Л. Н. ТРОФИМОВА, Е. С. КАЛИНИНА, А. В. ДОЛГОВА

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ И ЗАЩИТЕ ИНФОРМАЦИИ

ОМСК 2016

Министерство транспорта Российской Федерации
Федеральное агентство железнодорожного транспорта
Омский государственный университет путей сообщения

Л. Н. Трофимова, Е. С. Калинина, А. В. Долгова

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ И ЗАЩИТЕ ИНФОРМАЦИИ

Утверждено методическим советом университета
в качестве учебно-методического пособия для самостоятельной работы
студентов по дисциплине «Информатика»

Омск 2016

УДК 004.7(075.8)
ББК 32.973.202.5я73
Т76

Основные понятия и определения в компьютерных сетях и защите информации: Учебно-методическое пособие / Л. Н. Трофимова, Е. С. Калинина, А. В. Долгова; Омский гос. ун-т путей сообщения. Омск, 2016. 44 с.

Учебно-методическое пособие содержит базовые понятия защиты информации и основы построения компьютерных сетей. Рассмотрены методы и средства защиты информации, основные типы сетевого оборудования, основные принципы построения глобальной сети Интернет. Представлены примеры тестовых вопросов, темы рефератов для выполнения индивидуального задания.

Предназначено для студентов всех специальностей очной и заочной форм обучения, изучающих дисциплины «Информатика», «Информационные технологии», «Компьютерные технологии и информатика», «Программные средства офисного назначения», «Современные информационные технологии», а также для студентов третьего курса специальностей «Информационная безопасность телекоммуникационных систем» и «Информационная безопасность автоматизированных систем», изучающих дисциплины «Основы информационной безопасности», «Компьютерные сети и системы».

Библиогр.: 6 назв. Табл. 1. Рис. 17.

Рецензенты: доктор техн. наук, профессор А. В. Бубнов;
доктор техн. наук, профессор В. Е. Митрохин.

ОГЛАВЛЕНИЕ

Введение 5
1. Основы защиты информации 6
1.1. История развития средств и методов защиты информации 6
1.2. Основные понятия информационной безопасности 9
1.3. Классификация угроз информационной безопасности 10
1.4. Методы и средства защиты информации 13
1.4.1. Законодательные средства защиты информации 13
1.4.2. Организационные средства защиты информации 14
1.4.3. Технические и программные средства защиты информации .. 15
1.4.3.1. Компьютерные вирусы 17
1.5. Контрольные вопросы 19
2. Компьютерные сети 19
2.1. Понятие компьютерной сети 19
2.2. Классификация КС 20
2.3. Сетевое оборудование 24
2.3.1. Среда передачи данных 24
2.3.2. Сетевой адаптер 27
2.3.3. Маршрутизатор 28
2.3.4. Мост 28
2.3.5. Повторитель 29
2.3.6. Концентратор 29
2.3.7. Коммутатор 29
2.3.8. Сетевой шлюз 29
2.3.9. Межсетевой экран 30
2.4. Контрольные вопросы 30
3. Интернет. Информационные сервисы 30
3.1. Глобальные сети 30
3.2. История развития сети Интернет 31
3.3. Сетевые протоколы 32
3.4. Адресация в Интернете 34
3.5. Службы Интернета 36
3.6. Web-поиск 38
3.7. Электронная почта 40

3.8. Контрольные вопросы 41
4. Темы рефератов 41
5. Примеры тестовых вопросов 42
Библиографический список 43

ВВЕДЕНИЕ

Современный мир – это мир информационных технологий. Компьютерная индустрия – один из наиболее быстроразвивающихся секторов экономики. В настоящее время в каждой крупной компании имеется компьютерная сеть. Защита данных в компьютерных сетях становится одной из самых актуальных проблем в современной информатике. Поэтому необходимым является изучение основ построения компьютерных сетей и базовых понятий защиты информации.

В настоящем учебно-методическом пособии приведена классификация угроз информационной безопасности компьютерных автоматизированных систем. Изложена общая концепция методов и средств защиты информации. Приведены основные классификации компьютерных сетей и их топологии. Рассмотрены базовые компоненты вычислительных сетей. Представлены основные сведения о глобальной компьютерной сети Интернет.

Данное учебно-методическое пособие предназначено для студентов ОмГУПСа всех направлений подготовки и специальностей очной и заочной форм обучения, изучающих дисциплины «Информатика», «Информационные технологии», «Компьютерные технологии и информатика», «Программные средства офисного назначения», «Современные информационные технологии», а также для студентов третьего курса специальностей «Информационная безопасность телекоммуникационных систем» и «Информационная безопасность автоматизированных систем», изучающих дисциплины «Основы информационной безопасности», «Компьютерные сети и системы». Материал учебного издания может служить самоучителем и закладывает хорошую базу для дальнейшего, более глубокого изучения частных, узкоспециальных проблем, связанных с разработкой и обслуживанием компьютерных сетей.

Библиографический список, представленный в конце учебно-методического пособия, содержит литературу для углубленного изучения данной темы.

1. ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1. История развития средств и методов защиты информации

В процессе эволюции цивилизации изменялись виды и носители информации, а также различные средства и методы ее защиты. Вопросы создания и передачи информации имеют многовековую историю. Например, наскальные рисунки и древние рукописи – попытка сохранить информацию о реалиях окружающего мира. Некоторая информация не предназначается для широкой огласки, поэтому для сохранения ее в тайне применяются специальные меры.

История средств защиты информации насчитывает три временных периода (рис. 1).

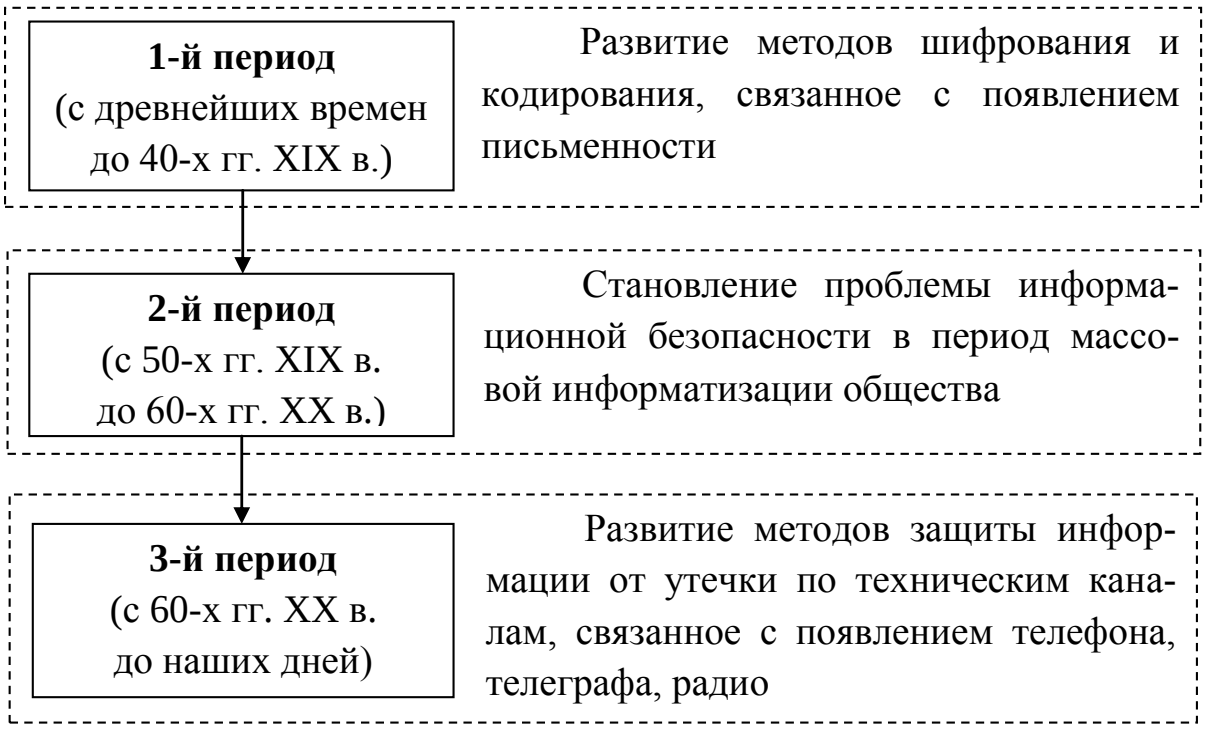

Рис. 1. Развитие методов и средств защиты информации

Первый период определяется началом создания осмысленных и самостоятельных средств и методов защиты информации. Он обусловлен изобретением письменности и связан с появлением возможности фиксации информационных сообщений на твердых носителях. Практически одновременно возникла проб-

лема сохранения в тайне конфиденциальной информации и возникли такие методы защиты информации, как ее шифрование и сокрытие.

Сведения о системах и способах шифрования упоминаются в исторических документах таких древних цивилизаций, как Индия, Египет, Месопотамия. Один из самых древних шифрованных текстов (Месопотамия,2000 лет до н. э.) представляет собой глиняную табличку, содержащую рецепт изготовления глазури в гончарном производстве. В этом тексте игнорировались некоторые гласные и согласные и употреблялись числа вместо имен.

Приблизительно в это же время зарождается наука о составлении шифров и методах шифрования информации – криптография.

Одним из известных древнейших криптографических устройств является скитала, которая применялась в V в. до н. э. во время войны Спарты против Афин. Скитала представляет собой цилиндр определенного диаметра (рис. 2), на который виток к витку наматывается узкая папирусная лента. Затем на этой ленте вдоль оси цилиндра записывается необходимый для передачи текст, лента снимается с цилиндра и направляется получателю.

