**Общество и информация, определение информации**

Появление информации является естественным следствием развития человеческого общества.

В настоящее время информация - один из самых дорогих видов ресурсов. Это проявляется в тенденции стремительного перекачивания трудовых ресурсов из сферы материального производства в информационную.

В настоящее время при обсуждении проблем информации существуют три точки зрения.

-Первая отождествляет понятие «**информация**» со знанием.

-Вторая точка зрения ограничивает предметную область понятия «**информация**» социальными и биологическими процессами, отвергая существование информационных процессов в неорганической природе.

-Третья точка зрения, широко используемая в настоящее время, связана с атрибутивным понятием информации.

Термин «**информация**» происходит от латинского слова «informatio» - разъяснение, изложение, осведомленность.

В широком смысле информация — это общенаучное понятие, включающее в себя обмен сведениями между людьми, обмен сигналами между живой и неживой природой, людьми и устройствами.

Информация — сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые уменьшают имеющуюся о них степень неопределенности, неполноты знаний.

Одновременно информация представляет собой новые сведения, позволяющие улучшить процессы, связанные с преобразованием вещества, энергии и самой информации. Информация неотделима от процесса информирования, поэтому необходимо рассматривать источник информации и потребителей информации.

**Виды и свойства информации, базовые информационные процессы**

**Информация обладает следующими свойствами:**

* всегда существует вещественный или энергетический ее носитель — сигнал;
* в социально-экономических системах она не тождественна своему носителю и данным, она относительна конкретного получателя;
* информация имеет количественные и качественные характеристики, что позволяет автоматизировать управленческий труд;
* информация количественно не изменяется от употребления и может многократно использоваться;
* информация способна накапливаться;
* существование информации определяется ее использованием, неиспользуемые сведения устаревают.

# Виды информации

*научная информация*. Ее делят

- по областям получения или использования на следующие виды: политическая, техническая, биологическая, химическая, физическая и т.д.;

- по назначению - на массовую и специальную.

*документальной информации*.

*экономическую информацию*,

*научно-техническая информация.*

**Экономическая информация, ее виды и особенности**

Экономическая информация отражает процессы производства, распределения, обмена и потребления материальных благ и услуг. В связи с тем, что экономическая информация большей частью связана с общественным производством, ее часто называют *производственной* информацией.

Экономическая информация характеризуется большим объемом, многократным использованием, обновлением и преобразованием, большим числом логических операций и относительно несложных математических расчетов для получения многих видов *результатной* информации.

Структурной единицей экономической информации является *показатель.* Показатель представляет собой контролируемый параметр экономического объекта и состоит из совокупности реквизитов. Реквизит имеет законченное смысловое содержание и потребительскую значимость. *Реквизит* - это логически неделимый элемент показателя, отражающий определенные свойства объекта или процесса. Реквизит нельзя разделить на более мелкие единицы без разрушения его смысла. Каждый показатель состоит из одного реквизита-основания и одного или нескольких реквизитов-признаков. *Реквизит - признак* характеризует смысловое значение показателя и определяет его наименование. *Реквизит-основание* характеризует, как правило, количественное значение показателя.

*По степени обработки информации:*

* + первичная, получаемая в результате наблюдения и фиксации фактов, имеющих отношение к деятельности организации;
  + производная (вторичная, выводная, обобщенная), образующаяся путем переработки первичной;

*По функциональному предназначению:*

* + служебная (производственная);
  + управленческая;

*По источникам получения:*

* + гласная (открытая);
  + конфиденциальная.

**Понятие и виды информационных технологий**

Согласно Закону РБ «Об информатизации» от 06.09.1995 № 3850-XII, **информационные технологии** – это совокупность методов, способов, приемов и средств обработки документированной информации, включая прикладные программные средства, и регламентированного порядка их применения.

Под **компьютерными информационными технологиями** можно понимать компьютерное оборудование и программное обеспечение, предназначенное для получения, хранения и передачи информации.

В состав КИТ входит программное обеспечение.

