1. Структура процессов управления включает в себя:
    - Управляющий объект (УО);
    - Объект управления (ОУ);
    - Каналы связи.

Управляющий объект (УО) - предназначен для выработки информационных воздействий на основе обработки и отображения собранной информации. В роли УО могут выступать объекты, способные воспринимать, хранить, перерабатывать и выдавать информацию.

Объект управления (ОУ) - обеспечивает выдачу информации о своем состоянии и состоянии внешней среды, восприятие информационных воздействий от УО и их реализацию.

Каналы связи служат для обмена информацией между УО и ОУ.

Теория управления силами наряду с теорией систем является тем фундаментом, на котором базируется теория автоматизации управления.

2. Теория управления силами (ТУС) - это часть военной науки, которая объединяет все общее, что присуще управлению в различных областях военного дела. Она базируется на общих принципах вооруженной борьбы и принципах военного управления.

Предмет теории управления силами:

основные положения, категории, законы (закономерности) и принципы управления силами;

организационные формы и методы управления силами;

системы управления силами.

Функции теории управления:

познавательная функция - проявляется в раскрытии сущности процессов управления, их закономерностей и принципов;

прогнозирующая функция - определение основных тенденций и направлений дальнейшего развития процессов в управляемой системе, основа предвидения в управлении.

3. Методы управления классифицируются по нескольким признакам:

а) по характеру воздействия на личный состав метод может быть директивным и стимулирующим;

б) по характеру постановки задач личному составу методы делятся: на непосредственное воздействие и косвенное воздействие;

в) по характеру отношений между командирами и подчиненными методы разделяются на организационно-административные, распорядительные, экономические, морально-психологические и правовые.

Директивный метод предполагает прямое волевое воздействие командиров на подчиненных путем отдачи приказов, распоряжений и указаний в рамках прав, предоставленных им действующими уставами, наставлениями, инструкциями и т.п.

Стимулирующий метод основывается на использовании моральных, психологических, экономических и других стимулах и имеет цель обеспечить наилучшее выполнение подчиненными полученных задач. С их помощью повышаются активность и инициатива личного состава в выполнении служебного долга. К стимулирующим методам относятся: проведение собраний и индивидуальных бесед с личным составом, поощрение и награждение отличившихся, популяризация их в печати и др.

Непосредственное воздействие командира на подчиненных осуществляется единолично, минуя заместителей и других должностных лиц. Например, постановка командиром взвода задачи какому-либо солдату напрямую минуя командира отделения.

Косвенное воздействие характеризуется тем, что командир ставит задачи в порядке подчиненности. Непосредственное воздействие целесообразно только в случае крайней необходимости.

Организационно-административные методы имеют цель обеспечить постоянное воздействие вышестоящих органов на подчиненные звенья управления. В военной организации эти методы закреплены всем укладом жизни и службы. Они заложены в принципе единоначалия, которое выражается в праве командира (начальника), исходя из всесторонней оценки обстановки, единолично принимать решения, отдавать соответствующие приказы в строгом соответствии с требованиями законов и воинских уставов и обеспечивать их выполнение.

Распорядительный метод обеспечивает оперативное воздействие на всю систему управления путем перераспределения сил и средств в ходе решения частных или внезапно возникающих задач. Он реализуется в приказах и распоряжениях, отдаваемых устно или письменно.

Экономические методы занимают одно из ведущих мест и представляют собой взаимосвязанную систему материального воздействия на все стороны жизнедеятельности подразделения. Имея в своем распоряжении значительные материальные средства, командир и подчиненные ему органы управления в процессе управления должны соблюдать их экономное использование.

4. Принципы управления войсками – это наиболее общие основополагающие требования к содержанию, организации и осуществлению управления, которые должны учитываться и выполняться в практической деятельности командира.

По своему назначению принципы управления являются связующим звеном между основой теории и практикой управления. К ним можно отнести:

единоначалие;

личную ответственность командиров за принимаемые решения;

централизацию управления во всех звеньях с предоставлением инициативы в определении способов выполнения задач;

твердость и настойчивость в проведении принятых решений и планов;

оперативность и гибкость реагирования на изменения обстановки.

5. Сущность принципа единоначалия заключается в том, что командир наделяется всей полнотой распорядительной власти по отношению к подчиненным и несет полную ответственность за все стороны жизни и деятельности вверенных ему подразделений.

Объединяя в своих руках всю полноту власти, командир несет личную ответственность за постоянную боевую и мобилизационную готовность подчиненных ему подразделений и успешное выполнение ими поставленных задач.

Централизация управления позволяет командиру в короткие сроки и наилучшим образом координировать боевую и повседневную деятельность подчиненных подразделений, контролировать выполнение ими задач, а в случае необходимости брать управление на себя. При этом наиболее полно используются высокая компетентность, осведомленность и практический опыт командира, его возможность в выработке и принятии обоснованного решения и последовательном проведении его в жизнь.

6. К общим функциям управления относятся: планирование, контроль, оперативное управление (регулирование) и учет. Все функции взаимосвязаны – изменение в одной из них сразу же влияет на другие.

Функции планирования и оперативного управления являются основными.

Планирование заключается в определении, исходя из состояния объекта управления и среды, требуемых ресурсов и порядка их использования по достижению поставленной цели. Результатом планирования является план.

Планирование делится на долгосрочное (стратегическое, перспективное), среднесрочное (оперативное) и краткосрочное (тактическое, текущее).

Контроль направлен на выявление отклонений между фактическими и запланированными значениями показателей функционирования управляемого объекта, а также на выяснение причин обнаруженных отклонений и возможностей их устранения. Как говорил А. Файоль, существо функции контроля «состоит в подтверждении того, что все идет в соответствии с принятым планом, существующими директивными документами и принятыми принципами управления». Функция контроля позволяет также не только выявлять, но и предупреждать отклонения и ошибки.

Контроль может проводиться периодически или непрерывно. Различают три вида контроля: предварительный, текущий и заключительный.

Оперативное управление (управление в ходе операции, регулирование) предполагает оценку выявленного при контроле несоответствия фактических значений показателей функционирования управляемого объекта плановым значениям и выработку корректирующих воздействий для вывода его на запланированную линию поведения.

Учет заключается в фиксации, накоплении и частичной (первичной) обработке информации о состоянии объекта управления и среды.

7. Различают следующие виды управления: командное, адаптивное, ситуационное и рефлексивное.

При командном управлении поведение управляемого объекта формируется на основе приема и выполнения команд. Это самый простой вид управления. Необходимыми условиями его реализации выступают:

высокая информированность управляющего объекта об управляемом объекте и среде;

высокая оперативность и устойчивость информационного обмена между управляющим и управляемым объектами;

высокая точность приема и выполнения команд управляемым объектом.

Адаптивное управление основывается на способности управляемого объекта менять свое поведение с целью сохранения, улучшения или приобретения новых характеристик в условиях меняющейся во времени среды, априорная информация о которой является неполной.

Для ситуационного управления характерна привязка к типовым ситуациям, которые возникают при функционировании управляемых объектов. Перечень типовых ситуаций выявляется заранее. На каждую типовую ситуацию определяется набор описывающих ее признаков и подлежащая выполнению в случае ее возникновения команда.

Рефлексивное управление состоит в выработке и передаче управляемому объекту оснований (мотивов) для принятия им решений (вырабатываются не готовые команды, а стимулы). Чтобы стимулировать выработку командной информации, определяющей движение к цели, управляющий объект должен иметь информацию об управляемом объекте и среде такого объема, который позволяет предвидеть его возможные действия по стимулам.

8. В зависимости от степени использования априорной и текущей информации о состоянии управляемых объектов и среды выделяют следующие способы управления: программное управление, управление по возмущениям и управление по состоянию.

