессами разграничения доступа, в частности фиксировать все незаконные попытки доступа к информации и сигнализировать о ситуациях, требующих немедленной реакции, экранирующие системы делают несимметричными, для экранов определяются понятия внутри и снаружи, и задача экрана состоит в защите внутренней сети от потенциально враждебного окружения.

Важнейшим примером потенциально враждебной внешней сети является интернет.

Рассмотрим какие проблемы возникают при построении экранирующих систем.

1. Это обеспечение безопасности внутренней, защищаемой сети и полный контроль над внешними подключениями и сеансами связи
2. Экранирующая система должна обладать мощными и гибкими средствами управления для простого и полного воплощения в жизнь политики безопасности организации, для обеспечения простой реконфигурации системы при изменении структуры сети.
3. Экранирующая система должна работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий.
4. Экранирующая система должна работать эффективно и успевать обрабатывать весь входящий и исходящий трафик в пиковых режимах — это необходимо для того,” Firewall нельзя было забросать большим количеством вызовов, которые привели бы к нарушению ее работы.
5. Система обеспечения безопасности должна быть сама надежно защищена от любых несанкционированных воздействий, поскольку является ключом к конфиденциальной информации в организации.
6. В идеале, если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах. Система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики безопасности.
7. Система Firewall должна иметь средства автоматизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать (например в командировки) и в процессе их работы требуется доступ к некоторым ресурсам внутренней компьютерной сети. В этом случае система должна уметь надежно распознавать таких пользователей и предоставлять им доступ.

**Рассмотрим два способа ограничения доступа к www серверам**

1. Ограничить доступ по IP-адресам клиентских машин,
2. Ввести идентификатор получателя с паролем, для данного вида документов.

Такого рода ввод ограничений, стал часто использоваться, так как многие стремятся в интернет, чтобы использовать его коммуникации. С помощью таких механизмов, по разграничению прав доступа

Доступ к приватным документам можно запретить или разрешить, используя присвоенное имя и пароль конкретного пользователя.

Защита электронной почты

1)Протокол PEM – это стандарт интернета для защиты электронной почты, с использованием открытых или симметричных ключей. Он требует жесткой иерархии сертификационных центров для выдачи ключей.

2)S/MIME – новый стандарт, он задействует криптографические алгоритмы, использует цифровые сертификаты и, следовательно, при обеспечении аутентификации, полагается на сертификационный корпоративный центр

3)PGP -

Приложения для шифрования/расшифровки PGP выпускаются для всех операционных систем

Задачи и методы, цели обеспечения ИБ

Формирование множества задач осуществляется на основе анализа объективных возможностей по реализации поставленных целей защиты. Такое их множество может состоять из ряда классов.

Класс задач – это однородная в функциональном отношении множества задач, обеспечивающих полную или частичную реализацию целей.

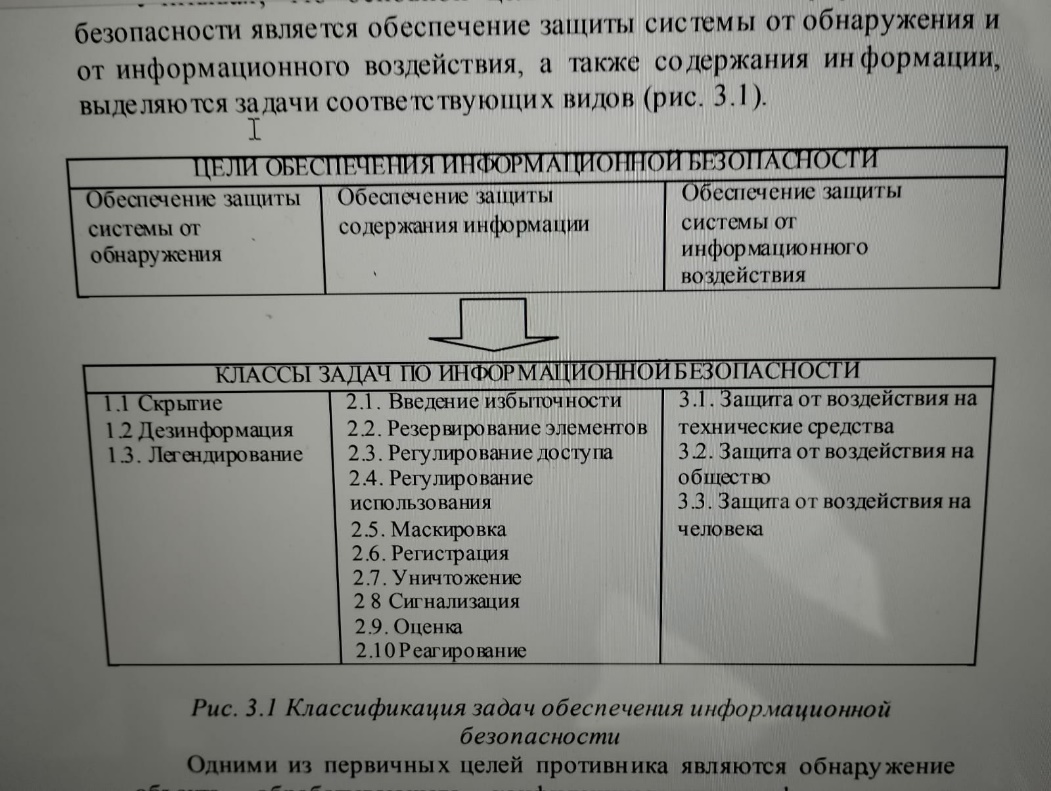


Рисунок – схема Обеспечения ИБ

Одними из первичных целей противника являются обнаружения объекта, обрабатывающего конфиденциальную информацию и выявление сведений о его предназначении, поэтому к первому задач можно отнести задачи уменьшения степени распознавания объектов. К этому виду относятся следующие виды задач – скрытие сведений о средствах обработки информации. Технические задачи направлены для устранения и ослабление демаскирующих признаков, при этом вскрытие осуществляется уменьшением электромагнитной, временной, структурной и признаковой доступности.