По функциональному принципу выделяют системное и прикладное ПО.

Под **системным** понимается ПО, включающее в себя операционные системы, которые управляют физическими и логическими ресурсами и процессами вычислительных систем; сетевое ПО для управления общими ресурсами в распределенных вычислительных системах; сервисные программы, расширяющие возможности операционных систем и предоставляющие набор дополнительных услуг.

**Прикладным** называется ПО, предназначенное для решения определенной целевой задачи из проблемной области. Спектр проблемных областей

- Типовое ПО позволяет решать широкий круг задач.

- Специализированное ПО предназначено для решения узких специальных задач.

1. **По типу используемой информации**

- Текстовая информация (текст)

- Числовые, символьные данные

- Графика

-Знание

- Объемы реального мира (они говорят и выглядят)

**2.** **По типу программного обеспечения.**

- системные программы,

- инструментальные средства, используемые для создания отдельных информационных технологий;

- прикладные программы,

***3.*****По способу функционирования**

Функциональные:

Обеспечивающие:

**4.** **По типу пользовательского интерфейса.**

Пользовательский интерфейс

Объектно-ориентированная

**5.** **По методу их взаимодействия между собой.**

- Дискретные технологии

- Сетевые информационные технологии

- базовые

-прикладные.

**Этапы развития информационных технологий**

Информационная технология, в своем развитии, прошла несколько этапов.

**Первый этап - ручной.** В основе информационной технологии были ручка и бухгалтерская книга. Связь осуществлялась путем направления писем. Данный этап характеризовался низкой продуктивностью информационной обработки данных.

**Второй этап - механический.** Характеризуется тем, что для обработки информации стали применять пишущие машинки и телефон.

**Третий этап - электрическая обработка информации.** Для обработки информации использовались электрические пишущие машинки и копировальные машины.

**Четвертый этап - компьютерная технология.** Появление ЭВМ. Информационная технология, содержит как минимум три компоненты обработки информации: учет, анализ и принятие решений и происходит перенос центра тяжести развития автоматизированных систем управления на данные компоненты с максимальным применением человеко-машинных процедур.

**Пятый этап - появление персональных компьютеров.** Происходит переход от вычислительных центров к распределенному вычислительному потенциалу, происходит повышение однородности технологии обработки информации.

**Шестой этап - этап новых информационных технологий**, основу которых составляют:

1. развитые коммуникации;

2. дружественное программное обеспечение;

3. распределенная компьютерная техника.

**Понятие и этапы развития информационной системы**

*Экономическая информационная система (ЭИС)* — это *совокупность внутренних и внешних потоков прямой и обратной информационной связи экономического объекта, методов, средств, специалистов, участвующих в процессе обработки информации и выработке управленческих решений.*

*Автоматизированная информационная система (АИС)* представляет собой *совокупность информации, экономико-математических методов и моделей, технических, программных, технологических средств и специалистов, предназначенную для обработки информации и принятия управленческих решений.*

Создание АИС способствует повышению эффективности производства экономического объекта и обеспечивает качество управления. Наибольшая эффективность АИС достигается при оптимизации планов работы предприятий, фирм и отраслей, быстрой выработке оперативных решений, четком маневрировании материальными и финансовыми ресурсами и т.д

**Структура и классификация информационных систем**

Автоматизированные информационные системы разнообразны и могут быть классифицированы по ряду признаков



# Информационные инфраструктуры

Основополагающими принципами формирования инфраструктуры информационных технологий являются:

1) комплексный подход к изучению спектра функций предприятия с их полной интеграцией;

2) модульный принцип построения, позволяющий легко конфигурировать системы с последующим наращиванием;

3) открытость технологий, способных взаимодействовать с различными внешними системами, обеспечивать выбор программно-технической платформы и переносимость ее на другие аппаратные средства;

4) гибкость настройки модулей системы и адаптация их к потребностям конкретного предприятия;

5) масштабируемость, предусматривающая расширение и усложнение функциональных модулей системы;

6) многопользовательский доступ к данным в режиме реального времени и реализация функций в едином информационном пространстве;

7) моделирование предприятия и его бизнес-процессов, непрерывное развитие и совершенствование системы.