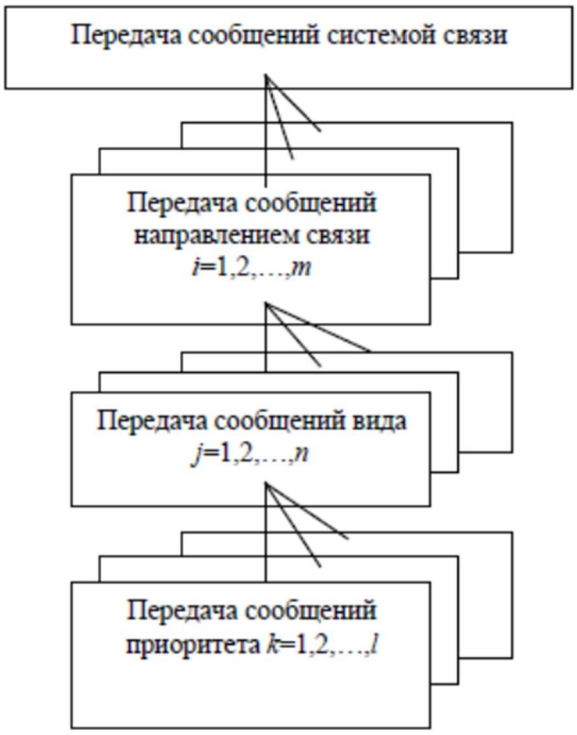
Программное управление – способ управления, при котором управляющие воздействия вырабатываются на весь период достижения цели и вводятся в систему заранее. Принимаемая однократно последовательность управляющих воздействий есть не что иное, как программа. Для реализации программного способа управления достаточно иметь только каналы прямой связи.

Управление по возмущениям – способ управления, при котором управляющие воздействия вырабатываются на основе текущих возмущений среды. При использовании данного способа управляющий объект производит измерения возмущений и с их учетом формирует управляющие воздействия (рис. 5). Изменилось состояние среды – соответствующим образом меняется управляющее воздействие.

Управление по состоянию – способ управления, при котором управляющие воздействия вырабатываются на основе выяснения различий между действительным и требуемым состояниями управляемого объекта. Механизмом, позволяющим контролировать управляемый объект, выступает обратная связь (рис. 6). Благодаря наличию обратной связи становится возможным получать информацию о текущем состоянии управляемого объекта и тем самым определять отклонения его от намеченной линии поведения. Комбинирование способов управления.

9. Решение принимается на операцию. Под операцией понимается этап функционирования системы с управлением, ограниченный достижением определенной цели. Пока не задана цель, говорить об операции неправомерно. Для примера можно привести такие операции, как развёртывание подвижного комплекса средств автоматизации, передача сообщений в сети передачи данных, отладка программы на компьютере. К началу операции система должна иметь соответствующие ресурсы. В зависимости от содержания операции ресурсами выступают люди, материалы, энергия, транспортные средства, деньги, время и т.д.

Операции могут быть простыми и составными. Простая операция не подвергается декомпозиции в рамках данного рассмотрения, составная – может быть представлена в виде совокупности взаимосвязанных простых операций. Примером составной операции является передача сообщений системой связи. Ее можно разбить на ряд операций по направлениям связи, виду и приоритету сообщений (рис.).



В каждом направлении связи передаются сообщения различных видов (телефонные, телеграфные, телекодовые). Для передачи каждого вида сообщений вводятся определенные приоритеты. Простая операция будет представлять собой передачу сообщений в одном направлении связи, одного вида и одного приоритета.

10. Выбор оптимального решения предполагает:

1) установление существования оптимального решения. Прежде чем искать оптимальное решение, целесообразно убедиться в его существовании. Вопрос существования оптимального решения имеет два аспекта:

выявление хотя бы одного допустимого решения;

установление факта достижения оптимума (максимума или минимума);

2) определение необходимых условий оптимальности. Необходимые условия позволяют выделить в множестве допустимых решений некоторое подмножество, к которому принадлежит оптимальное решение и тем самым облегчить его выбор;

3) определение достаточных условий оптимальности. Решение, удовлетворяющее достаточным условиям, является оптимальным;

4) разработку алгоритма выбора оптимального решения.

11. Выработка решений осуществляется группой исследования операций в следующем составе:

- лицо, принимающее решение;
- эксперты;
- операционалисты.

Лицо, принимающее решение (ЛПР) – должностное лицо (группа лиц) органа управления, имеющее цель, которая предопределяет операцию и поиск решения для нее, наделенное необходимыми полномочиями и несущее ответственность за принятое решение. В функции ЛПР

входит предоставление информации об условиях проведения операции, выделение множества допустимых решений и формулирование принципов оптимальности.

Эксперты – специалисты, достаточно компетентные по исследуемому типу операции. На них возлагается оценка условий проведения операции и альтернативных решений. Они не несут прямой ответственности за принятое решение, но отвечают за свои оценки и рекомендации.

Операционалисты – специалисты по исследованию операций, призванные организовывать действия ЛПР и экспертов и осуществлять информационно–аналитическую работу в интересах выработки решения (выбор или разработку моделей, проведение исследований на моделях, формирование процедуры выбора решения).

12. Процесс выработки решений организуется в виде совокупности этапов, имеющих прямые и обратные связи. Наличие обратных связей отражает итеративный характер процесса. При выполнении этапов решаются такие общие задачи информационной деятельности, как поиск, обобщение, распознавание, классификация, упорядочение и выбор.

В процессе выработки решений в системах управления выделяются следующие этапы

Анализ условий проведения операции.

При анализе данных условий основное внимание уделяется тому, чтобы уяснить до конца цель.

Построение модели функционирования системы при проведении операции. Процесс построения модели является весьма трудоемким и требует четкого понимания особенностей рассматриваемой системы. С помощью моделирования получают оценки решений и выбирают лучшее из них.

Выбор оптимального решения в рамках построенной модели. Выбор решения предполагает наличие двух компонентов: множества допустимых решений (предмета выбора) и некоторой совокупности правил упорядочения этих решений по предпочтительности (мотивов выбора).

Формирование принимаемого решения. Полученное при моделировании оптимальное или близкое к нему решение является таковым только в рамках построенной формальной модели и должно рассматриваться как рекомендуемый вариант, который требует, естественно, осмысления и зачастую последующей корректировки.

13. Военная наука следующим образом определяет цели и сущность управления войсками.

Сущность управления войсками заключается в деятельности командиров, штабов и других органов по поддержанию боевой готовности и боеспособности войск, подготовке войск к боевым действиям и руководству ими при выполнении поставленных задач.

Основная цель управления войсками – обеспечить максимальную эффективность использования подчиненных войск и решений поставленных задач в операции (бою) в различных условиях обстановки. Достижение этой цели связано с решением целого круга задач, составляющих содержание управления войсками.

Важнейшими из них являются:

- Поддержание высокой мобилизационной и боевой готовности войск.
- Непрерывное добывание, сбор, изучение, отображение и анализ данных обстановки (сведения о своих войсках, о противнике, внешних условиях) и предвидение возможных ее изменений.
- Выработка и принятие решений на операцию (бой).

- Доведение задач до подчиненных войск.
- Планирование операции (боя).
- Организация и поддержание непрерывного взаимодействия войск. Взаимодействие организуется по задачам, направлениям, способам и времени; оно постоянно поддерживается в ходе операции (боя) в соответствии со складывающейся обстановкой.
- Организация мероприятий по всем видам обеспечения войск.
- Организация контроля и помощи подчиненным, командирам, начальникам, штабам и войскам при подготовке и в ходе выполнения поставленных задач (операции, боя).

14. В управлении войсками действуют как общие законы войны и вооруженной борьбы, так и специфические законы управления.

Общие законы войны отражают наиболее существенные связи и отношения между войной и другими явлениями общественной жизни: зависимость войны от политических целей государств, зависимость хода и исхода войны от соотношения экономических, научных, моральных и собственно военных потенциалов противоборствующих сторон.

Специфические законы управления выражают наиболее существенные связи и отношение различных сторон управления между собой и с элементами внешней среды. Можно выделить следующие наиболее общие закономерности управления войсками:

Зависимость организационных форм и методов управления от структуры Вооруженных Сил, материально-технической базы и условий управления.

Совместимость технических средств и систем управления соподчиненных и взаимодействующих войск.

Соответствие необходимого и располагаемого времени при решении задач управления.

Зависимость эффективности решения задач управления от объема используемой информации.

Отметим два основополагающих принципа управления войсками.

1. В любых условиях обстановки управление войсками осуществляется командующим, командиром, начальником лично и через штаб, а также через своих заместителей, начальников служб в соответствии с приказами, директивами, с указаниями вышестоящих начальников.