**Обзор международных стандартов защиты информации**

Роль стандартов ИБ

С развитием информационных технологий появилась необходимость и требования ИБ. Главная задача стандартов ИБ – создать основу для взаимодействия между производителями, потребителями и специалистом по сертификации. Каждая из этих групп имеет свои интересы и свои взгляды на проблему ИБ. Производители нуждаются в стандартах как в средстве сравнения возможностей своих продуктов и в применении процедуры сертификации как в механизме оценки их свойств, а так же в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. Потребители заинтересованы в методике позволяющей обоснованно выбрать продукт отвечающий их нуждам и решающий их проблемы для чего им необходима шкала оценки безопасности и инструмент с помощью которого они могли бы формулировать свои требования к производителям. Специалисты по сертификации рассматривают стандарты как инструмент, позволяющий им оценивать уровень безопасности, обеспечиваемый системой и предоставить потребителям и предоставить потребителям сделать обоснованный выбор. Специалисты по сертификации заинтересованы в четких и простых критериях так как они должны дать обоснованный ответ пользователю. В конечном счете именно они принимают на себя ответственность за безопасность продукта получившего квалификацию уровня безопасности и прошедшего сертификацию. Таким образом перед стандартами информационной безопасности стоит непростая задача, создать эффективный механизм взаимодействия всех сторон.

Наиболее значимыми стандартами ИБ являются: “Критерии безопасности компьютерных систем министерства обороны США”, руководящие документы гос. тех. Комиссии России, “Европейские критерии безопасности Инф. Тех.”, “Федеральные критерии безопасности информационных технологий США”, “Канадские критерии безопасности компьютерных систем”, “Единые критерии безопасности информационных технологий”

Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга)

Критерии безопасности компьютерных систем, получивших неформальное название оранжевая книга были разработаны министерством обороны США в 1983 году, с целью определения требований безопасности предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем и выработке соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения.

В данном документе были в первые нормативно определены такие понятия как политика безопасности, ядро безопасности и т.д.

Предложенные в этом документе концепции защиты и набор функциональных требований, послужили основой для формирования всех появившихся в последствии стандартов безопасности.

О: Ядро безопасности – это совокупность аппаратных, программных и специальных компонент вычислительной системы, реализующих функции защиты и обеспечения безопасности.

О: Таксономия – это наука о систематизации и классификации сложно организованных объектов и явлений, имеющих иерархическое строение. Таксономия основана на декомпозиции явлений и поэтапном уточнении свойств объектов.

Политика безопасности – это совокупность норм и правил обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности.

Модель безопасности – это формальное представление политики безопасности.

Дискреционное управление доступом – это управление доступом осуществляемого на основании заданного администратором множества разрешенных отношений доступа.

Мандатное управление доступом – это управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности, субъектов и объектов.

В оранжевой книге предложены три критерия безопасности:

1. Политика безопасности
2. Аудит
3. Корректность

В рамках этих критериев сформулированы шесть базовых требований безопасности.

1. Политика безопасности
2. Метки
3. Идентификация и аутентификации
4. Регистрация и учет
5. Контроль корректности функционирования средств защиты
6. Непрерывность защиты

Политика безопасности система должна поддерживать точно определенную политику безопасности, возможность осуществления субъектами доступа к объектам должна определятся на основе их идентификации и набора правил управления доступом.

Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации – отмеченной грифом секретности).

Метки – с объектами должны быть ассоциируемы метки безопасности, используемы в качестве инструмента контроля доступа, для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности объекта и/или режима доступа к этому объекту.

Идентификации и аутентификация – все субъекты должны иметь уникальные идентификаторы, контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступ подтверждения подлинности их идентификаторов и правил разграничения доступа. Данные используемы для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и ассоциирована со всеми активными компонентами компьютерной системы функционирование которых критично с точки зрения безопасности.

Регистрация и учет – для определения степени ответственности пользователей за действия в системе все происходящие в ней события имеющие значения с точки зрения безопасности должны отслеживаться и регистрироваться в защищенном протоколе, система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификаций и уничтожения.

Корректность, контроль корректности и функционирование средств защиты – средства защиты должны содержать независимые аппаратные и или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает что все средства защиты, обеспечивающие политику безопасности, управления атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находится под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Непрерывность защиты – все средства защиты в том числе и реализующие данное требование, должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы, кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы. Приведенные базовые требования, к безопасности служат основой для критериев образующих единую шкалу оценки безопасности компьютерных систем, определяющую 7 классов безопасности.

Классы безопасности компьютерных систем

Оранжевая книга предусматривает четыре группы критериев, которые соответствуют различной степени защищенности от минимальной (группа D) до формально доказанной (группа A). Каждая группа включает один или несколько классов.

Классы защищенности компьютерных систем по Оранжевой книге

Уровень защищенности возрастает от группы D к группе A, а внутри группы, с увеличением класса.