Рис. 2. Устройство шифрования текста скитала

Для прочтения зашифрованного сообщения получатель должен использовать скиталу такого же диаметра, как и у отправителя, в противном случае полученная лента с сообщением не может быть прочитана.

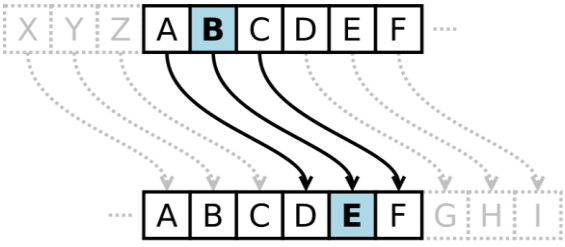

Рис. 3. Шифр Цезаря со сдвигом букв на три позиции

Одним из наиболее простых и широко известных методов шифрования считается шифр Цезаря (рис. 3). Достоверно известно, что переписка выдающегося политического деятеля и полководца Древнего Рима Гая Юлия Цезаря зашифровывалась. Шифр Цезаря (шифр подстановок) основывается на замене каждой буквы исходного алфавита другой буквой этого же алфавита, отстоящей от исходной на определенное число позиций от перво-

начального положения. Величина сдвига является ключом шифрования. Цезарь использовал сдвиг букв на три позиции.

Такие подстановочные шифры раскрываются чрезвычайно просто: для этого достаточно знать лишь алгоритм шифрования, а ключ шифрования подбирается простым перебором букв. Такой способ подбора ключа называется ***силовой атакой***.

Второй период характеризуется появлением технических средств обработки информации и передачи сообщений с использованием электрических сигналов и электромагнитных полей (например, телефон, телеграф, радио). Недостатками таких способов передачи информации являются проблемы защиты информации, связанные с возникновением технических каналов утечки (побочных излучений, наводок и др.). Для обеспечения защиты информации при передаче ее по телефонным и телеграфным каналам связи разработаны способы и технические средства их реализации, позволяющие шифровать сообщения в реальном времени. Одновременно с развитием криптографических способов активно развивались технические средства, направленные на перехват и расшифровку «чужих» сообщений. Этот период характеризуется фактами промышленного и государственного шпионажа специальными отделами разведки.

Одним из самых известных устройств шифрования информации этого периода можно назвать электрическую роторную шифровальную машину «Энигма» (рис. 4), которая использовалась армией Германии во время Второй мировой войны для шифрования и дешифрования секретных сообщений.

Рис. 4. Трехроторная шифровальная машина «Энигма»

Третий период – период массовой информатизации общества – характеризуется дальнейшим интенсивным развитием криптографических методов защиты информации, что обусловлено внедрением автоматизированных систем обработки и передачи информации.

В настоящее время криптография востребована во всех сферах общественной, политической и военной областей, т. е. там, где используются элек-

тронные средства коммуникаций. Современные криптографические алгоритмы основываются на сложных, постоянно совершенствующихся математических конструкциях. Развитие методов и инструментов защиты информации предполагает также использование организационных и законодательных мер.

В настоящее время основными направлениями защиты информации являются охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности граждан.

1.2. Основные понятия информационной безопасности

В настоящее время информация становится все более уязвимой. Этому способствует использование сети Интернет, возрастающие объемы обрабатываемых данных, расширение круга пользователей персональных компьютеров (ПК), недостаточный уровень защиты аппаратных и программных средств и коммуникационных сетей и др.

Основные понятия ***компьютерной (информационной) безопасности (КБ)***:

конфиденциальность информации – свойство информации быть доступной только ограниченному кругу пользователей;

целостность информации – свойство сохранять свою структуру и содержание в процессе хранения, использования и передачи;

достоверность информации – строгая принадлежность информации ее источнику;

доступность информации – возможности системы обеспечивать своевременный беспрепятственный доступ к информации.

идентификация – получение от субъекта сведений (имя, учетный номер и т. п.), позволяющих выделить его из множества субъектов;

аутентификация – получение от субъекта сведений (пароль, биометрические параметры, электронные жетоны, механические ключи и т. п.), подтверждающих его подлинность (т. е. что идентифицируемый субъект является тем, за кого себя выдает);

правила разграничения доступа – регламентация прав доступа субъекта к определенному компоненту системы;

санкционированный доступ к информации – доступ с выполнением правил разграничения доступа;

***угроза информационной безопасности* (ИБ) *компьютерной автоматизированной системы* (КАС)** – возможность воздействия на информацию компьютерной системы с целью ее искажения, уничтожения, копирования или блокирования, а также возможность воздействия на компоненты компьютерной системы, приводящая к сбою их функционирования;

комплекс средств защиты – совокупность аппаратных и программных средств, обеспечивающих ИБ;

политика безопасности – совокупность норм и правил, регламентирующих работу средств защиты от угроз;

дискреционная модель разграничения доступа – способ разграничения доступа субъектов к объектам в соответствии с перечнем их прав доступа. Эта модель реализуется в виде матрицы (строки – субъекты, столбцы – объекты, элементы матрицы – набор прав доступа);

полномочная (мандатная) модель разграничения доступа – способ разграничения доступа, при котором для каждого объекта устанавливается уровень секретности, а для каждого субъекта – уровень допуска. Субъект может получить доступ к объекту, если его уровень допуска (т. е. доверия к нему) не меньше уровня секретности объекта.

Операционной системой Windows поддерживаются обе модели разграничения доступа.

1.3. Классификация угроз информационной безопасности

Наиболее характерными и часто реализуемыми угрозами ИБ КАС являются несанкционированное копирование информации; действия, приводящие к разглашению конфиденциальной информации и игнорирование организационных ограничений (установленных правил) в КАС.

Возможные угрозы ИБ КАС классифицируются по ряду базовых признаков.

1. *По природе возникновения*:

естественные угрозы – угрозы, вызванные воздействиями на КАС и ее компоненты объективных физических процессов или стихийных природных явлений, не зависящих от человека;

искусственные угрозы – угрозы ИБ КАС, вызванные деятельностью человека.

2. *По степени преднамеренности проявления угрозы*:

случайные (ошибки пользователей или халатность персонала, нарушение работы аппаратно-программных средств КАС);

преднамеренные (диверсии в работе оборудования, вскрытие шифров, хищение носителей информации).

3. *По степени воздействия на КАС*:

пассивная (несанкционированные сбор или копирование секретных данных);

активная (установка программ с последующим необоснованным расходованием ресурсов, разглашение атрибутов разграничения доступа (паролей, ключей шифрования), заражение компьютера вирусами или шпионскими программами, умышленная модификация информации).

4. *По расположению источника угроз*:

внешние (перехват данных, дистанционная фото- и видеосъемка, хищение носителей информации);

внутренние (программы, представляющие опасность для работоспособности КАС).

5. *По степени зависимости от активности КАС*:

не зависящие от активности КАС (вскрытие шифров криптозащиты информации, хищение любых носителей информации КАС);

возникающие только в процессе автоматизированной обработки данных (выполнение и распространение программных вирусов).

6. *По способу доступа к ресурсам КАС*:

использование прямого стандартного пути доступа к ресурсам КАС (незаконное получение атрибутов разграничения доступа; несанкционированное использование терминалов, имеющих уникальные физические характеристики);

использование скрытого нестандартного пути доступа к ресурсам КАС (вход в систему в обход средств защиты, загрузка посторонней операционной системы со сменных магнитных носителей);

использования недокументированных возможностей операционных систем.

7. *По текущему месту расположения информации*:

на внешних запоминающих устройствах (несанкционированное копирование конфиденциальной информации с любых внешних носителей);

в оперативной памяти (чтение остаточной информации из оперативной памяти, информации из областей оперативной памяти);

угрозы доступа к информации в результате использования недостатков мультизадачных КАС и систем программирования;

угрозы доступа к системной области оперативной памяти при обращении к ним прикладных программ;

угрозы доступа к информации, циркулирующей в линиях связи при несанкционированном подключении к линиям связи с целью передачи ложной или модификации существующей информации, прямой подмены зарегистрированных пользователей или перехвата потока данных;

угрозы доступа к информации, отображаемой на терминале или на принтере (запись отображаемой информации на скрытую видеокамеру).

В соответствии с существующими подходами принято считать, что информационная безопасность КАС обеспечивается в случае, если для любых информационных ресурсов в системе поддерживается определенный уровень конфиденциальности, целостности и доступности. В соответствии с этими признаками для КАС рассматривают следующие виды угроз по непосредственному воздействию на информацию.

1. *Угроза нарушения конфиденциальности*. Заключается в том, что информация становится известной субъектам, не имеющим полномочий доступа к ней. Для такого вида угрозы используется термин «*утечка*».

2. *Угроза нарушения целостности*. Включает в себя любое умышленное или неумышленное изменение информации, хранящейся в КАС. Такое изменение может возникнуть и из-за случайных ошибок программного или аппаратного обеспечения.

3. *Угроза отказа служб*. Возникает в результате преднамеренных действий пользователя или злоумышленника, блокирует доступ к ресурсам вычислительной системы. Блокирование может быть постоянным (запрашиваемый ресурс никогда не будет получен) или временным (задержка запрашиваемого ресурса).

На современном этапе развития информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация в КАС не представляется пользователю «в чистом виде», на пути к ней обязательно организуется система защиты.