Создание автоматизированной информационной системы предприятия связано с инфраструктурой информационной технологии предприятия. Все функциональные возможности предприятия можно представить в виде двух уровней:

- front-office – модули, которые обеспечивают быстрый и удобный ввод информации, ее первичную обработку и любое внешнее взаимодействие предприятия с клиентами, партнерами;

- back-office – приложения по различным направлениям деятельности внутри предприятия.

**Автоматизированное рабочее место**

Автоматизированное рабочее место индивидуального и коллективного пользования

Тенденция к усилению децентрализации управления влечет за собой распределенную обработку информации с децентрализацией применения средств вычислительной техники и совершенствованием организации непосредственно рабочих мест пользователей.

*Автоматизированное рабочее место (АРМ)* можно определить как *совокупность информационно-программно-технических ресурсов, обеспечивающую конечному пользователю обработку данных и автоматизацию управленческих функций в конкретной предметной области.*

Создание автоматизированных рабочих мест предполагает, что основные операции по накоплению, хранению и переработке информации возлагаются на вычислительную технику, а экономист выполняет часть ручных операций и операций, требующих творческого подхода при подготовке управленческих решений. Персональная техника применяется пользователем для контроля производственно-хозяйственной деятельности, изменения значений отдельных параметров в ходе решения задачи, а также ввода исходных данных в АИС для решения текущих задач и анализа функций управления.

Создание АРМ на базе персональных компьютеров обеспечивает:

• простоту, удобство и дружественность по отношению к пользователю;

• простоту адаптации к конкретным функциям пользователя;

• компактность размещения и невысокие требования к условиям эксплуатации;

• высокую надежность и живучесть;

• сравнительно простую организацию технического обслуживания.

Концептуальное отличие АРМ на базе ПК от просто ПК на рабочем столе пользователя состоит в том, что в АРМ открытая архитектура ПК функционально, физически и эргономически настраивается на конкретного пользователя (персональное АРМ) или группу пользователей (групповое АРМ).

**Система поддержки принятия решений**

Процесс принятия решения предполагает получение информации и знаний об объекте, с которым проводится работа. Зачастую процесс принятия решения происходит в проблемной, неожиданной ситуации. Действие направлено на то, чтобы превратить ее в желательную ситуацию. В этом случае человек, принимающий решение, стремится избежать двусмысленности и достичь определенности. Ему нужно обладать достаточными знаниями для оценки проблемы.

Процесс принятия решений может протекать по двум схемам:

1. интуитивно-эмпирической
2. формально-эмпирической Независимо от схемы протекания процесса принятия решения информационное обеспечение управления является одним из решающих факторов принятия эффективных решений.

При построении модели проблемной ситуации исследуют структуру процесса принятия решения, которая определяется следующими элементами:

- состояние исходных данных задачи;

- модель ситуации принятия решения;

- ограничения;

- варианты решений и их последствия;

- внешние факторы объективного и субъективного характера.

Совокупность этих элементов образует определенную **систему поддержки принятия решений**. Она обеспечивает лицо, принимающее решение, (ЛПР) необходимыми для принятия решения данными, знаниями, выводами, рекомендациями.

**Тактические** информационные системы предназначены для обработки данных и реализации моделей, помогающих решать отдельные, в основном слабо структурированные задачи (например, принятие решения о займе или инвестициях, составление прогнозов и т.п.).

**Стратегические** информационные системы предназначены прежде всего для принятия стратегических решений и используются руководителями высшего ранга.

Еще одна система IS (Inguiring Systems) существует в нескольких вариантах: основаны на рационализме, эмпиризме, диалектическом методе, идеализме каждая из моделей применима для решения определенного круга проблем.

**Метод анализа иерархий**

Объект сам по себе не представляет большого значения. Намного значительнее то, какие действия можно совершать над объектом, и какими свойствами он обладает. *Метод* как раз и представляет собой действие, выполняемое над объектом.