Группа D – минимальная защита

Класс D – минимальная защита

К этому классу относятся все системы не удовлетворяющие требованиям других классов

Граппа C – дискреционная защита

Группа характеризуется произвольным управлением доступом и регистрацией действий субъектов.

Класс C1 – дискреционная защита

Системы этого класса удовлетворяют требованиям обеспечения разделения пользователей и информации и включают средства контроля управления доступом, позволяющие задавать ограничения для индивидуальных пользователей, что дает им возможность защищать свою приватную информацию. Класс C1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня секретности.

Класс C2 – управление доступом

Системы этого класса осуществляют более избирательное управление доступом с использованием меток безопасности, чем системы классов C1 с помощью применений средств индивидуального контроля за действиями пользователей, регистрацией, учетом событий и выделением ресурсов.

Группа B – мандатная защита

Основные требования этой группы – нормативное управлением доступа с использованием меток безопасности, поддержка моделей и политики безопасности, а также наличие спецификаций на функции ядра безопасности. Для систем этой группы монитор взаимодействий должен контролировать все события в системе

Класс B1 – защита с применением меток безопасности.

Системы класса B1 должны соответствовать всем требованиям, предъявляемым к системам класса C2, и должны поддерживать неформальнe. модель безопасности, маркировку данных и нормативное управление доступом. При экспорте из системы информация должна подвергаться маркировке. Обнаруженные в процессе тестирования недостатки должны быть устранены.

Класс B2 – структурированная защита.

Для соответствия классу B2 система должна поддерживать формально определенную и четко документированную модель безопасности, предусматривающую произвольное и нормативное управление доступом, которое распространяется по сравнению с системами класса B1 на все субъекты. Кроме того, должен осуществляться контроль скрытых каналов утечки информации. В структуре Tсb должны быть элементы критичные с точки зрения безопасности. Интерфейс ядра безопасности должен быть четко определен, а его архитектура и организация выполнены с учетом возможности проведения тестовых испытаний. По сравнению с классом B1 должны быть усилены средства аутентификации. Управление безопасностью осуществляется администраторами системы, должны быть предусмотрены средства управления конфигурацией.

Класс B3 – домены безопасности

Для соответствия этому классу Tcb система должна поддерживать монитор взаимодействий. Который контролирует все типы доступа субъектов к объектам. Кроме того, Tcb должна быть структурирована, с целью исключения из нее подсистем, не отвечающих за реализацию функции защиты и достаточно компактна для эффективного тестированного и анализа. В ходе разработки и реализации Tcb, необходимо применение методов и средств, направленных на минимизацию ее сложности. Средства аудита должны включать механизмы оповещения администратора при возникновении событий, имеющих значение для безопасности системы. Требуется наличие средств, восстановления работоспособности системы.

Группа A -верифицированная защита.

Данная группа характеризуется применением формальных методов верификации и корректности работы, механизмов управления доступом. Требуется дополнительная документация, демонстрирующая что Tcb отвечает требованиям безопасности.

Класс A1 – формальная верификация.

Системы класса A1 функционально эквивалентны системам класса B3 и к ним не предъявляется никаких дополнительных функциональных требований. В отличие от систем класса B3 в ходе разработки должны применятся формальные методы верификации, что позволяет с высокой уверенностью получить корректную реализацию функций защиты. Процесс доказательства адекватности реализации начинается на ранней стадии разработки, с построением формальной модели политики безопасности и спецификации высокого уровня. Для обеспечения методов верификации системы классов A1 должны содержать более мощные средства управления конфигурацией и защищенную процедуру дистрибуции.

Высший класс безопасности, требующий осуществления верификации средств защиты построен на доказательстве соответствия программного обеспечения, его спецификациям. С помощью специальных методик, но это очень дорогое, трудоемкое и практически неосуществимое для реалий информационных систем.

Приведенные классы безопасности на долго определили основные концепции безопасности и ход развития средств защиты.

|  |  |  |
| --- | --- | --- |
| Класс D | Группа D | Все системы, не удовлетворяющие требованиям других классов |
| Класс C | Группа С1 | Разделение пользователей и информации. Включает возможность ограничивать доступ пользователей |
|  | Группа С2 | Управление доступом с использованием меток безопасности |
|  | Группа B1 | Соответствует системам с классом C2 и поддерживает неформальную модель безопасности |
| Класс B | Группа B2 | Соответствует системам с классом B1 и поддерживает четко документированную и формальную модель безопасности |
|  | Группа B3 | Система должна поддерживать монитор взаимодействий Средства аудита должны включать механизмы оповещения администратора |
| Класс A | Группа A1 | Системы этого класса функционально соответствуют системам с классом B, но дополнительно содержат формальную верификацию |

Европейские стандарты безопасности информационных систем.

ITSEC

Основываются на критериях, опубликованных в июне 91 года от четырех стран: Франции, Германии, Нидерландов и Великобритании.

Европейские критерии рассматривают задачи:

1. Защита информации от несанкционированного доступа с целью обеспечения конфиденциальности
2. Обеспечение целостности информации по средствам защиты от ее несанкционированной модификации или уничтожения
3. Обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании

В европейских критериях проводятся различия между системами и продуктами.

О: Система – это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

О: Продукт – это аппаратно-программный пакет, который можно купить и по своему усмотрению встроить в ту или иную систему.

Основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Относительно угроз продукту можно лишь строить предположения.