2. Основой управления войсками является решение командующего, командира, начальника.

15. Анализ показывает, что управленческая деятельность с одной стороны представляет собой, совокупность последовательно выполняемых офицерами органов управления работ, объединенных единством цели и общностью решаемых задач по управлению, а с другой – совокупностью тесно связанных между собой организационных форм работы, методических приемов непосредственного решения задач управления и субъективных качеств должностных лиц органов управления. Все эти стороны в конечном итоге составляют технологию управленческой деятельности (технология – от греч. «techno» – мастерство, умение и «логос» − учение – является учением (набором правил) о способах достижения положительного результата в некоторой области деятельности). В соответствии с содержанием управленческой деятельности, процесс управления войсками в общем случае складывается из последовательной реализации комплекса ряда взаимосвязанных этапов. Эти этапы составляют цикл управления, который охватывает комплекс мероприятий, выполняемых командирами и органами управления с учетом конкретных условий обстановки.

В общем случае, каждый цикл управления слагается из следующих этапов:

- Сбора и обработки информации о противнике, своих войсках, состоянии боевых средств, специальной техники, средств управления и связи, окружающей обстановке.
- Уяснения задачи управления и оценки обстановки.
- Планирования боевых действий войск в условиях изменившейся обстановки.
- Выработки и принятия решения по управлению войсками.
- Формирования управляющих сигналов, команд, распоряжений, приказов.
- Доведения управляющих сигналов, команд, приказов и распоряжений до подчиненных войск.
- Контроля доведения и исполнения приказов и распоряжений.

16. Характерными особенностями войск как целостных системных формирований являются:

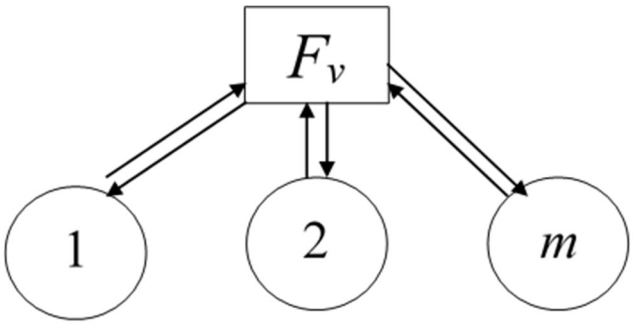
- Способность осуществить целенаправленный выбор своего поведения.
- Большое число и разнообразие входящих в войска элементов, связей между этими элементами.
- Сложная иерархическая структура, сочетание принципов централизованного и децентрализованного управления.
- Сложность выбора поведения в условиях существенной неопределенности, воздействия со стороны противника.
- Циркуляция в войсках больших информационных, энергетических и материальных потоков.
- Интенсивный обмен с внешней средой, особенно в конфликтных ситуациях.
- Наличие биологических подсистем, непосредственная связь с различными социальными системами и вполне определенное отношение к ним.
- Сложность развития вооруженных сил.
- Деятельность войск делится на два различающихся периода: период мирного времени и период ведения боевых действий. Между этими периодами нет полной преемственности. Учения, игры и другие модели боевых действий неспособны отразить все, что может иметь место в ходе реальных активных боевых действий.
- Целью деятельности войск является не созидание, а разрушение − уничтожение агрессора.
- В процессе вооруженной борьбы управление войсками связано с расходованием особого вида ресурса – человеческих жизней (военнослужащих).
- Результаты деятельности войск часто трудно оценить экономически (например, человеческие жизни).

Указанные особенности дают основания отнести войска к большим системам и определяют необходимость рассмотрения их с системных позиций.

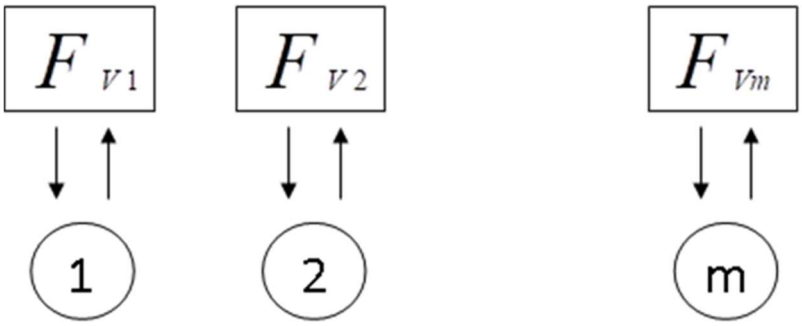
17. В реальных СУВ, имеющих, как правило, сложную иерархическую структуру, управляющие объекты могут взаимодействовать с одним или с несколькими объектами управления. Кроме того, могут выступать как в качестве управляющего органа, так и в качестве подчиненных, управляемых объектов по отношению к объектам более высокого иерархического уровня.

В зависимости от характера связей между управляющими и управляемыми объектами, числа уровней иерархии в системе управления, можно выделить три основных типа структуры управления:

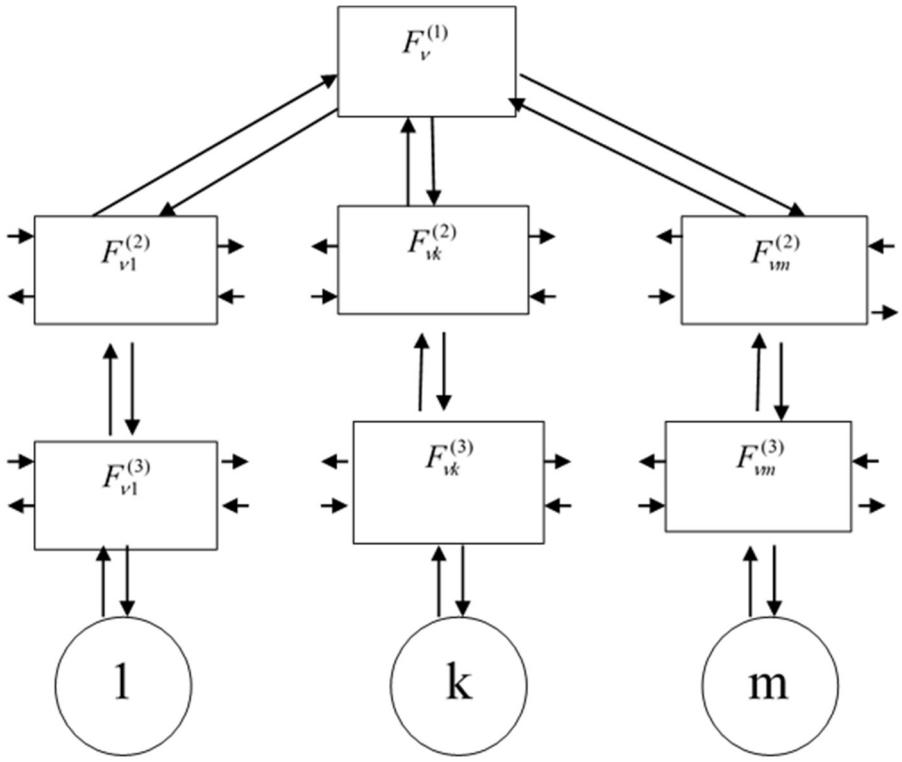
1. Централизованная структура управления (рис.1.2) характеризуется тем, что в ней все функции управления задаются множеством частных алгоритмов управления



2. Децентрализованная структура управления () Для такой структуры управления характерно отсутствие взаимных связей между частными парами «объект управления – управляющий объект»..



3. Иерархическая структура управления. Иерархическая структура управления представляет собой разновидность централизованных структур, в которой все частные алгоритмы управления реализуются несколькими соподчиненными органами управления с одновременным соблюдением принципа централизации управления.



18. К общим основополагающим требованиям к управлению войсками относятся: устойчивость, оперативность, качество управления, скрытность.

1. Устойчивость (от лат. Stabilitas – устойчивость, стабильность, прочность, надежность, неизменность) – комплексное свойство системы управления войсками, характеризуемое живучестью, надежностью, помехоустойчивостью.

Таким образом, под устойчивостью управления войсками как процесса функционирования СУВ – следует понимать свойство системы сохранять свою работоспособность в условиях действия любых возмущающих воздействий.