Синтаксис применения метода:

Объект.Метод

В данном примере при помощи метода Quit (закрыть) закрывается приложение (объект Application).

Application.Quit

Метод можно применять ко всем объектам семейства. В данном примере к семейству ChartObjects (диаграммы) рабочего листа лист1 применен метод Delete (удалить), который приводит к удалению всех диаграмм с рабочего листа Лист1:

Worksheets("Лист1").ChartObjects.Delete

**Понятие и виды компьютерных систем**

**Компьютерная сеть (**КС) - это совокупность нескольких компьютеров или вычислительных систем, объединенных между собой средствами телекоммуникаций в целях эффективного использования вычислительных и информационных ресурсов при выполнении информационно-вычислительных работ.

Использование компьютерных сетей предоставило пользователю преимущества, без которых компьютерный мир не мог бы достичь современного прогресса:

> автоматизация обмена информацией и программными средствами между отдельными ПЭВМ;

*>* свободный доступ к обширным информационным ресурсам, накопленным человечеством;

> создание распределенных БД, размещаемых на разных компьютерах;

*>* организация параллельной обработки данных многими пользователями;

> специализация отдельных ЭВМ для эффективного вычисления отдельных классов задач;

> перераспределение мощностей компьютерной техники в зависимости от круга решаемых задач пользователей;

> повышение загрузки компьютерной техники, включая дорогое периферийное оборудование;

> взаимозаменяемость отдельных компьютеров и участков сети, что позволяет быстро восстанавливать работу сети на всех участках;

> сочетание различных режимов работы, включая (пакетный диалоговый и режим-запрос, режим-ответ.

***Все многообразие компьютерных сетей можно классифицировать по некоторым признакам. Прежде всего, различают локальные, глобальные и региональные сети, общая характеристика которых будет дана в этой главе.***

***По принадлежности***

- ведомственные - государственные сети.

***По скорости передачи***

низко-, средне- и высокоскоростные

***По совместимости******компьютерных средств*** различают *гомогенные* и гетерогенные сети.

***По характеру функций***выполняемых в сети,

*- вычислительные сети*

*- информационные сети*

- *смешанные сети*

***По типу организации передачи данных***

*коммутацией каналов, сообщений и пакетов.*

***по территориальному размещению*** на:

***По способу распределения информационных ресурсов се*ти** различают *централизованные, децентрализованные* и *смешанные* формы организации данных.

**Архитектура «клиент-сервер». Локальные вычислительные сети**

В компьютерной технологии, называемой архитектурой «клиент-сервер», программное обеспечение ориентировано не только на коллективное использование ресурсов, но и на их обработку в месте размещения ресурсов по запросам пользователей. Программные системы архитектуры клиент-сервер состоят из двух частей: программного обеспечения ***сервера***и программного обеспечения пользователя - ***клиента****.* Основная идея технологии «клиент-сервер» состоит в том, что функции по обработке информации разделяются между программой-приложением (клиентом) и программой управления базой данных (сервером).

Работа этих систем организуется следующим образом: *программы-клиенты* выполняются на компьютере пользователя и посылают запросы к *программе-серверу,* которая работает на компьютере общего доступа. Основная обработка производится мощным сервером, а на компьютер пользователя посылаются только результаты выполнения запроса. Серверы, используемые в этой технологии, рассчитаны на работу с большими объемами данных и большое число пользователей, поэтому обладают мощными техническими характеристиками. Они обеспечивают высокую производительность, надежность и защищенность. В глобальных сетях архитектура «клиент-сервер» является основной.

**Локальные вычислительные сети**

Под ***локальной вычислительной сетью***(ЛВС) понимают совместное подключение нескольких компьютерных рабочих мест (рабочих станций) к единому каналу передачи данных с помощью соответствующих средств коммуникации.