Угрозы безопасности системы носят вполне конкретный и реальный характер. Относительно угроз продукту можно лишь строить предположения. Разработчик может специфицировать условия, пригодные для функционирования продукта; дело покупателя обеспечить выполнение этих условий.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем — облегчить и удешевить оценку системы, составленной из ранее сертифицированных продуктов. В этой связи для систем и продуктов вводится единый термин — **объект оценки**.

Для того чтобы удовлетворить требованиям конфиденциальности, целостности и работоспособности, необходимо реализовать соответствующий набор функций безопасности, таких как идентификация и аутентификация, управление доступом, восстановление после сбоев и т.д. Чтобы средства защиты можно было признать эффективными, требуется определенная степень уверенности в правильности их выбора и надежности функционирования.

Для решения этой проблемы в **«Европейских критериях»** впервые вводится **понятие адекватности (assurance) средств защиты**. Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

Большинство требований безопасности совпадает с аналогичными требованиями Оранжевой книги. В «Европейских критериях» определено десять классов безопасности. Классы F-C1, F-C2, F-B1, F-B2, F-B3 соответствуют классам безопасности Оранжевой книги с аналогичными обозначениями.

**Класс F-IN предназначен** для систем с высокими потребностями в обеспечении целостности, что типично для систем управления базами данных.

Его описание основано на концепции «ролей», соответствующих видам деятельности пользователей, и предоставлении доступа к определённым объектам только посредством доверенных процессов. Должны различаться следующие виды доступа: чтение, запись, добавление, удаление, создание, переименование и выполнение объектов.

**Класс F-AV** характеризуется повышенными требованиями к обеспечению работоспособности.

Это существенно, например для систем управления технологическими процессами. В **требованиях** этого класса указывается, что система должна восстанавливаться после отказа отдельного аппаратного компонента таким образом, чтобы все критически важные функции постоянно оставались доступными. В таком же режиме должна происходить и замена компонентов системы. Независимо от уровня загрузки должно гарантироваться определенное время реакции системы на внешние события.

**Класс F-DI** ориентирован на распределенные системы обработки информации. Перед началом обмена и при получении данных стороны должны иметь возможность провести идентификацию участников взаимодействия и проверить ее подлинность.

Должны использоваться средства контроля и исправления ошибок. В частности, при пересылке данных должны обнаруживаться все случайные или намеренные искажения адресной и пользовательской информации. Знание алгоритма обнаружения искажений не должно позволять злоумышленнику производить нелегальную модификацию передаваемых данных. Необходимо обнаруживать попытки повторной передачи ранее переданных сообщений.

**Класс F-DC** уделяет особое внимание требованиями к конфиденциальности передаваемой информации. Информация по каналам связи должна передаваться в зашифрованном виде. Ключи шифрования защищают от несанкционированного доступа.

**Класс F-DX** предъявляет повышенные требования и к целостности и к конфиденциальности информации. Его можно рассматривать как объединение классов F-DI и F-DC с дополнительными возможностями шифрования и защиты от анализа трафика. Следует ограничить доступ к ранее переданной информации, которая в принципе может способствовать проведению криптоанализа.

**Критерии адекватности.**

Адекватность включает в себя два аспекта: эффективность, отражающую соответствие средств безопасности решаемым задачам, и корректность, характеризующую процесс их разработки и функционирования.

**Эффективность** — соответствие между задачами, поставленными перед средствами безопасности, и реализованным набором функций защиты — их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты.

**Корректность** — правильность и надежность реализации функций безопасности.

Европейские критерии определяют **семь уровней адекватности** — от Е0 до Е6. При проверке адекватности анализируется весь жизненный цикл системы — от начальной фазы проектирования до эксплуатации и сопровождения.

**Уровни адекватности от Е1 до Е6** выстроены по нарастанию требований тщательности контроля. Так, на уровне Е1 анализируется лишь общая архитектура системы, а адекватность средств защиты подтверждается функциональным тестированием.

**На уровне ЕЗ** к анализу привлекаются исходные тексты программ и схемы аппаратного обеспечения. **На уровне Е6** требуется формальное описание функций безопасности, общей архитектуры, а также политики безопасности.

В Европейских критериях определены три уровня безопасности — базовый, средний и высокий. Степень безопасности системы определяется самым слабым из критически важных механизмов защиты.

Безопасность считается базовой, если средства защиты способны противостоять отдельным случайным атакам. Безопасность считается средней, если средства защиты способны противостоять злоумышленникам, обладающим ограниченными ресурсами и возможностями. Наконец, безопасность можно считать высокой, если есть уверенность, что средства защиты могут быть преодолены только злоумышленником с высокой квалификацией, набор возможностей и ресурсов которого выходит за рамки возможного.

Итак, **Европейские критерии безопасности информационных технологий**, появившиеся вслед за Оранжевой книгой, оказали существенное влияние на стандарты безопасности и методику сертификации.

Главное **достижение** этого документа — **введение понятия адекватности средств защиты и определение отдельной шкалы для критериев адекватности**. Как уже упоминалось, Европейские критерии придают адекватность средств защиты даже большее значение, чем их функциональности. Этот подход используется во многих появившихся позднее стандартах информационной безопасности.

Критерии США

Федеральные критерии разрабатывались как одна из составляющих

Под продуктом информационных технологий понимается совокупность аппаратных и программных средств которые представляют собой поставляемое конечному потребителю готовое к использованию средство обработки информации

IT- продукт эксплуатируется не автономно, а интегрируется в систему обработки информации представляющую собой совокупность IT – продуктов объединенных функционально полный комплекс

Кроме того, профиль содержит требования по соблюдению технологической дисциплины.