1.4. Методы и средства защиты информации

Для обеспечения защиты информации используется комплекс мероприятий, включающий в себя законодательные средства, организационные мероприятия, технические и программные средства.

1.4.1. Законодательные средства защиты информации

В Российской Федерации к законодательным (нормативно-правовым) актам в области информационной безопасности относятся

– международные договоры РФ;

– Конституция РФ;

– законы федерального уровня (включая федеральные конституционные законы, кодексы);

– указы Президента РФ;

– постановления Правительства РФ;

– нормативные правовые акты федеральных министерств и ведомств;

– нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Законодательные средства защиты определяются законодательными актами государства. Эти акты регламентируют правила пользования, обработки и передачи информации ограниченного доступа и устанавливают меры ответственности за нарушение этих правил.

Наиболее общим законом Российской Федерации является Конституция РФ. Главы 41 и 42, статьи 23 и 29 Конституции РФ затрагивают вопросы информационной безопасности.

Главы 41 и *42* гарантируют право на знание фактов, создающих угрозу жизни и здоровью людей, право на знание достоверной информации о состоянии окружающей среды.

Статья 23 Конституции РФ гарантирует право на личную и семейную тайну, на тайну переписки, телефонных разговоров, почтовых и иных сообщений.

Статья 29 Конституции РФ гарантирует право свободно искать, получать, передавать и распространять информацию любым законным способом.

Уголовным кодексом (УК) Российской Федерации предусматриваются наказания за преступления, связанные с нарушением конфиденциальности информации.

Глава 28 УК (статьи 272 – 274) посвящена преступлениям, связанным с неправомерным доступом к компьютерной информации, созданием и распространением вредоносных программ.

Федеральным законом 152-ФЗ «О защите персональных данных» обеспечивается защита прав и свобод граждан РФ при обработке их персональных данных.

Интересы государства в плане обеспечения конфиденциальности информации представлены в Законе РФ «О государственной тайне».

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

Для защиты сведений, составляющих государственную тайну, Закон определяет средства защиты: технические (аппаратные), криптографические, программные и др. Система органов обеспечения информационной безопасности РФ включает в себя министерства обороны и юстиции.

1.4.2. Организационные средства защиты информации

Гарантом информационной безопасности является Президент Российской Федерации, при котором существует организация Федеральная служба по техническому и экспертному контролю (ФСТЭК России). ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики в области безопасности по следующим вопросам.

1. Обеспечение безопасности информации в системах информационной и телекоммуникационной инфраструктуры.

2. Противодействие иностранным техническим разведкам на территории РФ.

3. Обеспечение защиты информации, содержащей сведения, составляющие государственную тайну.

4. Защита информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

5. Осуществление экспертного контроля.

Обеспечение безопасности информации в вычислительной сети осуществляется комплексом организационных, организационно-технических, технических и программных мер.

К организационным мерам защиты информации относятся

– организация охраны и надежного пропускного режима;

– организация контроля за работой пользователей;

– мероприятия, осуществляемые при подборе и подготовке персонала;

– мероприятия по применению правил доступа к информации;

– организация учета, хранения, использования, уничтожения документов и носителей информации;

– мероприятия по разработке и модификации технических средств.

Организационно-технические меры защиты информации включают в себя

– осуществление бесперебойного питания оборудования;

– установку на дверях помещений кодовых замков;

– использование для отображения информации дисплеев и принтеров с низким уровнем электромагнитного излучения;

– уничтожение информации, хранящейся в компьютере, при списании или отправке его в ремонт;

– установку клавиатуры и принтеров на специальные прокладки с целью снижения возможности снятия информации акустическим способом;

– ограничение электромагнитного излучения от компьютеров путем экранирования помещений, где происходит обработка информации, специальными материалами.

1.4.3. Технические и программные средства защиты информации

Технические (аппаратные) методы защиты информации реализуются приборами, встраиваемыми непосредственно в ПК или в устройства, сопрягаемые с ними по стандартному интерфейсу.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации.

Программно-технические средства и методы защиты информации подразумевают наличие систем мониторинга сетей, антивирусных средств, межсетевых экранов, криптографических средств, систем резервного копирования, бесперебойного питания и аутентификации.

Криптография – наука об обеспечении секретности и (или) аутентичности передаваемых сообщений.

Криптографические методы являются наиболее эффективными средствами защиты информации в компьютерных системах. Показателями надежности криптографической защиты информации являются ее *криптостойкость* и *достаточность защиты*.

Криптостойкость – минимальный объем информации, который можно вскрыть в результате анализа.

Принцип достаточности защиты предполагает, что затраты на вскрытие информации должны превышать ее ценность.

Для шифрования текста применяют криптографические методы (алгоритмы), называемые ***шифром***. Наиболее простыми методами шифрования являются методы подстановки – замены символов шифруемого сообщения другими буквами того же или другого алфавита.

Более криптостойкие методы основаны на использовании ключа. ***Криптографический ключ*** – некоторая секретная последовательность символов или битов. Методы, использующие для шифрования и обратного чтения сообщения один и тот же ключ, называются *симметричными*. Недостаток этих методов – необходимость передачи ключа шифрования по защищенным каналам связи для прочтения сообщения.

В настоящее время наибольшее распространение получили *несимметричные* криптографические системы, основанные на использовании двух ключей: открытого (*public*) и закрытого (*private*). Открытый и закрытый ключи создаются одновременно и являются половинками одного ключа.

Принцип несимметричной системы заключается в том, что открытый ключ доступен всем и шифрование сообщения производится с его помощью. Зашифрованное сообщение можно прочесть только при использовании закрытого ключа, который находится у получателя сообщения.

При обмене электронными документами важным является установление авторства и подлинности документа. Решение этих задач возлагается на электронную цифровую подпись (ЭЦП).

Электронная подпись реализуется использованием открытого и закрытого ключей. Документ кодируется отправителем с помощью личного закрытого ключа, а расшифровать его можно только открытым ключом.

Назначение ЭЦП – сделать невозможным отказ отправителя от отправленного им сообщения, изменение отправленного сообщения получателем, изменение сообщения (с целью искажения) или повтор третьим лицом.

ЭЦП подтверждает целостность отправленной информации и личность отправителя. Электронная цифровая подпись применяется сегодня гораздо чаще, чем чистое шифрование.

1.4.3.1. Компьютерные вирусы

Надежность и защищенность работы компьютерных систем во многом определяется мерами самозащиты, которые предполагают противостояние разрушительному действию вредоносных программ – компьютерных вирусов. В результате заражения возможны искажение информации, полная ее потеря, а в некоторых случаях и выход из строя аппаратного обеспечения.

Компьютерный вирус – это программа, предназначенная для несанкционированного доступа к данным с целью их изменения или уничтожения.

Классификация вирусов осуществляется по следующим признакам:

1) *по среде обитания*:

сетевые (распространяются по компьютерным сетям);

файловые (внедряются в исполняемые файлы: .exe, .com);

загрузочные (внедряются в загрузочный сектор диска);

макровирусы (заражают текстовые файлы и файлы электронных таблиц, используя содержащиеся в них макросы);

2) *по способу заражения*:

резидентные (после исполнения зараженной программы остаются в оперативной памяти и продолжают деструктивные действия вплоть до выключения ПК);

нерезидентные (не заражают память компьютера и являются активными ограниченный период времени);

3) *по степени воздействия*:

безвредные (не оказывают влияния на работу ПК кроме уменьшения свободной памяти на диске в результате своего распространения);

неопасные (не выполняют деструктивных действий, уменьшают объем памяти на диске или производят графические и звуковые эффекты);

опасные (вызывают искажение или уничтожение информации);

очень опасные (кроме уничтожения информации выводят из строя ПК);

4) *по алгоритму функционирования*:

«троянские кони» («логические бомбы») – вирусы, маскирующиеся под полезные программы, нарушающие работу системы или собирающие информацию о ней;

стелс-вирусы (невидимки) – вирусы, способные скрываться при попытках их обнаружения. Они перехватывают обращения операционной системы к пораженным файлам или секторам дисков и подставляют вместо себя незараженные участки информации;

вирусы-призраки (мутанты) – трудно обнаруживаемые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса-призрака не будут иметь ни одного совпадения;

репликаторы (черви) – саморазмножающиеся сетевые вирусы.

Основное средство защиты информации от компьютерных вирусов – резервное копирование информации, вспомогательное – антивирусные программы.

Антивирус – программное средство, предназначенное для борьбы с вирусами.

Антивирусные программы подразделяются

на *программы-детекторы* (сканеры). Осуществляют поиск конкретных вирусов. Основаны на сравнении специфической последовательности сигнатур, содержащихся в теле вируса, и сигнатур проверяемых программ. Эти программы требуют регулярного обновления, так как быстро устаревают и не могут выявлять новые виды вирусов;

программы-доктора. Это программы, которые способны не только обнаружить, но и уничтожить вирус, т. е. удалить его код из зараженных программ и восстановить их работоспособность;

программы-ревизоры. Запоминают исходное состояние файлов и системных областей дисков и сравнивают его с текущими значениями;

программы-фильтры. Выявляют подозрительные процедуры, например, коррекцию исполняемых программ или загрузочных записей диска, изменение атрибутов или размеров файлов и др.;

программы-иммунизаторы (вакцины). Модифицируют существующую информацию, представляя ее вирусам как уже зараженную.

Многие современные антивирусные программы могут объединять в себе несколько из перечисленных компонентов.

1.5. Контрольные вопросы

1) Что такое ИБ?

2) Назовите известные модели разграничения доступа.