Возможности ЛВС:

— экономное использование аппаратных средств,

— доступ к данным и управление запросами БД с периферийных рабочих станций, с использованием *разделения данных;*

— возможность одновременного использования централизованных программных средств;

— совместное использование вычислительных мощностей для обработки данных, доступное каждой рабочей станции, благодаря *разделению ресурсов процессора.*

Локальные вычислительные сети подразделяются на *одноранговые {одноуровневые)* и *иерархические (многоуровневые).*

Способ организации и хранения информации на сервере устанавливается специальным лицом — администратором сети. На нем лежит ответственность за сохранность коллективно используемой информации. Для идентификации пользователей каждому из них присваивается уникальное имя и пароль, которые регистрирует администратор сети. Администратор сети также определяет, какие ресурсы сервера являются разделяемыми, какие доступны различным пользователям, и их права доступа. В иерархических сетях возможны как режимы удаленного доступа, так и удаленного управления в зависимости от прав, предоставленных пользователю администратором.

ЛВС классифицируются по назначению:

• сети терминального обслуживания.

• сети, на базе которых построены системы управления производством и учрежденческой деятельности.

• сети, которые объединяют системы автоматизации, проектирования. • сети, на базе которых построены распределенные вычислительные системы;

**Понятие, история развития и ПО интернет**

**Интернет** — сеть сетей, равной которой по мощности нет, и никогда не было. Массовое покорение мира сетью Интернет началось в 1993—1994 гг., с появлением в сети Интернет новой службы (подсистемы) World Wide Web. В настоящее время Интернет — это всемирная сеть, связывающая между собой миллионы компьютеров. Сейчас, по разным оценкам, с Интернет работает свыше 300 миллионов пользователей из разных стран мира и более 40 000 локальных сетей, причем это число лавинообразно увеличивается, по некоторым экспертным оценкам к 2005 г. с Интернет будет работать 2,5 миллиарда пользователей.

*История развития*

В начале 60-х годов прошлого столетия по заданию министерства обороны США был разработан проект по созданию экспериментальной сети передачи пакетов. Сеть, названная ARPANET, предназначалась первоначально для изучения методов обеспечения надежной связи между компьютерами различных типов. Многие методы передачи данных через модемы были разработаны в ARPANET. Идея создания Интернет возникла в связи с необходимостью построения отказоустойчивой сети, которая могла бы продолжать работу, даже если большая часть ее стала неработоспособной. Решение состояло в том, чтобы создать сеть, где информационные пакеты могли бы передаваться от одного узла к другому без какого-либо централизованного контроля. Если основная часть сети не работает, пакеты самостоятельно должны передвигаться по сети до тех пор, пока не достигнут точки своего назначения. Одновременно сеть должна быть достаточно устойчивой к возможным ошибкам при передаче пакетов, т.е. обладать механизмом контроля пакетов и обеспечить наблюдение за доставкой информации.

**Характеристика основных информационных ресурсов Интернет. Интранет. Экстранет**

**Интранет** (интрасеть) — это корпоративная сеть (возможно — сеть офиса, предприятия, лаборатории или кафедры), использующая продукты и технологии Интернета для хранения, связи и доступа к информации.

**Интернет** — сеть сетей, равной которой по мощности нет, и никогда не было. Массовое покорение мира сетью Интернет началось в 1993—1994 гг., с появлением в сети Интернет новой службы (подсистемы) World Wide Web. В настоящее время Интернет — это всемирная сеть, связывающая между собой миллионы компьютеров. Сейчас, по разным оценкам, с Интернет работает свыше 300 миллионов пользователей из разных стран мира и более 40 000 локальных сетей, причем это число лавинообразно увеличивается, по некоторым экспертным оценкам к 2005 г. с Интернет будет работать 2,5 миллиарда пользователей.

Интернет предоставляет пользователям большой спектр информационных услуг:

**Понятие информационной безопастности. Виды угроз информационной безопасности**

информационный компьютерный интернет

**Информационная безопасность** - состояние защищенности информационной среды общества, обеспечение её формирования, использования и развитие в интересах граждан, организаций, государства. Информационная среда - сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов граждан, юридических лиц и государства. Это, в первую очередь, обусловлено потребностью создания развитой и защищенной информационной среды общества. Вместе с тем, через информационную среду осуществляются угрозы национальной безопасности в различных сферах жизнедеятельности личности, общества и государства.