Тестирования и квалификационного анализа It-продукта. Профиль безопасности анализируется на полноту, непротиворечивость и техническую корректность

Второй этап

Разработка и квалификационный анализ IT-продуктов

Разработанные IT-продукты подвергаются независимому анализу, целью которого является определение степени соответствия характеристик продукта разработанных в профиле защиты требований и спецификации

Третий этап

Компоновка и систематизация систем безопасности в целом

Успешно прошедшие квалификацию уровня безопасности IT-продукты интегрируются в систему обработки информации.

Полученная в результате система должна удовлетворять заявленным в профиле защиты требованиям.

Федеральные критерии регламентирует только первый этап этой схемы – разработку и анализ профиля защиты, процесс создания IT-продуктов и компоновка систем обработки информации остаются в нестандартном

Профиль защиты:

1 Описание – информация для его идентификации находится в специальной картотеке

2 Обоснование – описание среды эксплуатации предполагаемых угроз и методов использования IT-продуктов

Функциональные требования к IT-продукту

Определение условий, в которых требуется безопасность – в виде перечня угроз.

4 Требования технологий разработки IT-продуктов

5 Требования к процессу сертификации

Федеральные критерии безопасности информационных технологий – это первый стандарт информационной безопасности, в котором определяются три независимые группы требований: Функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалификационного анализа.

Данный стандарт ознаменовал появление нового поколения руководящих документов в области информационной безопасности, а его положения послужили базой для разработки Канадских критериев безопасности информационных систем и единых критериев безопасности информационных технологий

Единые критерии безопасности информационных технологий являются результатом совместных усилий авторов европейских критериев безопасности информационных технологий, федеральных критериев безопасности технологий и канадских критериев безопасности компьютерных систем. Направленных на объединение основных положений и создания единого международного стандарта безопасности информационных технологий.

Работа над этим стандартом началась в 93 году. Версия 2.1 этого стандарта утверждена международной организацией по стандартизацией в 1999 году в качестве международного стандарта информационной безопасности 15.408. В РФ стандарт действует под номером ГОСТ Р ИСО/МЭК15408. Этот документ разработан на основе достижений многочисленных исследований в области безопасности информационных технологий 90-х годов и на результатах анализа опыта применения положенных в его основу стандартов. Единые критерии оперируют уже знакомыми по федеральным критериям понятиям “Продукт информационных технологий” или “IT-продукт” и используют предложенную в них концепцию профиля защиты.

Единые критерии разрабатывались в расчете на то, чтобы удовлетворить запросы трех групп специалистов: Производителей, потребителей, а также экспертов по квалификации уровня их безопасности. Потребители рассматривают квалификацию уровня безопасности It-продукта как метод определения соответствия It-продукта их запросам.

Единые критерии играют существенную роль в процессе формирования запроса потребителей. Так как содержат механизмы позволяющие сформулировать эти запросы в виде стандартизированных требований. Это позволяет потребителям принять обоснованное решение о возможности использования тех или иных продуктов. Единые критерии предоставляют потребителям механизм профилей защиты, с помощью которого они могут выразить специфичные для них требования, не заботясь о механизмах их реализации. Производители должны использовать единые критерии, в ходе проектирования и разработке IT-продуктов, а также в подготовке к анализу и сертификации. Этот документ дает возможность производителям, на основании анализа запросов потребителей, которым должен удовлетворять разработанный ими продукт. Производители используют предлагаемую едиными критериями технологию, для обоснования своих претензий на то, что поставляемый ими IT-продукт успешно противостоит угрозам безопасности, на основании того, что он удовлетворят выдвинутым функциональным требованиям и их реализация осуществлена с достаточным уровнем адекватности. Для осуществления этой технологии единые критерии предлагают производителям специальный механизм, названный проект защиты, дополняющий профиль защиты. И позволяющий соединить описания требований, на которые ориентировался разработчик. Эксперты по квалификации используют этот документ в качестве основных критериев определения соответствия средств защиты, предъявляемых к нему потребителями и угрозам, действующим в среде его эксплуатации.

Единые критерии описывают только общую схему проведения квалификационного анализа и сертификации, но не регламентирует процедуру их осуществления. Единые критерии обеспечивают нормальное функционирование и служат руководящим материалам для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки.

Единые критерии рассматривают критерии безопасности как совокупность. Ставят перед средствами защиты задачи, противодействия угрозам, актуальным для среды эксплуатации этого продукта, единые критерии регламентируют все стадии разработки. Они предлагают единый процесс разработки, требующий от потребителей и производителей, оформления подробных документов. Задача защиты – базовое понятие единых критериев, выражающая потребность потребителя It-продукта в противостоянии заданному множеству угроз.

Профили защиты – это нормативный документ, представляющий собой совокупность задач защиты.

Проект защиты – это документ, представляющий собой совокупность задач защиты, функциональных требований, функциональных спецификаций и список общих спецификаций средств защиты.

Таким образом единые критерии безопасности информационных технологий представляют собой результат обобщения всех достижений последних лет в области информационной безопасности.

Информация как объект познания имеет ряд особенностей

-Нематериальна по своей природе

-После записи на носитель информация приобретает определенные параметры и может быть измерена в объеме

-Информация, записанная на материальный носитель, может хранится, обрабатываться, передаваться по каналам связи

-Перемещаясь по линиям связи информация создает физические поля, которые отражают ее содержание.