3) Что такое угроза ИБ? По каким признакам классифицируются угрозы информационной безопасности?

4) Назовите основные средства, обеспечивающие защиту информации.

5) Сформулируйте принцип достаточности защиты информации.

6) Что такое компьютерный вирус? По каким признакам классифицируются компьютерные вирусы?

2. КОМПЬЮТЕРНЫЕ СЕТИ

2.1. Понятие компьютерной сети

С появлением компьютеров вопросы обмена данными приняли глобальный характер. Потребность в совместном использовании данных на удаленных друг от друга компьютерах в конечном счете привела к созданию компьютерных сетей (КС).

Впервые в мире компьютерная сеть была применена в 1960 г. для работы комплекса противоракетной обороны СССР «Система А». В сеть объединили разработанные Институтом точной механики и вычислительной техники АН СССР компьютеры «Диана I» и «Диана II», в задачу которых также входило автоматическое слежение за воздушными целями.

Первая компьютерная сеть появилась в 1965 г. в США между Массачусетским технологическим институтом и корпорацией *SDC* (Калифорния).

Компьютерная сеть – совокупность компьютеров, объединенных средствами передачи данных.

Основное назначение КС – обеспечение совместного доступа к сетевым ресурсам: аппаратным, программным и информационным.

Аппаратные ресурсы – использование файлового сервера (компьютер с увеличенной емкостью жесткого диска), сетевого принтера и др.

Программные ресурсы – подключение к более мощной электронно-вычислительной машине (ЭВМ) для выполнения сложных расчетов и т. д.;

Информационные ресурсы – глобальная система объединенных компьютерных сетей для хранения и передачи информации.

Основные преимущества использования КС:

– совместный доступ пользователей к сетевым ресурсам;

– обеспечение высокой надежности передачи данных;

– расширяемость, т. е. возможность добавления новых компьютеров в КС;

– масштабируемость – способность увеличивать производительность КС по мере роста нагрузки;

– экономия средств;

– обеспечение возможности передачи данных между удаленными пользователями без промежуточных носителей информации.

2.2. Классификация КС

Компьютерные сети классифицируются по следующим признакам.

1. *По территориальной распространенности*:

– локальные вычислительные сети;

– корпоративные сети (Интранет);

– муниципальные или региональные вычислительные сети;

– глобальные вычислительные сети.

Локальная вычислительная сеть (ЛВС) – группа компьютеров, связанных каналами передачи информации и находящихся в пределах одного здания или на территории какой-либо организации площадью до нескольких квадратных километров. ЛВС создаются для совместного доступа к общим ресурсам (принтеры и др.) и эффективного обмена информацией. Разновидностью ЛВС считаются персональные сети, предназначенные для взаимодействия различных устройств, принадлежащих одному владельцу.

Основными преимуществами ЛВС являются высокая скорость передачи информации; незначительный уровень ошибок передачи, вызванных как внутренними, так и внешними факторами; быстродействующий механизм управления обменом данных.

К недостаткам ЛВС относятся значительные материальные затраты на сетевое оборудование, программное обеспечение и т. д.; потребность в специали-

сте (администраторе сети), обслуживающем, контролирующем сетевое оборудование; необходимость защиты информации.

Корпоративные сети (Интранет) – разновидность ЛВС, располагающихся в пределах крупной организации. Примером Интранета является ЛВС ОАО «РЖД».

Муниципальная, или региональная, вычислительная сеть (МВС) – группа компьютеров, связанных каналами передачи информации и находящихся в пределах одного города. Распространенным примером МВС является система кабельного телевидения.

Глобальная вычислительная сеть (ГВС) – сеть, охватывающая значительную географическую область, часто целую страну или континент. ГВС объединяет множество компьютеров, называемых *хóстами*, которые соединяются коммуникационными подсетями. Задачей подсети является передача данных от хоста хосту.

2. *По принципу организации иерархии компьютеров*: одноранговые и с выделенным сервером.

В одноранговых сетях все компьютеры имеют одинаковые права (ранги). В сетях с выделенным сервером компьютеры подразделяются на два типа: сервер и клиент.

Устройство, подключенное к сети и активно участвующее в информационном обмене, называется ***абонентом***. Абонентом сети является компьютер, терминал, промышленный робот или другое устройство, имеющее возможность напрямую подключаться к сети.

Сервер – компьютер, предоставляющий свои ресурсы другим абонентам, не используя их ресурсы.

Выделенный сервер – сервер, управляющий распределением сетевых ресурсов.

Клиент – абонент сети, использующий сетевые ресурсы. Компьютер-клиент называется ***рабочей станцией***.

В сетях с выделенным сервером различают две архитектуры использования сервера: файл-сервер и клиент-сервер.

При использовании архитектуры *файл-сервер* данные по запросу пользователя пересылаются с сервера ему на компьютер-клиент, где обрабатываются.

В *клиент-сервере* данные обрабатываются на сервере по запросу пользователя, компьютер-клиент получает только результаты запроса.

Совокупность приемов разделения и ограничения прав участников сети называется ***политикой сети***. Управление сетевыми политиками осуществляет ***системный администратор***.

3. *По типу среды передачи*: проводные и беспроводные.

4. *По типу сетевой топологии* выделяются радиальные, шинные, кольцевые и древовидные КС. *Топология КС* характеризует способ организации физических связей компьютеров и других сетевых компонентов.

В зависимости от назначения КС могут иметь различную топологию (архитектуру, конфигурацию). Приведем базовые топологии КС.

Радиальная (*звездообразная*) топология является наиболее распространенной архитектурой КС (рис. 5). В центре такой КС находится управляющий компьютер-концентратор, который последовательно связывается с абонентами и связывает их друг с другом.

Кольцевая конфигурация подразумевает соединение компьютеров в замкнутое кольцо (рис. 6). Каждый абонент непосредственно связан с двумя ближайшими соседями. Данные в КС передаются от одного компьютера к другому до тех пор, пока не найдут своего адресата.

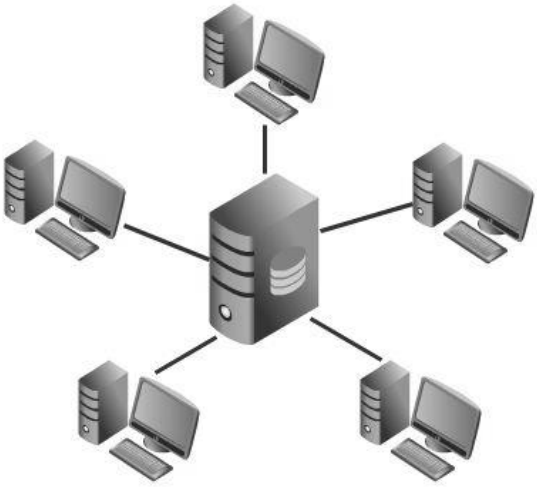

Рис. 5. Радиальная топология КС

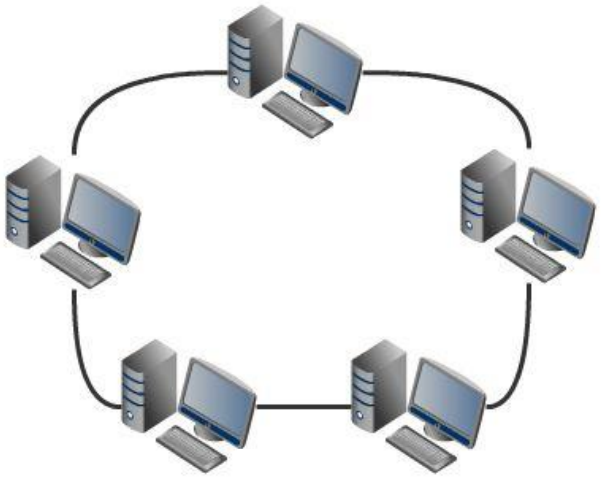

Рис. 6. Кольцевая топология КС

Шинная конфигурация подразумевает подключение компьютеров к общему для них каналу (шине), по которому они обмениваются данными (рис. 7).

Древовидная конфигурация предполагает многоуровневую, разветвленную архитектуру с сервером, которому подчинены компьютеры следующего уровня и т. д. (рис. 8).

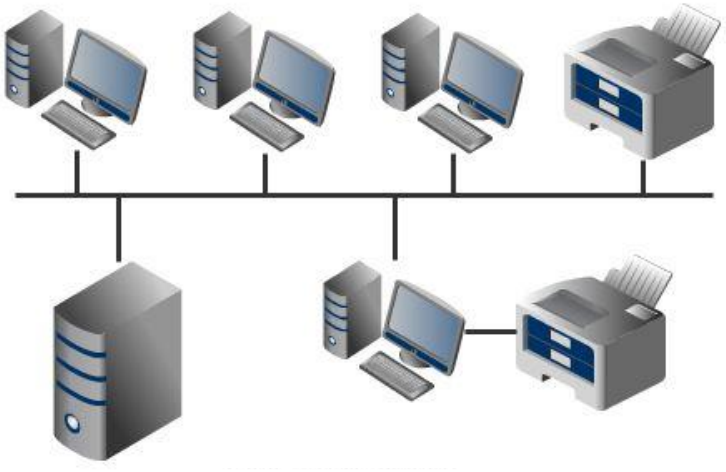

Рис. 7. Шинная топология КС

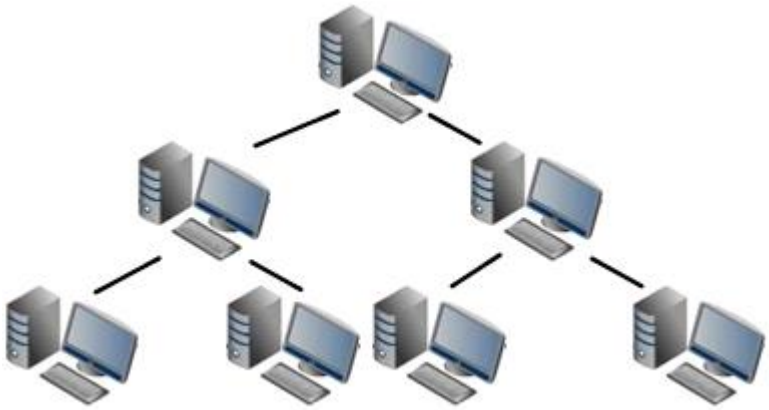

Рис. 8. Древовидная топология КС

Существуют определенные *стратегии доступа* от одного компьютера к другому:

маркерный метод доступа (селективная передача): маркер передается от центрального компьютера сети компьютеру пользователя.