- Живучесть – это свойство системы, характеризующее ее способность выполнять свои функции в условиях воздействия средств поражения противника и стихийных воздействий природной среды катастрофического характера.
- Надежность – это свойство системы сохранять во времени в установленных пределах значения всех параметров, характеризующих ее способность выполнять требуемые функции в заданных режимах и условиях применения.
- Помехоустойчивость – это свойство системы, характеризующее ее способность выполнять свои функции при воздействии любых видов помех.

2. Оперативность – это свойство системы, характеризующее способность управляющего органа (командования, штаба, пункта управления и др.) обеспечивать реализацию цикла управления за установленное время.

3. Качество управления – это свойство системы управления войсками, характеризующее способность системы вырабатывать и принимать оптимальные или близкие к оптимальным решения (правильное решение).

4. Скрытность управления – это свойство СУВ противостоять раскрытию противником факта существования системы управления, ее функционирования, мест дислокации ПУ, КП, факта передачи информации и ее содержания.

Также важным является требования к СУВ по глобальности, мобильности, непрерывности, пропускной способности, адаптивности.

19. Согласно этим требованиям системы управления военного назначения должны функционировать во всех видах военного управления и уровней его иерархии, в мирное и военное время по видам и родам ВС, родам войск видов ВС, специальным и другим войскам и войсковым формированиям ВС страны. Они должны отвечать общим требованиям, которые предъявляются к ним, особенно в отношении целостности, целеобусловленности, работоспособности, делимости, интегративности, комплексности, адекватности, и полностью вписываться в структуру вышестоящих систем.

Любая СУВ должна находится в постоянной готовности к боевому (учебно-боевому) применению и обеспечивать:

- возможность функционирования своих подсистем и входящих в их состав элементов при различной степени централизации управления в любом уровне иерархии управления;
- высокую оперативность, устойчивость, непрерывность, скрытность, адекватность, адаптивность, и мобильность действий своих элементов;
- проведения комплекса мероприятий по снижению демаскирующих признаков элементов системы и повышению их помехоустойчивости;
- автоматизацию процесса управления;

- обмен информацией со всеми сопрягаемыми (вышестоящими, подчиненными, соседними-взаимодействующими) системами;
- управление штатными и приданными объектами управления при выходе из строя отдельных управляющих элементов системы;
- гарантированную защиту информации от несанкционированного доступа (НСД), несанкционированного использования средств связи, электронного, информационного и программного поражения;
- информационно-лингвистическую, программную, техническую, организационную, методическую и иную совместимость всех элементов системы и сопрягаемых элементов других систем, а также синхронизацию единого времени.

20. Объекты управления СУВН должны:

- функционировать в автоматизированном контуре управления войсками (силами) и оружием;
- быть информационно, лингвистически, технически и в ином отношении совместимыми с соответствующими ПУ, между собой и объектами других систем;
- осуществлять поиск, обнаружение, распознавание, определение координат, размеров, степени защищенности и других характеристик объектов противника (в соответствии с техническими возможностями и условиями обстановки);
- обеспечивать прием информации по каналам связи, своевременную и качественную ее обработку (анализ и обобщение), отображение, учет, хранение, обновление и передачу;
- обеспечивать работу вручную в условиях возможного выхода из строя систем автоматизированного управления и связи;
- выполнять другие соответствующие задачи в мирное и военное время.

21. Технически средства управления и связи должны:

- обеспечить автоматизацию управленческой работы во всех органах, пунктах и объектах управления систем военного управления;
- обеспечить максимально возможную степень унификации информационного, математического, программного и технического обеспечения на основе сокращения типажа комплексов и средств автоматизации управления, перечня задач и реализации блочно-модульного принципа их построения;
- использовать быстродействующую систему передачи и приема информации единого типа, обеспечивающую эффективный информационный обмен между элементами СУВ и с сопрягаемыми подсистемами (элементами) других систем в режиме реального времени;
- обеспечивать создание локальных сетей с распределенными вычислительными ресурсами на основе использования ПЭВМ, реализующих многоуровневую, скрытую обработку информации с различными степенями доступа пользователей, прежде всего, должностных лиц аппарата военного управления, при обеспечении высокого уровня защиты всего информационного массива.

22. Одной из важнейших проблем для войск как сложной организационно-технической системы является проблема эффективного управления. Конкретно она обусловлена следующими факторами:

- Большим размахом и динамичностью действий войск, решительностью целей при ведении боевых действий в современных условиях.
- Возможностью быстрого изменения соотношения сил как на отдельных театрах боевых действий, так и в войне в целом.
- Резким возрастанием фактора времени.
- Необходимостью обеспечения обмена различной информацией между взаимодействующими объектами системы управления, которые могут находиться на значительном расстоянии друг от друга, располагаться на земной поверхности, в

воздушном или космическом пространстве при их общем количестве десятки, сотни и более.

- Необходимостью вырабатывать и принимать ответственные решения в условиях неопределенности, неполноты информации, действия различных возмущающих факторов, включая целенаправленные воздействия со стороны противника, ограничений, обусловленных моральными и этическими нормами и др.
- Необходимостью вырабатывать и принимать оптимальные или близкие к оптимальным решения, поскольку цена неоптимальных решений может быть чрезвычайно высокой, а результатом их использования может быть непоправимый ущерб.

23. В первую очередь в органах и объектах управления автоматизируются следующие процессы управления:

- Сбор и обработка данных об обстановке (о своих войсках, о противнике, об условиях ведения боевых действий и т.п.).
- Производство оперативных, информационных и других расчетов, а также математического моделирования операции.
- Наглядное отображение информации.
- Документирование, оформление, размножение боевых документов.
- Доведение задач до подчиненных войск.
- Доведение информации до взаимодействующих штабов и должностных лиц данного органа управления.
- Решение вспомогательных задач (кодирование, декодирование, засекречивание, рассекречивание информации и т.п.)

24. В целом, средства автоматизации органов управления АСУВ должны обеспечивать решение следующих основных задач:

- Ведение и отображение информации по оперативно-тактической обстановке, плану применения сил и средств.
- Выдачу оперативному составу вышестоящих органов управления предложений, рекомендаций для выработки решения на применение сил и средств в соответствии с реальной обстановкой.
- Ведение базы данных по всем объектам инфраструктуры подчиненных войск.
- Сбор, хранение, обмен, обработку и представление информации по типовым ситуациям в боевой и повседневной деятельности войск.
- Проработку вариантов решений на выполнение войсками поставленных задач с учетом реальной обстановки.
- Решение задач управления повседневной деятельностью войск (учет личного состава, контроль исполнения документов, формирование потребностей и учет вооружения, контроль и расчет всех видов довольствия личного состава и др.).
- Обеспечение доступа к базам данным штаба, его отделов, служб для использования имеющейся информации при планировании применения сил и средств, а также при управлении повседневной деятельностью войск в соответствии с порядком подчиненности и должностными полномочиями.
- Разработку и обмен установленными видами документов в порядке подчиненности между органами управления различных уровней иерархии (организация автоматизированного документооборота).
- Организацию автоматизированного информационного обмена с взаимодействующими органами управления других видов и родов войск.

25. В АСУВ, являющейся автоматизированной системой организационного (административного) или интегрированного типа (в состав которой также входит АСУ организованного типа), на человека возложена реализация следующих функций:

- Функции управления (командные функции);
- Операторские функции;
- Функции эксплуатации аппаратных и программных средств.

Командные функции реализуются человеком, включенным непосредственно в контур управления. Специалисты, принимающие участие в реализации командных функций, ответственны за выработку и принятие управленческих решений на всех этапах планирования и оперативного управления. Они также осуществляют контроль над реализацией принятых решений.

Командные функции связаны с решением следующих основных задач:

- постановка и корректировка целей и критериев управления;
- внесение творческого элемента в поиск наилучших путей достижения поставленных целей (человек мыслит содержательно, а не формально);
- окончательный отбор вырабатываемых системой решений и придание им юридической силы;
- снабжение системы первичной информацией, сбор которой невозможно или нерационально автоматизировать полностью.

Операторские функции связаны с организацией взаимодействия специалистов, реализующих командные функции, с объектом (объектами) управления, с получением ими всей необходимой информации для выработки и принятия управленческих решений.