При обработке, хранении, передаче информации, информация циркулирует в информационной системе. Простейшая информационная система состоит из источника информации, канала связи и получателя информации.

Уровни представления информации

1 Уровень носителей

2 Уровень средств взаимодействия с носителем

3 Логический уровень

4 Синтаксический уровень

5 Семантический уровень

1 Уровень носителей информации

По своей природе информация нематериальна и в чистом виде человеку не доступна.

Для того чтобы человек воспринял информацию, должен быть материальный носитель: другой человек, вещество, энергия.

Информация, являясь предметом защиты, требует защищенности тех объектов, в которых она присутствует в той или иной материальной форме.

Все носители имеют две категории информации.

1 Признаковая информация: информация носителя о себе, о видовых признаках: форма, размер, структура, физические свойства и параметры.

2 Семантическая информация – то что не зависит от вида носителя, продукт абстрактного мышления на языке символов.

Как носитель человек нуждается не только в физической защите, его так же следует защищать от избыточной информации, бесполезной, от дезинформации, от разрушающей информации. Многие механизмы защиты работают у человека на биологическом уровне. При поступлении ненужной или избыточной информации, снижается внимание, ухудшается запоминание, замедляется реакция. Так как часто на основе имеющейся информации принимаются неверные решения, что возможно вследствие ложной информации или сверх информированности (сложности из-за приоритета и остальных факторов). Вещественные носители разнообразны по своим качествам.

Особенности вещественных носителей:

1 Придают информации свойство статичности (постоянство во времени), в связи с этим используются для хранения информации.

2. Информация фиксируется очно, ее трудно уничтожить

3. Со временем вещественные носители разрушаются и стареют, при этом информация гибнет вместе с носителями.

4 Запись информации связана с изменением физических и химических свойств носителя.

Вещественные носители следует защищать от повреждения, хищения, износа, потери.

Энергетические носители

О: это электромагнитные поля, которые используются для передачи информации, они не стареют, бесконтрольно распространяются обратно, способны к взаимному преобразованию, запись информации связана с изменением параметров поля.

Основные свойства защиты информации на энергетическом носителе, обеспечение по меха устойчивости при выборе кодирования, обеспечение требуемой энергетике сигнала, защита от утечки, в том числе через побочные электромагнитные излучения и наводки, защита от перехвата в основном канале

Второй уровень – Уровень средств взаимодействия с носителем.

Взаимодействие с носителем не всегда возможно и часто осуществляется через сложные технические устройства, для защиты на этом уровне нужно следить за исправностью устройств считывания, за отсутствием технических средств несанкционированного доступа к информации, задачей которых является перехват или перенаправление потока считываемой информации.

Уровень 3 – логический.

На логическом уровне в информационной системе информация может быть представлена в виде логических дисков, секторов, кластеров. В современных ОС уровни отдельных байтов, кластеров, секторов не видны. Следует помнить что удаление информации на высоком логическом уровне не приводит к удалению информации на нижних уровнях, откуда она может быть считана.

Уровень 4

Синтаксический уровень представления информации связан с кодированием. Информация записывается и передается при помощи символов. Символ – это некоторый знак. Которому придается определенный смысл. Линейный набор символов образует алфавит. В процессе кодирования один алфавит может быть преобразован в другой.

Различают несколько уровней кодирования с целью устранения избыточности.

1

2 С целью недоступности информации – криптографическое кодирование

3.

Уровень 5 -Семантический уровень

Одинаковые лексические конструкции могут иметь различный смысл в разном контексте.

Использование профессионализмов многозначных слов и слов значение которых изменилось с течение времени может исказить значение информации.

Основные свойства защищаемой информации.

1 Ценность

2 Секретность (субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации.Эта характеристика обеспечивается способностью системы сохранять указанную информацию в тайне от субъектов не имеющих полномочий на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений информационных отношений.

3 Целостность

4 Доступность

5 Концентрация (суммарное количество информации может оказаться секретным, сводные данные обычно секретнее, чем одиночные

6 Рассеяние – ценная информация может быть разделена на части и перемешана с менее ценной с целью маскировки

7 Сжатие – Возможно сжатие без потери информации, без ее потери, например архивирование. Для уменьшения объема информации или увеличения скорости передачи, применяется сжатие с частичной потерей, используется так же необратимое сжатие (например алгоритм электронной цифровой подписи). Односторонне кэш преобразование

Прагматическое свойство: важность, полнота, достоверность, своевременность, целесообразность, со относимость с фактами, явлениями.

Для удовлетворения законных прав интересов владельцев информации необходимо постоянно поддерживать секретность, целостность и доступность информации.