Маркер – сигнал на право ведения передачи данных в течение определенного времени, после чего маркер передается другому компьютеру;

конкурентный метод доступа: передача данных компьютером начинается, если обнаруживается свободная линия или передача откладывается на некоторый промежуток времени, если линия занята другим компьютером;

метод резервирования времени: у каждого компьютера имеется определенный промежуток, в течение которого линия принадлежит только ему.

Наиболее часто применяется конкурентный метод доступа.

2.3. Сетевое оборудование

В состав базовых компонентов КС входит специальное аппаратное (сетевой адаптер, сетевой кабель, концентратор, средства связи) и программное обеспечение (сетевые программные средства). Сетевыми программными средствами осуществляется управление работой КС, а также защищаются передаваемые по сети данные.

2.3.1. Среда передачи данных

Среда передачи данных – линия связи, по которой производится обмен данными между компьютерами.

Линии связи – промежуточная аппаратура и физическая среда, по которой передаются информационные сигналы (данные).

Канал связи – совокупность технических средств, обеспечивающих одностороннюю передачу данных от отправителя к получателю (рис. 9). Канал связи является составной частью канала передачи данных.

Канал передачи данных – средства обмена данными, обеспечивающие передачу сигнала во взаимопротивоположных направлениях, включающие в себя линии связи и аппаратуру передачи (приема) данных.

Рис. 9. Канал связи

В проводных линиях связи передача данных в КС осуществляется электрическими сигналами и световыми импульсами.

В проводных линиях связи все используемые кабели разделяются на три группы: симметричные (витая пара), коаксиальные и оптоволоконные кабели.

При выборе типа кабеля учитываются особенности решаемой в рамках конкретной КС задачи.

Симметричный кабель (витая пара) – кабель связи, представляющий собой несколько пар скрученных изолированных медных проводов в единой диэлектрической оболочке. Пары проводов скручиваются между собой для улучшения помехозащищенности. Существует два типа витой пары: неэкранированная (рис. 10, а) и экранированная (рис. 10, б), которые находят применение в радиальной и шинной топологиях.

а б

Рис. 10. Витая пара: а – неэкранированная; б – экранированная

Неэкранированная витая пара характеризуется низким уровнем помехозащищенности и слабой защищенностью от несанкционированного доступа. Для устранения этих недостатков витая пара экранируется, т. е. каждая пара проводов помещается в металлическую оплетку-экран.

Основным преимуществом витых пар является простота монтажа разъемов на концах кабеля и ремонта любых повреждений. Скорость передачи данных через витую пару составляет до 100 Мбит/с.

Коаксиальный кабель – электрический кабель, состоящий из центрального медного провода и металлической оплетки, разделенных слоем изоляции и помещенных в общую внешнюю оболочку (рис. 11).

Коаксиальный кабель, как правило, применяется в КС с шинной топологией.

Существенными недостатками этого кабеля являются сложность монтажа, высокая стоимость, ограниченная полоса пропускания. Скорость передачи информации через коаксиальный кабель достигает 50 Мбит/с.

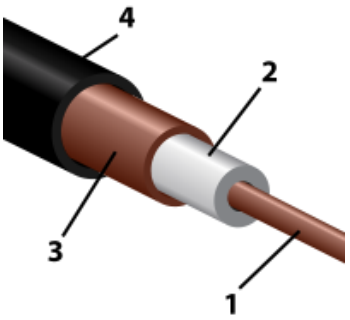

Рис. 11. Коаксиальный кабель:
1 – центральный медный провод;
2 – изоляционный слой;
3 – металлическая оплетка;
4 – внешняя оболочка

Основными преимуществами коаксиального кабеля являются высокая помехозащищенность, большие допустимые расстояния передачи данных, защищенность от несанкционированного доступа.

Оптоволоконный кабель – кабель, состоящий из прозрачного стекловолокна, по которому проходит световой сигнал (рис. 12). Оптоволоконный кабель применяется, как правило, в сетях с радиальной и кольцевой топологиями.

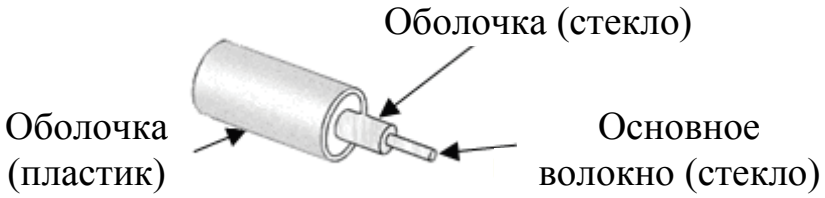

Рис. 12. Оптоволоконный кабель

В зависимости от траектории распространения света различают одномодовый и многомодовый кабели (рис. 13). Главное различие одномодового и многомодового кабелей – размерные показатели. В одномодовом кабеле толщина основного волокна составляет 8 – 10 мкм. Это обусловливает возможность передавать волну только одной длины по центральной моде.

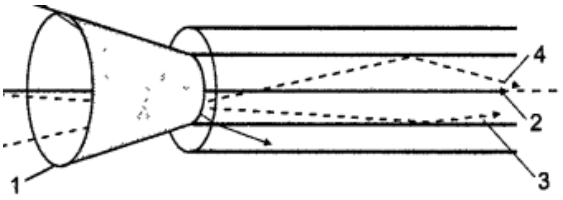

Рис. 13. Ввод света в оптоволокно:
1 – входной конус; 2 – осевая мода;
3, 4 – моды низкого и
высокого порядка

В многомодовом кабеле толщина основного волокна составляет 50 – 60 мкм. Такой кабель позволяет одновременно передавать несколько волн с разной длиной по нескольким модам. Следует отметить, что большое количество мод сужает пропускную способность оптоволоконного кабеля.

К недостаткам оптоволоконного кабеля относятся сложность монтажа, меньшая прочность и гибкость по сравнению с витой парой, чувствительность к механическим повреждениям и резким перепадам температуры окружающей среды. Основными положительными свойствами оптоволоконного кабеля являются надежные помехозащищенность и защита передаваемых данных от несанкционированного доступа. Световой сигнал не порождает внешних электромагнитных излучений.

Скорость передачи информации через одномодовый оптоволоконный кабель варьируется от 2,5 до 10 Гбит/с, через многомодовый кабель – от 10 Мбит/с до 1 Гбит/с.

В зависимости от стратегии сетевого доступа применяются различные среды передачи данных. Например, коаксиальный кабель, неэкранированная витая пара и оптоволоконный кабель применяются при конкурентном методе доступа.

В беспроводных линиях связи передача данных осуществляется инфракрасными и радиоволнами.

Радиоканал – беспроводной канал связи, использующий для передачи данных радиоволны. Радиоканал не применяется в ЛВС из-за высокой стоимости передающих и приемных устройств, низкой помехозащищенности и практически полного отсутствия защиты от несанкционированного доступа к передаваемой информации. Для глобальных сетей радиоканал является одним из способов простой передачи данных через спутники-ретрансляторы. Скорость передачи данных в радиоканале достигает десятков мегабит в секунду.

Инфракрасный канал – беспроводной канал связи, использующий для передачи данных инфракрасное излучение. К недостаткам инфракрасного канала относятся высокая чувствительность к запыленности воздуха, низкая скорость передачи информации (5 – 10 Мбит/с), отсутствие защиты от несанкционированного доступа к информации, дорогостоящие приемники и передатчики. Основное преимущество инфракрасного канала по сравнению с радиоканалом заключается в нечувствительности к электромагнитным помехам.

Все беспроводные каналы применяются в КС с шинной топологией.

2.3.2. Сетевой адаптер

Сетевой адаптер – периферийное устройство компьютера, предназначенное для приема-передачи сигналов КС.

Функции сетевого адаптера:

1) анализ корректности принимаемых сигналов;

2) получение доступа к среде передачи данных;

3) кодирование информации из формы, удобной для ее представления, в форму, удобную для передачи;

4) поддержание постоянного синхронизма приемника и передатчика информации для устойчивого приема данных.

2.3.3. Маршрутизатор

Маршрутизатор (роутер) – устройство, работающее на сетевом уровне и позволяющее перенаправлять данные из одной КС в другую (рис. 14).

Маршрутизатором выполняется функция оптимизации пути передачи данных.

Существуют два типа маршрутизирующих устройств: статические и динамические. Статические маршрутизаторы используют таблицы маршрутизации, создаваемые и вручную обновляемые сетевым администратором. Динамические маршрутизаторы создают и обновляют свои собственные таблицы маршрутизации.