Специфика функционирования АСУВ требует от всех должностных лиц высокой подготовленности (как профессиональной, так и психологической), ответственности при решении возложенных на них задач, внимания, умения качественно, безошибочно работать в напряженных условиях на длительных интервалах времени.

Участие человека в реализации большого числа достаточно важных функций в АСУВ, уровень выполнения которых определяет эффективность АСУВ в целом, требует при ее разработке и совершенствовании в обязательном порядке рассмотрения проблемы «человек-техника». Эта проблема для АСУВ как сложной, недетерминированной информационной человеко-машинной системой связана с решением вопросов рационального распределения функций между человеком и техникой.

26. Угроза безопасности информации – совокупность условий и факторов, создающих опасность нарушения безопасности информации.

Угроза информационной безопасности Автоматизированной Системы (АС) – возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к нарушению конфиденциальности, целостности и доступности этой информации, а также возможность воздействия на компоненты АС, приводящего к из утрате, уничтожению или сбою функционирования.

Классификация возможных угроз ИБ АС может быть проведена по следующим базовым признакам.

- По природе возникновения;
- По степени преднамеренности проявления;
- По непосредственному источнику угроз;
- По положению источника угроз;
- По степени зависимости от активности АС;
- По степени воздействия на АС;
- По этапам доступа пользователей или программ к ресурсам;

- По способу доступа к ресурсам АС;
- По текущему месту расположения информации, хранимой и обрабатываемой в АС.

27. Используемые в настоящее время на практике подходы к защите компьютерной информации определяются следующим характеристиками:
    - формализованными требованиями к набору и параметрам механизмов защиты, регламентирующими современные требования к обеспечению компьютерной безопасности;
    - реальными механизмами защиты;
    - существующей статистикой угроз компьютерной безопасности.

Выделяются следующие основные группы механизмов защиты:

1. механизмы управления доступом;
2. механизмы регистрации и учета;
3. механизмы криптографической защиты;
4. механизмы контроля целостности.

28. Под политикой безопасности организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности является тем средством, с помощью которого реализуется деятельность в компьютерной информационной системе организации.

Основные цели — обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. К частным целям относятся:

- обеспечение уровня безопасности, соответствующего нормативным документам;
- следование экономической целесообразности в выборе защитных средств;
- обеспечение безопасности в каждой функциональной области локальной сети;
- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;
- обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности.

29. Уязвимость информации в автоматизированных комплексах обусловлена большой концентрацией вычислительных ресурсов, их территориальной распределенностью, долговременным хранением большого объема данных на магнитных носителях, одновременным доступом к ресурсам многих пользователей.

    Основные трудности по защите информации:

    - на сегодняшний день нет единой теории защищенных систем;
    - производители средств защиты в основном предлагают отдельные компоненты для решения частных задач, оставляя вопросы формирования системы защиты и совместимости этих средств на усмотрение потребителей;
    - для обеспечения надежной защиты необходимо разрешить целый комплекс технических и организационных проблем и разработать соответствующую документацию.

Концепция — официально принятая система взглядов на проблему информационной безопасности и пути ее решения с учетом современных тенденций. Она является методологической основой политики разработки практических мер по ее реализации.

На базе сформулированных в концепции целей, задач и возможных путей их решения формируются конкретные планы обеспечения информационной безопасности.

Разработку концепции защиты рекомендуется проводить в три этапа.

На первом этапе должна быть четко определена целевая установка защиты, т. е. какие реальные ценности, производственные процессы, программы, массивы данных необходимо защищать.

На втором этапе должен быть проведен анализ преступных действий, которые потенциально могут быть совершены в отношении защищаемого объекта.

Главной задачей третьего этапа является анализ обстановки, в том числе местных специфических условий, производственных процессов, уже установленных технических средств защиты.

30. Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов ИТ.

Потребители заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности.

Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов, в применении процедуры сертификации как механизма объективной оценки их свойств, а также в стандартизации определенного набора требований безопасности.

Эксперты по квалификации и специалисты по сертификации рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый продуктами ИТ, и предоставить потребителям возможность сделать обоснованный выбор.

Таким образом, перед стандартами информационной безопасности стоит непростая задача — примирить три разные точки зрения и создать эффективный механизм взаимодействия всех сторон. Причем ущемление потребностей хотя бы одной из них приведет к невозможности взаимопонимания и взаимодействия и, следовательно, не позволит решить общую задачу — создание защищенной системы обработки информации.

31. на сегодняшний день нет единой теории защищенных систем. Производители средств защиты в основном предлагают отдельные компоненты для решения частных задач, оставляя вопросы формирования системы защиты и совместимости этих средств на усмотрение потребителей. Для обеспечения надежной защиты необходимо разрешить целый комплекс технических и организационных проблем и разработать соответствующую концепцию.

Концепция — официально принятая система взглядов на проблему информационной безопасности и пути ее решения с учетом современных тенденций. Она является методологической основой политики разработки практических мер по ее реализации.

На базе сформулированных в концепции целей, задач и возможных путей их решения формируются конкретные планы обеспечения информационной безопасности.

Разработку концепции защиты рекомендуется проводить в три этапа.

На первом этапе должна быть четко определена целевая установка защиты, т. е. какие реальные ценности, производственные процессы, программы, массивы данных необходимо защищать.

На втором этапе должен быть проведен анализ преступных действий, которые потенциально могут быть совершены в отношении защищаемого объекта.

Главной задачей третьего этапа является анализ обстановки, в том числе местных специфических условий, производственных процессов, уже установленных технических средств защиты.

32. Система защиты информации — это комплекс организационных и технических мер, направленных на обеспечение информационной безопасности предприятия.

Главным объектом защиты являются данные, которые обрабатываются в автоматизированной системе управления (АСУ) и задействованы при выполнении рабочих процессов.

К организационным мерам ЗИ относятся:

- Ограничение доступа в помещения, в которых происходит подготовка и обработка информации;
- доступ к обработке и передаче конфиденциальной информации только проверенных должностных лиц;
- хранение магнитных носителей и регистрационных журналов в закрытых для доступа посторонних лиц сейфах;
- исключение просмотра посторонними лицами содержания обрабатываемых материалов через дисплей, принтер и т.д.;
- использование криптографических кодов при передаче информации по каналам связи ценной информации;
- уничтожение красящих лент, бумаги и иных материалов, содержащих фрагменты ценной информации

Технические средства защиты информации - это системы охраны территорий и помещений с помощью экранирования машинных залов и организация контрольно-пропускных систем.

Защита информации в сетях и вычислительных средствах с помощью технических средств реализуется на основе организации доступа к памяти с помощью:

- контроля доступа к различным уровням памяти компьютера;
- блокировки данных и ввода ключей;
- выделения контрольных битов для записей с целью идентификации и др.

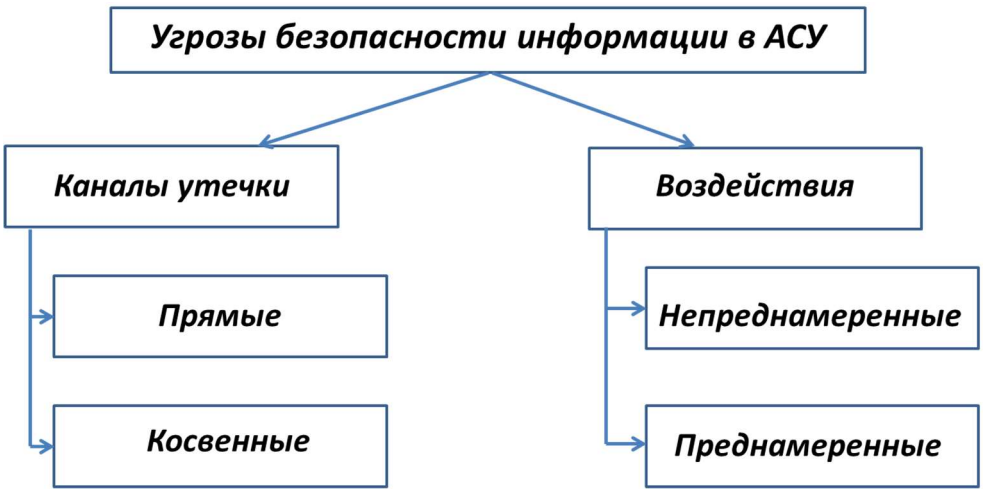
33. Информация с точки зрения информационной безопасности обладает следующими категориями:

- конфиденциальность – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации
- целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения.
- аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией.
- апеллируемость – довольно сложная категория, но часто применяемая в электронной коммерции – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой.