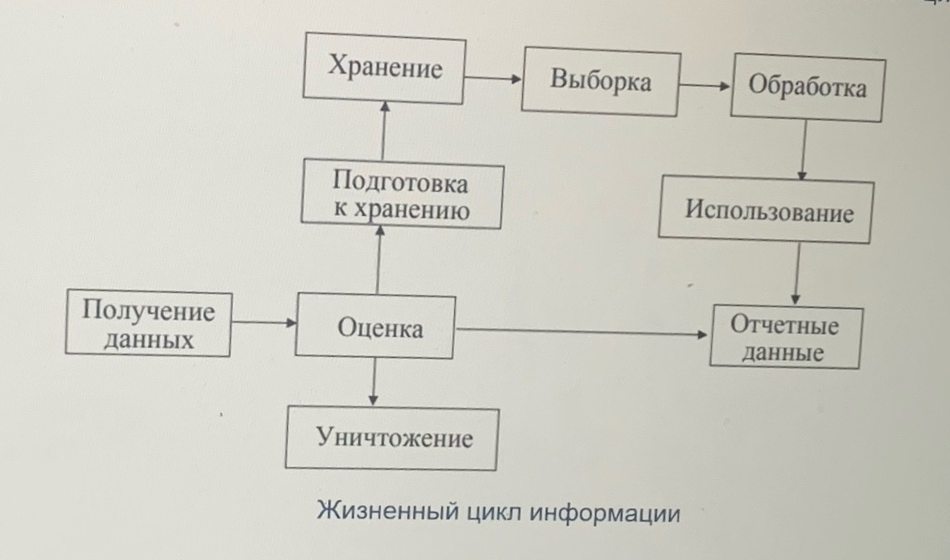
При нарушении хотя бы одного из этих свойств, ценность информации снижается либо теряется.

1 Если ценность теряется при ее раскрытии, то говорят, что имеется опасность нарушения секретности информации.

2 Если ценность теряется при изменении или уничтожении информации, то говорят, что имеется опасность для целостности информации.

3 Если ценность информации теряется при ее неоперативном использовании, то говорят, что имеется опасность нарушения доступности информации.

Ценность информации теряется со временем, к изменению ценности информации приводит ее распространение и ее использование. Характер изменения ценности зависит от вида информации. Для большинства видов можно представить жизненный цикл информации.



Ценность большинства видов информации, циркулирующей в системе, со временем стареет.

Ценность информации просчитывается следующей формулой, где C0 -ценность информации в момент ее возникновения, t-время от момента возникновения информации до момента ее использования. Tж,ц – это продолжительность жизненного цикла информации от момента возникновения до момента устаревания. В соответствии с этим выражением.

Виды и формы представления информации

Любая документируемая информации имеет реквизиты.

1 Наименование

2 Гриф секретности или конфиденциальности

3 Регистрационный номер

4 Дата создания и регистрации

5 Автор или исполнитель

6 Срок действия грифа секретности ли конфиденциальности если таковые имеются

7 Атрибуты учреждения

8 В реквизитах могут указываться адреса рассылки

9 Документированная информации может быть представлена в виде справок решений, заданий, отчетов, ведомостей, приказов, заданий, распоряжений, инструкций, комментариев, писем, чеков, статей и другого. Все эти виды документов могут отличаться по форме. В информационных системах документируемая информация представлена в виде файлов, папок, массивов, баз данных, программ.

В федеральных органах исполнения власти документирование информации осуществляется в порядке установленном правительством Российской Федерации

Структура и шкала ценности информации

Ценность информации может быть стоимостной категории и характеризовать конкретный размер прибыли при ее использовании или размер убытков при ее утрате.

Степень ценности информации и необходимая надежность ее защиты находятся в прямой зависимости.

Информация часто становится ценной в виду ее правового значения для фирмы или развития бизнеса.

Ценность может проявляться в ее перспективном научном, техническом и технологическом значении.

Следует учитывать что документ может быть не только управленческим имеющим в большинстве случаев текстовую табличную или амперную форму. Большие объемы наиболее ценных документов представлены в изобразительной форме: конструкторские документы, картографические, научно-технические, документы на фотографических, магнитных и иных носителях. В соответствии с этим выделяют два вида интеллектуально ценой информации

1 Техническая\технологическая – методы изготовления продукции, программное обеспеченье, производственные показатели, химические формулы, рецептуры, результаты испытаний, данные контроля качества.

2 Деловая – стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы и так далее. По принадлежности к виду собственности информационные ресурсы могут быть государственными или не государственными, находится в собственности граждан, органов гос. Власти, исполнительных органов и т.д.

Защите подлежит любая официальная документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу. Таким образом наличие права собственности на информацию как результат интеллектуальной действенности определяет целесообразность защиты информационных ресурсов. Существует так же экономическая целесообразность защиты информационных ресурсов, основанная на потребительских свойствах информации, прежде всего основанная на ее стоимости.

В соответствии

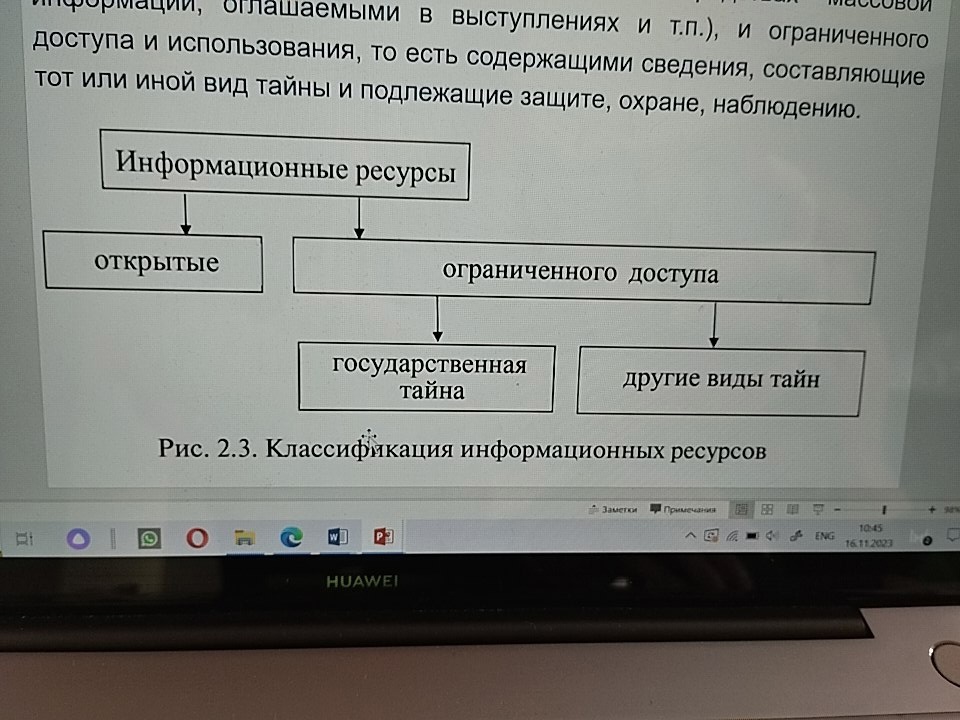
обеспечения интересов национальной безопасности и степенью безопасности государства, а так же правовыми, экономическими и другими интересами, информационные ресурсы могут быть открытыми (используемыми без спец. Разрешения, публикуемыми в средствах массовой информации) и ограниченного доступа и использования, то есть содержащими сведенья, составляющие тот или иной вид тайны и подлежащие защите, охране, наблюдению