Рис. 14. Маршрутизатор

2.3.4. Мост

Мост (бридж) – устройство, обеспечивающее соединение нескольких ЛВС между собой (рис. 15).

Мост предназначается для структуризации КС или для соединения нескольких КС, имеющих различную топологию. Одной из проблем крупных КС является напряженный обмен данными. Такая проблема решается с применением моста и разделением КС на сегменты.

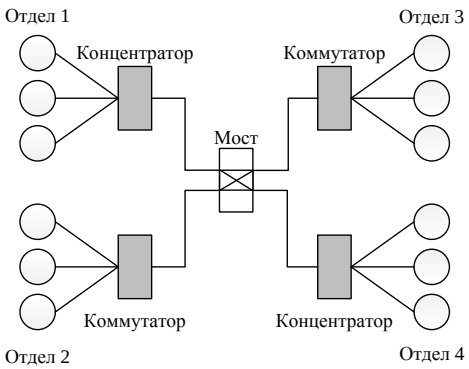

Рис.15. Мост

Мост ограничивает передачу сообщений из одного сегмента сети в другой без подтверждения права на переход.

2.3.5. Повторитель

Повторитель (репитер) – устройство, обеспечивающее усиление и фильтрацию сигнала без изменения его информативности.

Повторители используются для уменьшения явления затухания сигналов. Повторитель не только копирует или повторяет принимаемые сигналы, но и восстанавливает характеристики сигнала, т. е. происходит усиление сигнала и устранение помех.

2.3.6. Концентратор

Концентратор (хаб) – сетевое устройство, принимающее сигналы одного порта и воспроизводящее их для всех остальных портов (см. рис. 15).

У концентраторов и повторителей имеются одинаковые характеристики, поэтому концентраторы часто называются многопортовыми повторителями. Различие между повторителем и концентратором заключается в количестве кабелей, присоединяемых к устройству: у повторителя имеется два порта, у концентратора – от четырех до 20 и более портов.

2.3.7. Коммутатор

Коммутатор (свитч) – устройство, объединяющее несколько сегментов КС и обеспечивающее прием данных и их передачу адресатам (см. рис. 15).

Отличие коммутатора от концентратора заключается в способности передавать сообщения конкретному компьютеру. При отправлении сообщения от одного компьютера другому через коммутатор считывается физический адрес целевого устройства и устанавливается соединение, по которому происходит обмен данными.

2.3.8. Сетевой шлюз

Сетевой шлюз – специальный аппаратно-программный комплекс, обеспечивающий совместимость между сетями, которыми используются различные сетевые протоколы.

Шлюз преобразует данные, поступившие из одной КС, соответственно требованиям другой КС. Работа шлюза не зависит от используемой среды передачи данных, но зависит от используемых сетевых протоколов обмена данными.

2.3.9. Межсетевой экран

Для обеспечения сетевой безопасности между КС устанавливается межсетевой экран (брандмауэр, файрвол).

Межсетевой экран – компьютер, или компьютерная программа, препятствующая несанкционированному перемещению данных между КС.

Основной задачей межсетевого экрана является защита КС от данных, не удовлетворяющих заранее определенным критериям.

2.4. Контрольные вопросы

1) Что называется КС?

2) По каким признакам классифицируются КС?

3) В чем заключается отличие одноранговых КС от сетей с выделенным сервером?

4) Какие базовые топологии КС существуют?

5) Назовите основные виды сетевого оборудования. Какие функции оно выполняет?

6) Какие среды передачи данных существуют? Назовите их основные преимущества и недостатки.

3. ИНТЕРНЕТ. ИНФОРМАЦИОННЫЕ СЕРВИСЫ

3.1. Глобальные сети

Потребности формирования единого мирового информационного пространства привели к созданию глобальных КС.

Глобальная КС – совокупность КС и компьютеров, расположенных на больших расстояниях и соединенных в единую систему.

Глобальные КС объединяют как отдельные компьютеры, так и отдельные КС, в том числе и использующие различные сетевые протоколы. При подключении КС к глобальной КС важную роль играет сетевая безопасность. Основное отличие глобальных КС от ЛВС заключается в увеличенных физических и географических размерах. Крупнейшей глобальной КС является Интернет.

Интернет – глобальная КС, объединяющая компьютеры тысяч региональных КС и миллионов пользователей всего мира. В настоящее время Интер-

нет – коммуникационная платформа, соединяющая людей и организации в самых разных сферах жизнедеятельности. Благодаря глобальной сети мировому сообществу стал доступен огромный объем разнообразной информации: от повседневных новостей до деловой информации корпораций и организаций. Интернет обеспечивает пользователям доступ к информации, размещенной на многочисленных интернет-серверах. Серверы имеют свои адреса и управляются специализированными программами, позволяя обмениваться информацией, производить поиск в базах данных и т. д. Обмен информацией между серверами сети выполняется по высокоскоростным каналам связи.

Доступ отдельных пользователей к информационным ресурсам Интернета осуществляется через ***поставщика интернет-услуг (провайдера)***. Организации, предоставляющие услуги для работы в сети, называются ***сервис-провайдерами***.

3.2. История развития сети Интернет

Зарождение Интернета связано с реализацией первой исследовательской программы Агентства передовых исследовательских проектов в области обороны при Министерстве обороны США. Работа над системой глобальной коммуникации началась 4 октября 1962 г. Возглавлявший программу Дж. Ликлайдер опубликовал работу «Galactic Network», в которой описал возможность существования в будущем глобальной компьютерной связи между людьми, имеющими мгновенный доступ к программам и базам данных из любой точки планеты.

В 1966 г. началась разработка проекта компьютерной сети ARPANet. В декабре 1969 г. сдана в эксплуатацию первая экспериментальная КС, объединяющая четыре узла со скоростью передачи данных 56 кбит/с. В 1970-х гг. сеть использовалась в основном для пересылки электронной почты. Впоследствии к сети ARPANet подключились тысячи серверов и локальных сетей, что привело к созданию прародительницы современной сети Интернет ARPA Internet.

С 1983 г. в качестве основы архитектуры сети ARPANet стал применяться протокол *TCP/IP* (см. подразд. 3.3). Перегрузки на линиях связи и запрет на использование КС в коммерческих целях осложнили развитие ARPANet.

В 1985 г. появилась новая КС NSFNet, созданная Национальным научным фондом США. Новая сеть объединила пять суперкомпьютеров, а впоследствии и

целый ряд университетских сетей. Кроме исследовательских задач NSFNet применялась для передачи электронной почты, файлов и публикации новостей.

В 1989 г. сотрудником Европейского центра ядерных исследований Т. Бернерс-Ли был предложен гипертекстовый проект, получивший название «Всемирная паутина» (*world wide web, www*). Проект рассматривал публикацию гипертекстовых документов, связанных между гиперссылками, а также возможность просмотра текста и графики.

В 1993 г. архитектура сети NSFNet радикальным образом изменилась:

1) доступ к информационным ресурсам стал осуществляться через провайдера;

2) создана разветвленная сеть точек доступа к КС, посредством которых провайдерами осуществлялся обмен данными;

3) согласованы протоколы работы в сети и управление адресами компьютеров-клиентов между провайдерами;

4) утвержден единый провайдер для службы обеспечения высокоскоростной магистральной КС.

30 апреля 1995 г. архитектура NSFNet превратилась в Интернет.

3.3. Сетевые протоколы

При создании КС, как правило, *основной решаемой задачей* является обеспечение совместимости характеристик (электрических и механических) оборудования и совместимости программ с данными по системе кодирования и формату представления. Для согласованной работы сетевого оборудования специалистами разрабатываются технические соглашения (протоколы) об унификации формы представления и способов пересылки данных, а также о совместной работе различного оборудования в КС.

Протокол – набор правил, определяющих характер аппаратного взаимодействия сети (аппаратный протокол) и характер взаимодействия программ и данных (программный протокол).

Протокол предназначается

для преобразования данных в набор пакетов на передающей стороне и сбора набора пакетов в сообщение на принимающей стороне;

управления адресацией пакетов, т. е. направления их по маршруту между узлами.

Компьютерными сетями и информационными службами, как правило, используются различные протоколы. В 1982 г. в рамках проекта Международной организации по стандартизации (*ISO – International Organization for Standardization*) и Международного союза электросвязи (*ITU – International Telecommunication Union*) разработана модель взаимодействия открытых систем передачи данных – *Model of Open System Interconnections* (*OSI*).

Архитектура КС в модели *OSI* рассматривается на семи уровнях (рис. 16). Высший уровень функционирования систем передачи данных – прикладной: на этом уровне пользователь взаимодействует с компьютерной системой, низший уровень – физический: он обеспечивает обмен сигналами между устройствами.

На прикладном уровне пользователем создается документ. Местоположение документа фиксируется на уровне представления. Затем в рамках сеансового уровня производится проверка прав пользователя на выход в сеть. На транспортном уровне документ преобразуется для передачи (нарезка пакетов). Пакетам присваиваются адреса, и на сетевом уровне определяется маршрут движения. На уровне соединения формируются сигналы передачи данных. Непосредственно передача данных производится на физическом уровне.