В отношении информационных систем применяются иные категории:

- надежность – гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано;
- точность – гарантия точного и полного выполнения всех команд;
- контроль доступа – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются;
- контролируемость – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса;
- контроль идентификации – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает;
- устойчивость к умышленным сбоям – гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как говорено заранее.

34.



Косвенными называется такие каналы утечки данных, использование которых для НСД не требует непосредственного доступа к данным и техническим устройствам АСУ. Косвенные каналы утечки данных возникают вследствие:

- недостаточной звукоизоляции и помещений;
- недостаточной защищенности технических средств АСУ от электромагнитных излучений;
- просчетов в организации применения законодательных и организационных средств защиты.

Прямые каналы утечки данных требуют непосредственного доступа к данным и техническим средствам АСУ и, в свою очередь, подразделяются на каналы утечки с модификацией данных и без модификации данных. Наличие прямых каналов утечки данных обусловлено недостаточной защищенностью технических и программных средств АСУ, недостатками ОС, СУБД, языков программирования и другого математического обеспечения.

По цели воздействия различают три основных типа угроз безопасности АСУ:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения работоспособности системы (отказы в обслуживании).

35. Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Организационно-техническими методами обеспечения информационной безопасности РФ являются:

- создание и совершенствование системы обеспечения ИБ;
- разработка, использование и совершенствование СЗИ и методов контроля эффективности этих средств;
- развитие защищенных телекоммуникационных систем, повышение надежности СПО;
- создание систем и средств предотвращения НСД к обрабатываемой информации;
- сертификация СЗИ, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и СЗИ.

Экономические методы обеспечения информационной безопасности включают в себя:

- разработку программ обеспечения информационной безопасности и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации.

36. СЭД МО РФ предназначена для:

- организации автоматизированного документооборота, хранения и работы с электронными документами;
- обеспечение единых методологических, организационных и информационно-технологических решений, объединяющих различные виды документов (открытого и ограниченного распространения) и различные группы пользователей;
- автоматизация процессов делопроизводства и регламентов, принятых в ОВУ МО РФ;
- обеспечение контролируемости процесса документооборота (создание, согласование, регистрация, рассмотрение, исполнение и т.д.);
- организации и систематизации единого хранилища электронных документов;
- поиска электронных документов по обязательным реквизитам и содержанию;
- обеспечения юридической значимости документооборота;
- исключения утери документов;
- обеспечения разграничения доступа к документам.

Организация и контроль работ по созданию СЭД в МО РФ реализованы следующим образом:

в ОВУ СЭД устанавливается в подразделениях, осуществляющих документационное обеспечение управления (ДОУ);

в каждом ОВУ (для каждого делопроизводства) организуется свой сервер СЭД и АРМ по количеству исполнителей СЭД;

в каждом ОВУ назначаются ответственные исполнители по СЭД (в соответствии с официальными документами каждого ОВУ).

37. К общим функциональным возможностям СЭД МО РФ относятся:

- регистрация и обработка документов;

- формирование регистрационно-контрольной карточки документа (РККД);
- подготовка сканированного образа документа для ввода в СЭД, обеспечение потокового сканирования комплекта документов;
- распределение входящих ЭД, подготовка проектов резолюций, постановка поручений, контроль исполнения ЭД, формирование отчетов;
- подготовка, согласование (визирование) и подписание (утверждение) ЭД;
- ведение дел в электронном виде, перенос ЭД в архив и уничтожение;
- поиск ЭД по реквизитам и содержанию;
- ведение ИЛО СЭД (словарей, классификаторов) с возможностью автоматической рассылки обновлений ИЛО и элементов самого СЭД;
- организация трех контуров обработки ЭД: контур обмена служебной информацией (официальный обмен служебными документами с их автоматизированной регистрацией); оперативно-распорядительный контур (издание и доведение приказов, директив, распоряжений и т.п. с контролем их исполнения); личный контур обмена информацией между должностными лицами ОВУ.

38. СЭД МО РФ представляет собой модульную систему, состоящую из компактного надежного ядра (интеграционной платформы «ИВК Юпитер») и задач (специального программного обеспечения СЭД «ИВК Бюрократъ»), функционирующих под его управлением. Модули разделены на функциональные подсистемы по типу реализуемых ими задач:

- Подсистема передачи данных в сетях.
- Подсистема интеграции.
- Подсистема хранения.
- Подсистема безопасности.
- Подсистема представления данных.
- Подсистема удаленного мониторинга и контроля функционирования клиентов АС.

Обмен документами осуществляется с помощью ПО «Система электронной почты». Сервер СЭП является составной частью комплекса программного обеспечения «Система электронной почты». СЭП – это аналог обычной почты, использующей для передачи сообщений электронные средства связи – локальные компьютерные сети, телефонные линии и т.п.

39. Защищенный комплекс программ гипертекстовой обработки данных – это ПО, осуществляющее взаимодействие по HTTP-протоколу между сервером и браузерами: прием запросов, поиск указанных файлов и передача их содержимого, выполнение приложений на сервере и передача клиенту результатов их выполнения.

Комплекс представлен web-сервером Apache2 и браузером Firefox. Web-сервер Apache2, входящий в состав ОС, не допускает возможности анонимного использования ресурсов web-сервера и требует обязательной настройки авторизации пользователей. Для работы используется «протокол передачи гипертекста» HTTP.

HTTP (HyperText Transfer Protocol — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных изначально — в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных. Основой HTTP является технология «клиент-сервер», то есть предполагается существование:

Потребителей (клиентов), которые инициируют соединение и посылают запрос;

Поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

40. Программа предназначена для организации доступа клиентов к гипертекстовым данным, расположенным на сервере, а также для разграничения прав доступа между клиентами на уровне ОС.

Программа обеспечивает выполнение следующих функций:

Обработку скриптовых файлов посредствам CGI-интерфейса (perl, shell и другие);

Выполнение PHP программ, как с использованием встроенного статического интерпретатора, так и через CGI-интерфейс;

Обеспечение разграничения доступа на уровне ОС, посредством обработки поступающих запросов с определенными для каждого клиента параметрами;

Затруднение анализа передаваемых сетевых пакетов путем их видоизменения.

Клиент ГОД включает в себя несколько взаимосвязанных частей:

Просмотр веб-страниц с использованием Навигатора;

Получение и отправка электронной почты, чтение групп новостей, установка параметров электронной почты и групп новостей с использованием Почтового клиента ГОД;

Использование функций Клиента ГОД, обеспечивающих приватность и безопасность при работе в сети – приватность и защита информации;

создание веб-страниц при помощи Компоновщика.

41. Соблюдение принципов работы с электронной почтой является обязательным условием нормального администрирования почтовых систем в средних и крупных организациях. Естественно, ими можно руководствоваться и в небольших организациях.

В небольшой организации серверы, реализующие указанные функции, могут работать на одном компьютере. В крупных сетях это должны быть отдельные компьютеры.

Существует два типа почтовых серверов: серверы, взаимодействующие с Интернетом для обработки входящих и исходящих сообщений, и внутренние серверы, взаимодействующие с пользователями.

Почтовая система состоит из двух частей: DMZ (демилитаризованной зоны), компьютеры которой подключены непосредственно к Интернету, и внутренней зоны, отделенной от зоны DMZ и Интернета с помощью брандмауэра.

Сервер исходящей почты, который непосредственно подключен к Интернету, наиболее уязвим. Он должен быть хорошо защищен, иметь мало пользователей и не выполнять посторонних процессов или услуг. Каждое сообщение, которое он обрабатывает, должно быть проверено.

Исходящая почта должна сканироваться на вирусы и спам, чтобы убедиться, что локальные компьютеры не инфицированы, и ограничить распространение вредоносных программ среди других организаций.