Рисунок – информационные ресуры

Запрещается относить к информации ограниченного доступа:

1 Законодательные и другие нормативные акты устанавливающие правовой статус органов гос. Власти, исполнительных органов, органов местного самоуправления и другое.

2 Документы содержащие информацию о чс, экологическую, географическую демографическую санитарно-эпидемиологическую и другую информацию необходимою для обеспечения безлопастного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом.

3 Документы, содержащие информацию о деятельности органов государственной власти, исполнительных органов и органов местного самоуправления об использовании бюджетных средст и других государственных и местных ресурсов. О состоянии и потребности населения.

4 Документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах, органах государственной власти.

Ценная информация охраняется нормами права (патентного, авторского), товарным знаком или защищается включением ее в категорию информации составляющей определенный вид тайны. Для информационных ресурсов ограниченного доступа, вид тайны является определяющем основанием их классификации.

Тайна – это неизвестная, неведомая, непознанная, скрываемая от других, известная не всем информация. Выделяются две глобальные, предметные сферы тайны.

1 Тайны природы – то есть объективные тайны

2 Тайны людей – то есть субъективные тайны

В понятие тайны включается не только документированная информация, а также базы данных, продукция, изделия, технологии, излучения, физические поля. Многообразие форм и субъектов собственности закрепляет за собственником право считать ту или иную ценную информацию тайной.

Состав видов тайны в современном Российском законодательстве, постоянно расширяется. Основными видами тайны являются: государственная, служебная, профессиональная, коммерческая и личная. Каждый из этих видов имеет несколько подвидов.

Государственная тайна – защищаемые государством сведенья в области военной, экономической, политической, разведывательной, контрразведывательной и оперативно-разыскной деятельности.

Служебная тайна – содержит информацию ограниченного распространения, к которой относятся несекретные сведенья, касающиеся деятельности организации, ограничения на распространения которой диктуются.

К служебной информации относятся сведенья, не подлежащие к публикации, использовании в открытых документах, оглашения на конференции, переговорах и выставках.

Профессиональная тайна – инструмент защиты персональных данных о гражданах и личной тайны граждан, имеется в виду что эти сведенья переданы их собственникам или находятся в распоряжении той или иной организации и необходимы ей для выполнения профессиональной деятельности: врачебная тайна, тайна страхования, тайна завещания, тайна голосования, тайна предприятий связи, тайна налоговых органов.

Коммерческая тайна - это информация имеющая ценность . …. Когда к ним нет свободного доступа на законных основания и обладатель этих сведений принимает меры к их охране. Учитывая, что коммерческая тайна отражает в значительной степени торговые секреты, используется термин предпринимательская тайна.

Личная – каждый имеет право на неприкосновенность личной жизни, личную и семейную тайну

Семейная тайна – представляет собой тайну нескольких лиц, связанных родством. Например, имущественное положение, взгляды и убеждения, отношения в семье и тайна факта усыновления

Основные свойства защищаемой информации.

1 Ценность

2 Секретность – субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов имеющих доступ к данной информации

3 Целостность – существование в неискаженном виде

Информация ограниченного доступа формируется в следующих направлениях деятельности предприятия

1 Прогнозирование и планирование деятельности

2 Управление предприятием

3 Финансовая деятельность

4 Торговая деятельность

5 Производственная деятельность

6 Переговоры и совещания по направлениям деятельности предприятия

7 Формирование ценовой политики на продукцию и услуги

8 Формирование состава партнеров, поставщиков и потребителей.

9 Изучение состава конкурентов

10 Участие в торгах и аукционах

11 Научная и исследовательская деятельность по созданию новой техники и технологий

12 Подбор и управление персоналом

13 Организация безопасности предприятия

При определении состава информации ограниченного доступа следует выделять ключевые элементы информации, являющиеся основными носителями секретов. Информация может быть отнесена к коммерческой тайне при соблюдении условий

1 Информация не должна отражать негативные стороны о деятельности предприятия

2 Не должна быть общедоступной или общеизвестной

3 Возникновение или получение информации должно быть законным и связано с расходованием материального, финансового или интеллектуального потенциала предприятия.

4 Персонал должен знать о ценности такой информации и обучен правилам работы с ней.

5 Должны быть выполнены действия по защите этой информации.