Компьютер-отправитель				**Компьютер-клиент**
1. Прикладной уровень	↓		↑	1. Прикладной уровень
2. Уровень представления	↓		↑	2. Уровень представления
3. Сеансовый уровень	↓		↑	3. Сеансовый уровень
4. Транспортный уровень	↓		↑	4. Транспортный уровень
5. Сетевой уровень	↓		↑	5. Сетевой уровень
6. Уровень соединения	↓		↑	6. Уровень соединения
7. Физический уровень	↓	⟹	↑	7. Физический уровень

Рис. 16. Архитектура компьютерных сетей (модель *ISO*/*OSI*)

Обмен данными в КС производится перемещением данных с высшего уровня на низший, затем – транспортировкой и обратным воспроизведением на компьютере клиента с низшего уровня на верхний.

Стандартным промышленным протоколом, обеспечивающим связь между компьютерами разных типов, является протокол *TCP/IP*, который состоит из двух частей, объединяющих более 100 протоколов различного уровня.

Протокол TCP (*transmission control protocol* – протокол управления передачей данных) – протокол транспортного уровня, преобразующий данные в поток пакетов на передающей стороне и собирающий пакеты в сообщения на принимающей стороне.

Протокол IP (*internet protocol* – протокол Интернета) – адресный протокол, принадлежащий сетевому уровню и определяющий наилучший маршрут движения пакетов данных между узлами сети.

3.4. Адресация в Интернете

Каждый компьютер имеет в сети два равноценных уникальных адреса: ***цифровой IP-адрес*** и ***символьный доме́нный адрес***. *IP*-адрес распознается сетевым оборудованием, доменный адрес используется пользователем.

IP-адрес компьютера представляет собой идентификационный номер, длиной 32 бита (4 байта). Первый и второй байты определяют адрес сети, третий байт – адрес подсети, четвертый – адрес компьютера в подсети. Для удобства *IP*-адрес записывается в виде четырех чисел со значениями от 0 до 255, разделенных точками, например: 192.45.9.200. Адрес сети – 192.45; адрес подсети – 9; адрес компьютера в подсети – 200.

```
Microsoft Windows [Version 6.1.7601]
<c> Корпорация Майкрософт <Microsoft Corp.>, 2009. Все права защищены.

C:\Users\User1>ipconfig
Настройка протокола IP для Windows


Ethernet adapter Подключение по локальной сети:

     DNS-суффикс подключения ..... : omgups.ru
     Локальный IPv6-адрес канала  ..... : fe80::552b:2a5a:83a6:66844%11
     IPv4-адрес ..... : 192.168.4.66
     Маска подсети ..... : 255.255.255.0
     Основной шлюз ..... : 192.168.4.1

Туннельный адаптер  isatap.omgups.ru:

Состояние среды ..... : Среда передачи недоступна.
DNS-суффикс подключения ..... : omgups.ru
```

Рис. 17. Вид окна командной строки

Для определения *IP*-адреса компьютера в локальной сети необходимо нажать сочетание клавиш *Win+R* и в строку <Открыть> ввести команду <*cmd*>.

В открывшемся окне командной строки требуется ввести команду *ipconfig*, в строке *IPv*4-адрес появится искомая информация (см. рис. 17).

Для быстрого получения базовой информации о компьютере и сети можно воспользоваться командами, представленными в таблице.

Команды, применяемые для получения информации о компьютере и сети

Команда	Получаемые сведения
hostname	Имя компьютера
ipconfig	*IP*-адрес компьютера
ipconfig/all	Отображение полной информации о всех сетевых устройствах
ping доме́нное имя компьютера	Определение *IP*-адреса сетевого устройства с помощью доменной системы имен
ping IP-адрес компьютера	Проверка связи с другим компьютером

Наряду с цифровым *IP*-адресом в Интернете применяется *Доме́нная система имен*, которая ставит в соответствие цифровому *IP*-адресу компьютера уникальное доме́нное имя. Например, *IP*-адрес 80.89.136.2 соответствует доме́нному имени *www.omgups.ru*.

Домен – совокупность компьютеров с единой базой имен. Для преобразования символьного доме́нного имени в *IP*-адрес цифрового формата служат *DNS*-серверы (*DNS – domain name system*).

Система доме́нных имен строится по иерархическому принципу. Доменов верхнего уровня всего около 250. Как правило, это географические домены (*ru, uk* и т. д.). Следующий уровень доменов обычно указывает регион или название крупной корпорации и т. д. Доменные имена записываются, начиная с младшего уровня, например: *encycl.yandex.ru, encycl* – домен третьего уровня, *yandex* – домен второго уровня, *ru* – домен верхнего уровня.

Выделением *IP*-адресов и назначением им доменных имен в Интернете занимается специальная служба. Для определения *IP*-адреса компьютера по доменному имени применяются многочисленные интернет-сервисы, например,

2ip.ru, а также команда *ping доменное имя компьютера* через окно командной строки. Для определения доменного имени по известному *IP*-адресу применяются интернет-сервисы, например, *nslookup.su*.

Обращение к любому документу в сети Интернет осуществляется с помощью ***универсального указателя ресурса*** (*URL – uniform resource locator*), который указывает местонахождение каждого файла, хранящегося на компьютере, подключенном к Интернету. *URL* состоит из трех частей:

Протокол службы доступа к ресурсу://Доменное имя компьютера/
Полный путь к файлу

При записи *URL* следует точно соблюдать регистр символов.

Пример *URL*:

http://www.abc.def.ru/dir/name.htm

где http:// – протокол передачи гипертекста;

www.abc.def.ru – доменное имя компьютера (www – узел находится в *Web*; abc.def – имя сервера; ru – суффикс (узел находится в России));

dir/name.htm – расположение ресурса на данном сервере. Ресурсом в данном примере является файл *name* в формате *html*, который находится в папке *dir*.

Для обозначения коммерческих узлов применяется суффикс .com, правительственных – *.gov*, учебных – *.edu*, военных – *.mil*, некоммерческих – *.org* и т. д.

3.5. Службы Интернета

Интернет предоставляет своим клиентам ряд услуг (сервисов), называемых ***службами***. Наиболее часто используются следующие службы: электронная почта, всемирная информационная сеть *www*, службы телеконференции и мгновенных сообщений, передача файлов и др.

Электронная почта (*e-mail*) используется для передачи, приема, хранения и обработки почтовых сообщений.

Всемирная информационная сеть www – сервис Интернета, поддерживающий поиск и просмотр гипертекстовых документов, связанных между собой гиперссылками.

Текст, содержащий гиперссылки, связывающие слова или картинки документа с другим ресурсом, называется *гипертекстом*.

Документы, доступные через *web*, называются *web-страницами*, которые форматируются специальным образом и тематически объединяются в *web*-узлы, или *web*-сайты.

Для просмотра *web*-страниц и перемещения между ними используются специальные программы – *браузеры* (*browser* – обозреватель).

Основные функции браузера:

1) установление связи с *web*-страницей по ее *URL*-адресу и обеспечение управления загрузкой содержимого *web*-страницы на локальный компьютер пользователя;

2) отображение содержимого *web*-страницы на экране компьютера, в том числе ее мультимедийного содержимого, в соответствии с пользовательскими настройками компьютера и его аппаратно-программными возможностями;

3) сохранение содержимого *web*-страницы на локальном компьютере пользователя;

4) обеспечение сервисных возможностей работы с *web*-страницей;

5) предоставление пользователям доступа к средствам для работы с другими сервисами Интернета.

В настоящее время распространенными браузерами являются *Google Chrome, Mozilla Firefox, Internet Explorer, Opera, Safari* и др.

Для доставки документа браузеру *web*-сервером используется специальный протокол *HTTP* (*hypertext transfer protocol* – протокол передачи гипертекста).

Web-сервер – программа, умеющая получать *HTTP*-запросы пользователей и выполнять в соответствии с этими запросами определенные действия (запускать приложения и генерировать документы).

Служба телеконференции (*Usenet*) – рассылка электронной почты большой группе корреспондентов. Такие группы называются телеконференциями, или группами новостей. Служба телеконференции содержит тематические группы информации. Особенность службы телеконференции заключается в возможности пользователя задать вопрос по теме любой группы телеконференции и выбрать ответ из множества поступивших.

Служба мгновенных сообщений – беседы через Интернет в реальном времени. Сервис похож на телеконференции, но отличается тем, что переговоры с группой пользователей происходят в реальном времени без задержек, подобно разговору людей, собравшихся в одном помещении.

В настоящее время одним из самых распространенных информационных сервисов в сети Интернет является служба передачи файлов.

Служба передачи файлов (*FTP – file transfer protocol*) – средства доступа к *FTP*-серверам, хранящим архивы данных. Для работы с *FTP*-серверами используются специальные программы: *FTP*-клиент *Cute FTP*, файловый менеджер *Magellan Explorer* и др.

Адресация к *FTP*-архивам подчиняется тем же правилам, что и адресация к *web*-сайтам. Отличие адреса *FTP*-сервера от адреса *web*-сайта заключается в имени протокола. Наличие имени протокола в адресе *FTP*-сервера является обязательным в случае совпадения адреса *FTP*-сервера с адресом *web*-сайта. Это объясняется более высоким приоритетом протокола *HTTP* относительно протокола *FTP*. Например, при наборе в адресной строке только имени *mp3.int.ru* откроется *web*-сайт. Для доступа к *FTP*-серверу необходимо указать адрес вместе с протоколом. Например: *ftp://mp3.int.ru*

Для доступа к *FTP*-серверу зачастую требуется прохождение аутентификации: указание имени пользователя и пароля при запросе *FTP*-клиента или в *URL*:

ftp://<имя_пользователя>:<пароль>@<доменное_имя_*FTP*_сервера>

Аутентификация с применением *FTP*-клиента предпочтительнее, поскольку пользовательские регистрационные данные, передаваемые в строке *URL*, являются незащищенной информацией.