42. SMTP (Simple Mail Transfer Protocol — простой протокол передачи почты) — это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

В настоящее время под «протоколом SMTP» как правило подразумевают и его расширения. Протокол SMTP предназначен для передачи исходящей почты с использованием порта TCP 25.

Для доступа к хранилищам и загрузки сообщений электронной почты на локальное устройство используется два протокола: IMAP4 и POP. Ранние версии этих протоколов имели проблемы с безопасностью.

POP3 (Post Office Protocol Version 3 — протокол почтового отделения, версия 3) — стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению.

Альтернативным протоколом для сбора сообщений с почтового сервера является IMAP.

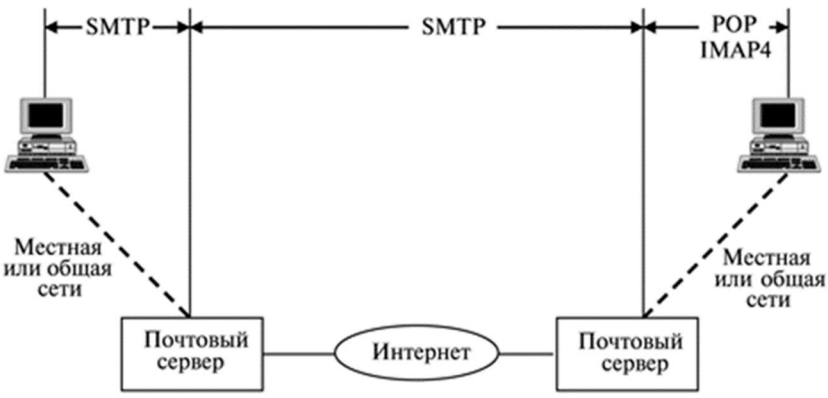
IMAP (Internet Message Access Protocol — протокол доступа к электронной почте Интернета). Он лучше, чем протокол POP, поскольку доставляет ваши почтовые сообщения по одному, а не все сразу, что более удобно для работы в сети.

IMAP предоставляет пользователю широкие возможности для работы с почтовыми ящиками, находящимися на почтовом сервере. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя.

43. Документ RFC4954 определяет расширение исходного протокола SMTP, позволяющее SMTP-клиенту идентифицировать себя и проходить аутентификацию у почтового сервера. После этого сервер может позволить клиенту использовать себя для пересылки почты. Этот протокол поддерживает несколько механизмов аутентификации. Обмен информацией состоит из следующих этапов:

- Клиент посылает команду EHLO, сообщая, что он использует протокол ESMT.
- Сервер отвечает и уведомляет о своих механизмах аутентификации.
- Клиент посылает команду AUTH и называет конкретный механизм аутентификации, который он хочет использовать, включая свои данные для аутентификации.
- Сервер принимает данные, присланные с командой AUTH, или начинает последовательность команд “вызов/ответ” для обмена информацией с клиентом.
- Сервер либо принимает, либо отвергает попытку аутентификации.
- Для того чтобы узнать, какой механизм аутентификации поддерживает сервер, можно применить утилиту telnet к порту 25 и выполнить команду EHLO.

44. Доставка почты от отправителя к получателю проходит через три стадии.



Первая стадия:

На первой стадии электронная почта проходит через пользовательского агента в локальный сервер. Почта, возможно, сразу не посылается на удаленный сервер, поскольку он может быть недоступен к этому моменту. Поэтому почта накапливается в локальном сервере, пока ее не удастся отправить. Пользовательский агент использует программное обеспечение SMTP-клиента, локальный сервер использует программное обеспечение SMTP-сервера.

Вторая стадия:

На втором шаге электронная почта идет с помощью локального сервера, который теперь действует как клиент SMTP. Электронная почта доставляется удаленному серверу, но не к удаленному агенту пользователя. Если бы SMTP был принятым сервером, всегда можно было бы обработать прибывшую почту в любой момент времени. Однако люди часто выключают свой компьютер до конца дня, а мини-компьютер или переносные компьютеры зачастую нормально не работают. Обычно организации предназначают свой компьютер для принятия электронной почты и постоянной работы в качестве программного сервера. Электронная почта получается с помощью такого сервера и накапливается в почтовом ящике для дальнейшего использования.

Третья стадия:

На третьей ступени удаленный агент пользователя применяет протокол POP3 или IMAP4 (оба протокола обсуждаются в следующих секциях), чтобы запустить почтовый ящик и получить почту.

45. В качестве защищенного комплекса программ электронной почты используется сервер электронной почты, состоящий из агента передачи электронной почты Exim4, агента доставки электронной почты Dovecot и клиента электронной почты Thunderbird, доработанных для реализации следующих дополнительных функциональных возможностей:

- интеграции с ядром ОС и базовыми библиотеками для обеспечения разграничения доступа;
- реализации мандатного разграничения доступа к почтовым сообщениям;
- автоматической маркировки создаваемых почтовых сообщений, отражающих уровень их конфиденциальности;
- регистрации попыток доступа к почтовым сообщениям.
- Агент передачи электронной почты использует протокол SMTP и обеспечивает решение следующих задач:
- доставку исходящей почты от авторизованных клиентов до сервера, который является целевым для обработки почтового домена получателя;
- прием и обработку почтовых сообщений доменов, для которых он является целевым;
- передачу входящих почтовых сообщений для обработки агентом доставки электронной почты.
- Агент доставки электронной почты предназначен для решения задач по обслуживанию почтового каталога и предоставления удаленного доступа к почтовому ящику по протоколу IMAP.
- Клиент электронной почты — прикладное ПО, устанавливаемое на рабочем месте пользователя и предназначенное для получения, написания, отправки и хранения сообщений электронной почты пользователя.

46. Программное средство «Сервер СИУ» предназначено для обеспечения возможности совместного использования информационных объектов (ИО) должностными лицами, АС

и АСУ различного назначения на базе предоставления им унифицированных услуг размещения, совместной обработки, поиска и извлечения ИО.

Сетеориентированные информационные услуги (СИУ) – согласованный набор услуг, обеспечивающий:

- семантическое описание данных, используемых в ССПД, ведение реестра метаданных;
- сегментирование пространства данных на основании описания предметных областей;
- услуги размещения (публикации), поиска и доступа к данным вне зависимости от их источников (на основании формируемых каталогов информационных объектов и репозитория данных);
- совместную работу с информацией, размещенной в ССПД, участников сетевых объединений пользователей;
- организацию информационного взаимодействия АС и АСУ различного назначения в режиме «Многие ко многим», совместную работу АС и АСУ с информацией.

Служба СИУ обеспечивает:

- формирование ССПД, которое является совокупностью опубликованных данных и метаданных всех сетевых объединений пользователей;
- возможности по ведению и обеспечению оперативного доступа к информации «в любом месте в любое время» в соответствии с правами доступа;
- средства доступа и отображения информации, в том числе в реальном масштабе времени;
- средства информационного подключения АС в качестве источников информации об объектах предметной области.

47. Основными задачами программного средства являются:

- ведение внутренних информационных рабочих пространств (распределенной системы взаимосвязанных рабочих пространств) организации – сетевых объединений пользователей;
- размещение информации для публичного доступа: события, распоряжения, приказы;
- классификация информации на основе ведущегося описания предметной области, базирующегося на системе классификаторов, описание информации с использованием метаданных;
- поиск и размещение в СОП информации из открытых сетей, подключенных хранилищ информации и информационных систем с привязкой к терминологии предметной области;
- отображение, редактирование и поиск объектов, обладающих пространственными характеристиками, на электронной карте;
- информационное взаимодействие сотрудников при работе над совместной задачей или участии в общем процессе управления;
- информационный обмен со сторонними информационными системами на основе мета-описаний информации.

48. Программное средство «Геоинформационный сервер» предназначено для реализации функций управления информационными объектами, имеющими географические характеристики.