Под ***угрозой безопасности информации*** понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

***Виды угроз информационной безопасности***

Среди угроз безопасности информации следует выделять как один из видов угрозы *случайные,* или *непреднамеренные.*

***Виды умышленных угроз безопасности информации***

*- Пассивные угрозы*

*- Активные угрозы* имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты.

Умышленные угрозы подразделяются также на ***внутренние***(возникающие внутри управляемой организации) и ***внешние.***

***К основным угрозам безопасности информации и нормального функционирования ИС относятся:***

■ утечка конфиденциальной информации;

■ компрометация информации;

■ несанкционированное использование информационных ресурсов;

■ ошибочное использование информационных ресурсов;

■ несанкционированный обмен информацией между абонентами;

■ отказ от информации;

■ нарушение информационного обслуживания;

■ незаконное использование привилегий.

*Утечка конфиденциальной информации* — это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

■ разглашения конфиденциальной информации;

■ ухода информации по различным, главным образом техническим, каналам;

■ несанкционированного доступа к конфиденциальной информации различными способами.

**Факторы угроз информационной безопасности**

*факторы, которые необходимо учитывать при оценке реального состояния информационной безопасности и определении ключевых проблем в этой области. По Вирковскому В. А., факторы угроз информационной безопасности можно разделить на политические, экономические и организационно-технические их виды.*

**Политическими факторами угроз информационной безопасности являются:**

- изменение геополитической обстановки

- информационная экспансия

- становление новой государственности в странах СНГ на основе принципов демократии, законности, информационной открытости;

- разрушение ранее существовавшей командно-административной системы государственного управления, а также сложившейся системы обеспечения безопасности;

- нарушение информационных связей

- стремление стран СНГ к более тесному сотрудничеству с зарубежными странами в процессе проведения реформ на основе максимальной открытости сторон;

- низкая общая правовая и информационная культура в обществе.

**Среди экономических факторов угроз информационной безопасности** наиболее существенными являются:

- переход на рыночные отношения в экономике

- критическое состояние отечественных отраслей промышленности, производящих средства информатизации и защиты информации;

- расширяющаяся кооперация с зарубежными странами в развитии информационной инфраструктуры

**Из организационно-технических факторов угроз информационной** безопасности ключевыми являются:

- недостаточная нормативно-правовая база в сфере информационных отношений

- слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг;

- широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств для хранения, обработки и передачи информации;

- рост объемов информации, передаваемой по открытым каналам связи, в том числе по сетям передачи данных и межмашинного обмена;

- обострение криминогенной обстановки, рост числа компьютерных преступлений, особенно в кредитно-финансовой сфере.

**Иерархическая классификация угроз информационной безопасности**

Региональные факторы угроз информационной безопасности

Локальные факторы угроз информационной безопасности

**Оценка безопасности информационных систем. Методы и средства построения информационной безопасноти, их структура**

Создание систем информационной безопасности (СИБ) в ИС и ИТ основывается на следующих принципах:

*Системный*

*Принцип непрерывного развития системы.*.

*Разделение и минимизация полномочий*

*Полнота контроля и регистрации попыток* несанкционированного доступа

*Обеспечение надежности системы защиты*

*Обеспечение контроля за функционированием системы защиты*

*Обеспечение всевозможных средств борьбы с вредоносными программами.*

*Обеспечение экономической целесообразности использования системы защиты*

Система информационной безопасности, как и любая ИС, должна иметь определенные виды собственного программного обеспечения, опираясь на которые она будет способна выполнить свою целевую функцию.

1. *Правовое обеспечение*

2. *Организационное обеспечение.*

3. *Информационное обеспечение*

4. *Техническое (аппаратное) обеспечение.*

5. *Программное обеспечение.*

6. *Математическое обеспечение.*

7. *Лингвистическое обеспечение.*

8. *Нормативно-методическое обеспечение.*

Обеспечение и контроль безопасности представляют собой комбинацию технических и административных мер.