Среди наиболее распространенных способов доступа в Интернет выделяются цифровая абонентская линия (1 – 8 Мбит/с) и сети кабельного телевидения, радиоканалы, спутниковые каналы (1 – 100 Мбит/с).

3.6. Web-поиск

Для поиска информации в сети Интернет созданы поисковые серверы (поисковики), для ускорения доступа информация упорядочена с помощью каталогов (рубрикаторов), списков рейтингов, тематических списков ссылок, онлайн-энциклопедий, справочников и т. д.

Поисковая система – комплекс программных и аппаратных средств с *web*-интерфейсом, предназначенный для автоматического просмотра интернет-

ресурсов, индексации их содержания и предоставления услуг по поиску информации пользователям сети Интернет.

Одной из первых поисковых систем является *Archie*. Среди первых поисковых машин для Интернета выделяется интернет-робот *Wandex*, разработанный в 1993 г. Одновременно с *Wandex* появляется другая поисковая машина *Aliweb*, функционирующая по настоящее время.

В 1994 г. появляется первая полнотекстовая поисковая машина *WebCrawler*. Ключевое отличие ее от предшественников заключается в возможности поиска по любым ключевым словам на любой *web*-странице. Эта возможность стала стандартом во всех основных поисковых машинах.

В 1996 г. русскоязычным пользователям сети Интернет становятся доступными оригинальные российские поисковые машины «Рамблер» и «Апорт». В 1997 г. становится доступной поисковая машина «Яндекс», а в 2014 г. – национальная поисковая машина «Спутник».

Поисковые системы классифицируются по эффективности поиска, по языку поиска (русский, английский и т. д.), по типу (универсальные и специализированные). Одни поисковые системы способны находить информацию только в виде *web*-страниц, другие – просматривать и группы новостей, и файловые серверы.

В настоящее время наиболее популярными международными системами для поиска информации в информационных ресурсах являются следующие:

Google (*http://www.google.com/*);

Microsoft Live Search (*http://www.live.com/*);

Alta Vista (*http://www.altavista.com/*);

Yahoo! (*http://www.yahoo.com/*);

Infoseek (*http://www.infoseek.com/*);

Hot bot (*http://hotbot.com/*).

Среди наиболее популярных российских поисковых систем выделяют:

Рамблер (*http://www.rambler.ru/*);

Яндекс (*http://www.yandex.ru/*);

Апорт (*http://www.aport.ru/*).

3.7. Электронная почта

Одним из самых популярных сервисов Интернета является электронная почта – услуги по пересылке и получению электронных сообщений через Интернет.

Впервые почтовое сообщение было отправлено в 1971 г. Реем Томплинсоном – создателем программы, отправляющей текстовые сообщения с одного компьютера на другой в пределах сети ARPANet. Через год объем передаваемых по сети сообщений электронной почты достиг 75 %. Впервые электронная рассылка – периодическая отправка на определенные адреса электронных писем – появилась в 1975 г.

Для приема и хранения писем используются почтовые серверы.

Почтовый сервер – программа, пересылающая сообщения из электронных почтовых ящиков на другие серверы или на компьютер пользователя по запросу его почтового клиента.

Электронный почтовый ящик – дисковое пространство, выделяемое на почтовом сервере для хранения писем пользователя. Электронный почтовый ящик защищается именем пользователя и паролем доступа. Пользователь электронного почтового ящика пользуется почтовым клиентом.

Почтовый клиент – программа, используемая для составления и рассылки электронных сообщений, а также для получения и отображения их на компьютере пользователя.

Для отправки и получения электронных писем применяются специальные протоколы.

SMTP (*simple mail transfer protocol*, простой протокол передачи почты) – протокол, применяемый для отправки сообщений от пользователя на почтовый сервер или от одного почтового сервера другому.

Пользователи электронной почты регистрируются на почтовом сервере. Каждой учетной записи присваивается электронный адрес, например:

my.name@bk.ru

где *my.name* – имя пользователя и его почтового ящика;

bk.ru – имя домена, в котором находится почтовая служба;

@ – символ «*at*», применяемый для отделения имени пользователя от имени домена.

Доступ пользователя к его почтовому ящику обеспечивается протоколами ***POP3*** (*post office protocol*, протокол почтового офиса, версия 3) или ***IMAP*** (*internet message access protocol*, протокол доступа к сообщениям Интернета). Отличие протокола *POP3* от *IMAP* заключается в возможности управления электронной корреспонденцией на почтовом сервере.

В настоящее время протокол *POP3* является самым распространенным. Протокол *POP3* позволяет пользователю получить доступ к почтовому ящику на сервере и переслать сообщения на компьютер пользователя. Протокол *IMAP* позволяет пользователю работать с сообщениями непосредственно на сервере.

Распространенными почтовыми клиентами являются *Microsoft Outlook*, *Netscape Messenger* и др.

3.8. Контрольные вопросы

1) Что такое глобальная КС?

2) Какая КС явилась прообразом сети Интернет?

3) На каких уровнях рассматривается архитектура КС в модели взаимодействия открытых систем OSI?

4) Что такое домен? Каково назначение символьного доменного имени компьютера?

5) Какой байт в *IP*-адресе компьютера отвечает за адрес подсети?

6) Что такое почтовый сервер и почтовый клиент?

7) Назовите протоколы, применяемые для отправки и получения электронных писем.

4. ТЕМЫ РЕФЕРАТОВ

1) История развития методов и средств защиты информации.

2) История развития компьютерных сетей.

3) Сетевое оборудование компьютерных сетей.

4) Структура сети Интернет.

5) Угрозы информационной безопасности.

6) Технические средства защиты информации.

7) Компьютерные вирусы.

8) Программные средства защиты информации.

9) Антивирусные программы.

10) Топологии компьютерных сетей.

11) Службы Интернета.

12) Электронная почта.

13) Модель взаимодействия открытых систем.

14) Web-поиск.

15) Адресация в сети Интернет.

16) Всемирная паутина.

17) Служба телеконференции.

18) Корпоративные сети Интранет.

19) Глобальные компьютерные сети.

20) Служба мгновенных сообщений.

21) Служба передачи файлов.

5. ПРИМЕРЫ ТЕСТОВЫХ ВОПРОСОВ

Вопрос № 1 (один верный ответ).

Транспортный протокол (*TCP*) обеспечивает …

Варианты ответов:

1) преобразование данных в поток пакетов на передающей стороне и сбор пакетов в сообщения на принимающей стороне;

2) прием, передачу и выдачу одного сеанса связи;

3) предоставление в распоряжение пользователя уже переработанной информации.

Вопрос № 2 (один верный ответ).

Протокол маршрутизации (*IP*) обеспечивает …

Варианты ответов:

1) управление адресацией пакетов, определяя наилучший маршрут движения пакетов данных между узлами сети;

2) интерпретацию данных и подготовку их для пользовательского уровня;

3) сохранение механических, функциональных параметров физической связи в компьютерной сети;

4) управление аппаратурой передачи данных и каналов связи.

Вопрос № 3 (один верный ответ).

Компьютер, подключенный к компьютерной сети, обязательно имеет …

Варианты ответов:

1) *IP*-адрес;

2) *web*-страницу;

3) домашнюю *web*-страницу;

4) *URL*-адрес.

Вопрос № 4 (один верный ответ).

Служба телеконференции в Интернете обеспечивает …

Варианты ответов:

1) прием и передачу файлов любого формата;

2) процесс создания, приема и передачи *web*-страниц;

3) рассылку электронной почты группе корреспондентов;

4) обмен письмами в глобальных сетях.

Вопрос № 5 (несколько верных ответов).

Сетевыми стратегиями доступа от одного компьютера локальной вычислительной сети к другому являются ...

Варианты ответов:

1) маркерный метод доступа;

2) конкурентный метод доступа;

3) метод резервирования времени;

4) иерархический метод доступа;

5) ступенчатый метод доступа.

Библиографический список

1. ГОСТ 29099-91. Сети вычислительные локальные. Термины и определения. М.: Комитет стандартизации и метрологии СССР, 1991. 18 с.

2. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М.: Стандартинформ, 2009. 16 с.

3. Грошев А. С. Информатика: Учебник / А. С. Грошев / Архангельский гос. техн. ун-т. Архангельск, 2010. 470 с.

4. Кудинов Ю. И. Основы современной информатики: Учебное пособие / Ю. И. Кудинов, Ф. Ф. Пащенко. СПб: Лань, 2011. 256 с.

5. Макарова Н. В. Информатика: Учебник / Н. В. Макарова, В. Б. Волков. СПб: Питер, 2011. 576 с.

6. Трофимов В. В. Информатика: Учебник / В. В. Трофимов. М.: Юрайт, 2011. 911 с.

Учебное издание

ТРОФИМОВА Людмила Николаевна,
КАЛИНИНА Екатерина Сергеевна,
ДОЛГОВА Анна Владимировна

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ И ЗАЩИТЕ ИНФОРМАЦИИ

Учебно-методическое пособие

Редактор Н. А. Майорова

***

Подписано в печать 19.09.2016. Формат 60 × 84 $^{1}/_{16}$.
Офсетная печать. Бумага офсетная. Усл. печ. л. 2,8. Уч.-изд. л. 3,0.
Тираж 430 экз. Заказ .

**

Редакционно-издательский отдел ОмГУПСа
Типография ОмГУПСа

*

644046, г. Омск, пр. Маркса, 35