ПС «Геоинформационный сервер» обеспечивает:

- управление информационными объектами с координатными метаданными;

- поиск информационных объектов путем задания на электронной топографической карте (ЭТК) (с возможностью ее масштабирования) интересующей области поиска, типов информационных объектов и значений метаданных;
- отображение найденных информационных объектов с координатными метаданными на фоне ЭТК и в отдельном окне с возможностью их группировки и сортировки по типам;
- задание пользователем координатных метаданных путем непосредственного ввода с клавиатуры или путем указания пользователем координат на ЭТК;
- связывание значений древовидных классификаторов с электронными условными знаками (точечными, линейными, площадными) для отображения на фоне ЭТК;
- возможность отображения на фоне ЭТК информационных объектов, связанных с заданным объектом (информационным объектом);
- управление (создание, удаление, изменение, просмотр) информационными объектами с координатными метаданными: линия и полигон.

ПС «Геоинформационный сервер» обеспечивает следующие функции по безопасности:

- аутентификация и идентификация, проводимая как между сервером и клиентом, так и между соседними серверами;
- управление доступом пользователей на основе дискреционного и мандатного принципов доступа.

49. В общем сетевом контексте любое устройство, которое отвечает на запросы от клиентских приложений, функционирует как сервер. Сервером обычно является компьютер, который хранит информацию, являющуюся общей для нескольких клиентских систем. Например, веб страницы, документы, базы данных, картинки, видео и аудио файлы - все это может храниться на сервере и передаваться клиентам, запрашивающим необходимые ресурсы. В других случаях, (использование сетевого принтера), сервер печати обрабатывает клиентские запросы на печать, передавая их на указанный принтер. Различные типы серверных приложений могут иметь разные требования для клиентского доступа. Некоторые серверы могут требовать аутентификации (предоставления информации об учетной записи пользователя), чтобы проверить, имеет ли пользователь разрешение обращаться к запрашиваемым данным или использовать какую-либо конкретную операцию. Такие серверы полагаются на центральный список учетных записей пользователей и авторизаций, или разрешений (как для доступа к данным, так и для операций), предоставленных каждому пользователю. При использовании FTP клиента, к примеру, если вы делаете запрос загрузки данных на FTP сервер, у вас есть разрешение на запись в определенную директорию, но нет права на запись/чтение для других директорий, к которым нет доступа.
50. Физическая адресация Канального уровня OSI (Уровня 2), реализованная в виде MAC-адреса Ethernet, используется для передачи кадра через локальный носитель. Хотя и будучи уникальными адресами узла, физические адреса не являются иерархическими. Они связаны с определенным устройством независимо от его расположения или сети, с которой это устройство соединяется. Эти адреса Уровня 2 не имеют никакого значения вне локальной сетевой среды. Пакету, вероятно, придется пересечь множество различных технологий Канального уровня в локальных и глобальных сетях прежде, чем он достигнет своего места назначения. Поэтому у отправляющего устройства нет сведений относительно технологии, используемой в промежуточной и целевой сетях или их адресации Уровня 2 и структурах кадра.

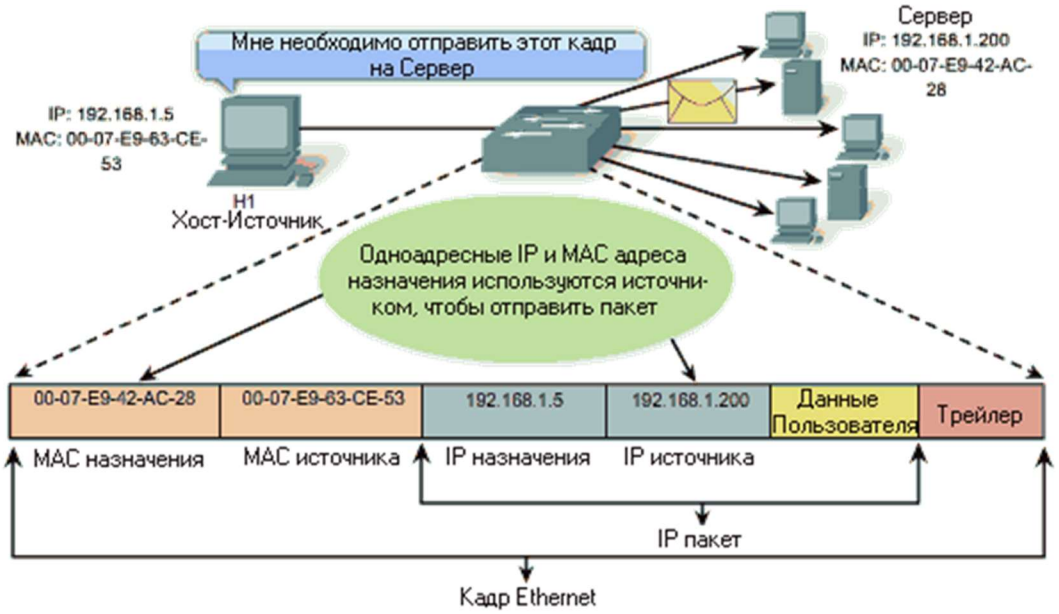
Адреса сетевого уровня (Уровня 3), такие как адреса IPv4, обеспечивают повсеместную, логическую адресацию, которая понимается и источником и местом назначения. Чтобы прибыть к своему возможному месту назначения, пакет переносит адрес назначения Уровня 3 из своего места отправления. Однако, по мере того, как он кадрируется различными протоколами Канального уровня по пути, адрес Уровня 2, который он получает каждый раз, применяется только к соответствующей локальной части маршрута и ее носителя.

И так:

• Адрес Сетевого уровня позволяет передать пакет к его месту назначения.

• Адрес Канального уровня позволяет локальному носителю переносить пакет через каждый сегмент.

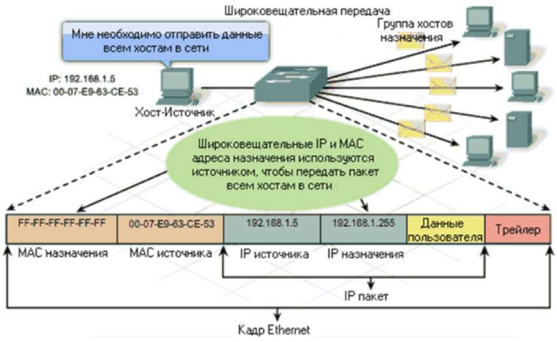
51.



Одноадресный MAC-адрес является уникальным адресом, используемым, когда кадр передается с одного передающего устройства на единственное устройство назначения.

В примере, показанном на рисунке, узел с IP-адресом 192.168.1.5 (источник) запрашивает веб-страницу с сервера по IP-адресу 192.168.1.200. Для одноадресного пакета, который будет отправлен и получен, IP-адрес назначения должен быть в заголовке пакета IP. Соответствующий MAC-адрес назначения также должен присутствовать в заголовке Кадра Ethernet. IP-адрес и MAC-адрес комбинируются, чтобы доставить данные одному определенному конечному хосту.

52.



При широковещательной передаче пакет содержит IP-адрес назначения, у которого в хостовой части адреса стоят одни единички. Эта нумерация в адресе означает, что все узлы в этой локальной сети (широковещательном домене) получат и обработают пакет. Ряд сетевых протоколов, таких как Протокол динамического конфигурирования узлов (DHCP) и Протокол определения адресов (ARP), используют широковещательные сообщения. Как показано на рисунке, широковещательный IP-адрес сети нуждается в соответствующем широковещательном MAC-адресе Кадра Ethernet. В Сетях Ethernet широковещательным MAC-адресом является адрес из 48 единиц, или "FF FF FF FF FF FF" - в шестнадцатеричном виде.

53.

Групповые адреса позволяют исходному устройству отправлять пакет группе устройств. Устройствам, которые принадлежат группе многоадресной передачи, присваиваются IP-адрес группы многоадресной передачи. Диапазон групповых адресов от 224.0.0.0 до 239.255.255.255. Поскольку групповые адреса представляют группу адресов (иногда называемую группой узлов), они могут использоваться только в качестве места назначения пакета. У источника всегда будет индивидуальный адрес. Многоадресный IP-адрес требует соответствующего многоадресного MAC-адреса для фактической доставки фрейма по локальной сети. Многоадресный MAC-адрес является специальным значением, которое начинается с 01-00-5E в шестнадцатеричной записи. Значение заканчивается путем преобразования младших 23 битов группового адреса многоадресного IP-пакета в оставшиеся 6 шестнадцатеричных символов Ethernet-адреса. Остающийся бит в MAC-адресе всегда "0".