Методы и средства обеспечения безопасности информации в ИС схематически представлены на рисунке 1.

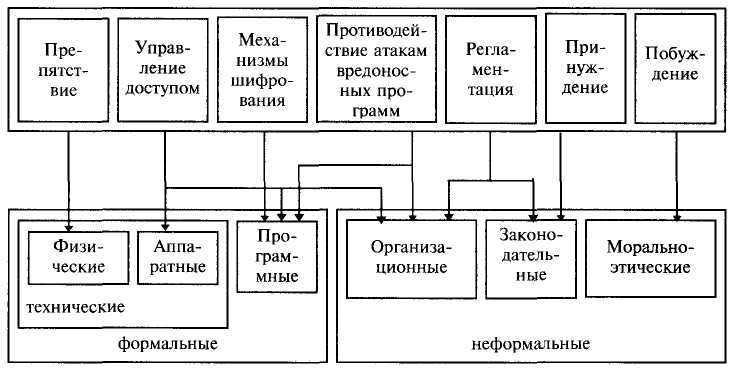


Рисунок 1 - Методы и средства обеспечения безопасности информации

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

*Управление доступом —* методы защиты информации регулированием использования всех ресурсов ИС и ИТ.

*Механизмы шифрования —* криптографическое закрытие информации.

*Противодействие атакам вредоносных программ*

*Регламентация —* создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

*Принуждение* — метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

*Побуждение* — метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на аппаратные и физические.

*Аппаратные средства* — устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

*Физические средства* включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

*Программные средства* — это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Как отмечалось, многие из них слиты с ПО самой ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Криптография — это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

*Организационные средства* осуществляют регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе

*Законодательные средства* защиты определяются законодательными актами страны

*Морально-этические средства* защиты включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются.

**Обеспечение информационной безопасности: правовое, организационно-экономическое, программно-техническое обеспечение защиты информационной безопасности**

Программно-техническая подсистема защиты автоматизированных информационных систем, какой бы совершенной она ни была, в полном объеме не решает задач комплексной защиты объектов информационной безопасности. Используемые данной подсистемой физические, аппаратные, программные, криптографические и иные логические и технические средства и методы защиты выполняются без участия человека по заранее предусмотренной процедуре. Для обеспечения комплексного подхода к проблеме программно-техническое обеспечение защиты объектов информационной безопасности должно быть дополнено соответствующим правовым обеспечением.

**Уголовно-правовая защита от компьютерных преступлений**

принятие законодательных актов по уголовно-правовому регулированию этих отношений. Впервые были приняты такие законы в середине 70-х годов в отдельных штатах США.

За правонарушения при работе с документированной информацией органы государственной власти, организации и должностные лица несут ответственность в соответствии с действующим законодательством.

Организационно-экономическое обеспечение информационной безопасности

Организационно-экономические методы защиты информации предусматривают формирование и обеспечение функционирования следующих механизмов защиты:

- стандартизации методов и средств защиты информации;

- сертификации компьютерных систем и сетей по требованиям информационной безопасности;

- лицензирования деятельности в сфере защиты информации;

- страхования информационных рисков, связанных с функционированием компьютерных систем и сетей;

- контроля за действием персонала в защищенных информационных системах.

Организационные методы защиты информации делятся на организационно-административные и организационно-технические методы защиты.

**Организационно-административные методы защиты информации**

Они регламентируют процессы создания и эксплуатации автоматизированных информационных систем, а также взаимодействие пользователей и систем таким образом, что несанкционированный доступ к информации становится либо невозможным, либо существенно затрудняется. Организационные методы зашиты информации охватывают все компоненты автоматизированных информационных систем на всех этапах их жизненного цикла: проектирования систем, строительства зданий, помещений и сооружений, монтажа и наладки оборудования, эксплуатации и модернизации систем.

# Программно-техническое обеспечение защиты информационной безопасности

Программно-техническая подсистема комплексной защиты объектов информационной безопасности включает: физические, аппаратные, программные, аппаратно-программные, криптографические методы и средства защиты информации. Остановимся на краткой характеристике методов и средств данной подсистемы защиты с учетом эволюции моделей информационных систем и тенденций развития технологии обеспечения безопасности в компьютерных сетях.

**Защита информации в корпоративных сетях информационных систем управления**

Создание системы защиты информации в корпоративной сети ИС порождает целый комплекс проблем. В комплексе корпоративная система защиты информации должна решать следующие ***задачи:***

1) обеспечение конфиденциальности информации;

2) защита от искажения;

3) сегментирование (разделение на части) и обеспечение индивидуальности политики безопасности для различных сегментов системы;

4) аутентификация пользователей — процесс достоверной идентификации отождествления пользователя, процесса или устройства логических и физических объектов сети для различных уровней сетевого управления;

5) протоколирование событий, дистанционный аудит, защита, регистрационных протоколов и др.

Построение системы информационной безопасности сети основывается на семиуровневой модели декомпозиции системного управления OSI/ISO. *Семь уровней сетевого управления включают: физический, канальный, сетевой, транспортный, сеансовый, представительский, прикладной уровни.*

На *физическом уровне,* представляющем среду распространений данных (кабель, оптоволокно, радиоканал, каналообразующее оборудование), применяют обычно средства шифрования или сокрытия, сигнала. Они малоприменимы в коммерческих открытых сетях, так как есть более надежное шифрование.

На *канальном уровне,* ответственном за организацию взаимодействия двух смежных узлов (двухточечные звенья), могут быть использованы средства шифрования и достоверной идентификации пользователя. Однако использование и тех и других средств на этом уровне может оказаться избыточным. Необязательно производить (пере-) шифрование на каждом двухточечном звене между двумя узлами.

*Сетевой уровень* решает задачи распространения и маршрутизации пакетов информации по сети в целом. Этот уровень критичен в отношении реализации средств криптозащиты. Понятие пакета существует на этом уровне. На более высоких уровнях есть понятие сообщения. Сообщение может содержать контекст или формироваться на прикладном уровне, защита которого затруднена с точки зрения управления сетью. Сетевой уровень может быть базовым для реализации средств защиты этого и нижележащих уровней управления. К ним относятся: *транспортный* (управляет передачей информации), *сеансовый* (обеспечивает синхронизацию диалога), *уровень представлений* (определяет единый способ представления информации, понятный пользователям и компьютерам), *прикладной* (обеспечивает разные формы взаимодействия прикладных процессов).

Таким образом, архитектурную концепцию системы защиты информации в сетях можно представить в виде трех слоев: средства защиты сетевого уровня, middleware-системы и средства защиты, предлагаемые прикладными системами.

**Этапы разработки систем защиты**

При первоначальной разработке и реализации системы защиты ИС обычно выделяют три стадии.

*Первая стадия* — выработка требований

На *второй стадии —* определение способов защиты — принимаются решения

*Третья стадия* — построение системы информационной безопасности

***Процесс организации защиты информации по методу Opsec проводится регулярно и каждый раз поэтапно.***

*Первый этап* (анализ объекта защиты) состоит в определении того, что нужно защищать.

*Второй этап* предусматривает выявление угроз:

На *третьем этапе* проводится анализ эффективности принятых и постоянно действующих подсистем обеспечения безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т.д.).

*На четвертом этапе* определяются необходимые меры защиты. На основании проведенных на первых трех этапах аналитических исследований вырабатываются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.

На *пятом этапе* руководителями фирмы (организации) рассматриваются представленные предложения по всем необходимым мерам «безопасности и расчеты их стоимости и эффективности.

*Шестой этап* состоит в реализации принятых дополнительных мер безопасности с учетом установленных приоритетов.

*Седьмой этап* предполагает контроль и доведение до персонала фирмы реализуемых мер безопасности.