П. М. БУЙ

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Гомель 2021

МИНИСТЕРСТВО ТРАНСПОРТА И КОММУНИКАЦИЙ
РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра автоматики, телемеханики и связи

П. М. БУЙ

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Рекомендовано учебно-методическим объединением по образованию в области транспорта и транспортной деятельности для обучающихся по специальностям 1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте», 1-37 80 01 «Транспорт» в качестве учебно-методического пособия по учебной дисциплине «Основы сетевых технологий и защиты информации»

Гомель 2021

УДК 656.254:621.372.8(075.8)
ББК 39.278
Б90

Рецензенты: кафедра защиты информации Белорусского государственного университета информатики и радиоэлектроники (заведующий кафедрой – д-р техн. наук, профессор *Т. В. Борботько*);
заместитель начальника по связи *А. В. Карпов* (Гомельская дистанция сигнализации и связи (ШЧ-9) Белорусской железной дороги).

Буй, П. М.

Б90 Защита информации в компьютерных системах и сетях железнодорожного транспорта : учеб.-метод. пособие / П. М. Буй ; М-во трансп. и коммуникаций Респ. Беларусь, Белорус. гос. ун-т трансп. – Гомель : БелГУТ, 2021. – 187 с.
ISBN 978-985-891-055-6

Изложены основы сетевых технологий и вопросы защиты информации в компьютерных системах и сетях железнодорожного транспорта. Рассмотрены вопросы организации компьютерных сетей, принципы адресации, коммутации и маршрутизации, уровни модели OSI и основные протоколы. Приведены основные методы и средства защиты информации на различных уровнях модели OSI, особое внимание уделено методам криптографической защиты информации, средствам аутентификации, технологиям разграничения доступа и вопросам сетевой безопасности. Даны рекомендации по безопасному использованию современных информационных технологий. Рассмотрены положения Концепции информационной безопасности Республики Беларусь.

Предназначено для студентов специальностей 1-37 02 04 «Автоматика, телемеханика и связь на железнодорожном транспорте» и 1-37 80 01 «Транспорт».

УДК 656.254:621.372.8(075.8)
ББК 39.278

ISBN 978-985-891-055-6

ВВЕДЕНИЕ

Белорусская железная дорога призвана обеспечивать потребности государства, юридических и физических лиц в железнодорожных перевозках, а также работах и услугах, оказываемых железнодорожным транспортом. В связи с этим железнодорожный комплекс Республики Беларусь имеет особое стратегическое значение, являясь связующим звеном единой экономической системы и обеспечивая стабильную деятельность промышленных предприятий. Кроме того, это еще и самый доступный вид транспорта для граждан Республики Беларусь.

В последнее время, в рамках стремительной информатизации и компьютеризации на Белорусской железной дороге вводятся в эксплуатацию современные компьютерные системы и сети, которые обеспечивают сбор, хранение, обработку, распределение, передачу и прием информации в ходе выполнения различных технологических процессов. Довольно часто такие системы могут использоваться не только для передачи и обработки информации, но и для организации автоматизированных систем управления технологическими процессами (АСУ ТП).

Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности Республики Беларусь 18 марта 2019 года № 1 «О Концепции информационной безопасности Республики Беларусь», указывает на то, что повсеместное функционирование объектов транспорта с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности.

Вместе с тем процессы информатизации и компьютеризации, а также использование современных сетевых технологий при организации управления на Белорусской железной дороге таят в себе множество потенциальных опасностей, область реализации которых касается исключительно сферы высоких технологий.

Безопасность компьютерных систем и сетей железнодорожного транспорта – это их защищенность от случайного или преднамеренного вмешательства в штатный процесс их функционирования. При отсутствии адекватных методов и надежных средств защиты угрозы такого рода могут привести к нарушению штатной работы систем управления и, как следствие, ухудшению уровня безопасности движения поездов. Поэтому обязательным является проведение анализа угроз, характерных как для самих компьютерных систем и сетей, так и для среды их функционирования.

1 ОСНОВНЫЕ ПОНЯТИЯ И ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Спектр вопросов, которые рассматриваются в контексте защиты информации, настолько широк, что затрагивает многие отрасли и имеет отдельные направления для ряда из них, например, защита банковских операций, обеспечение безопасного электронного документооборота, обеспечение информационной безопасности критически важных объектов информатизации, защита информации в компьютерных сетях и пр. В связи с этим неизбежно появляется множество терминов и их определений, знание которых помогает лучше понять научную и техническую документацию по соответствующим направлениям.

Базовые термины и их определения в сфере защиты информации, которые касаются всех направлений представлены в следующих официальных документах:

– Государственный стандарт Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения» (по состоянию на 1 февраля 2021 г.);

– Закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации» (по состоянию на 1 июля 2017 г.);

– Концепция информационной безопасности Республики Беларусь (по состоянию на 18 марта 2019 г.).

1.1 Основные термины и их определения

Согласно государственному стандарту Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения» установлены следующие основные термины и их определения в области защиты информации (приведены некоторые из них).

Защита информации (ЗИ) – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и преднамеренных воздействий на защищаемую информацию.

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами

(государство, юридическое лицо, группа физических лиц, отдельное физическое лицо).

Защита информации от несанкционированного воздействия (ЗИ от НСВ) – защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия – защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа (ЗИ от НСД) – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами (государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо) с нарушением установленных нормативными правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Защита информации от [иностранной] разведки – защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

Замысел защиты информации – основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Цель защиты информации – заранее намеченный результат защиты информации. Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которым руководствуется организация в своей деятельности.

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

Объект защиты информации – информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (государство, юридическое лицо, группа физических лиц или отдельное физическое лицо).

Техника защиты информации – средства защиты информации, в том числе физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Эффективность защиты информации – степень соответствия результатов защиты информации цели защиты информации.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

Прочие понятия, приведенные в государственном стандарте Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения», будут приводиться по мере необходимости в соответствующих разделах.

В законе «Об информации, информатизации и защите информации» применяются следующие основные термины и их определения, которые непосредственно касаются информационных технологий и сетей (ниже приведены некоторые из них).

База данных – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях.

Владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями в пределах и порядке, определенных их собственником в соответствии с законодательством Республики Беларусь.

Документированная информация – информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать.

Доступ к информации – возможность получения информации и пользования ею.

Доступ к информационной системе и (или) информационной сети – возможность использования информационной системы и (или) информационной сети.

Информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи.

Информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Комплекс программно-технических средств – совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий.

Конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь.

Обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору.

Персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными

актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо.

Пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею.

Пользователь информационной системы и (или) информационной сети – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими.

В Концепции информационной безопасности Республики Беларусь приведены следующие основные термины и их определения (ниже приведены некоторые из них).

Воздействие на информацию – действие по изменению формы предоставления и (или) содержания информации.

Государственная информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств, формируемая или приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц.

Государственный информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах, формируемая или приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц.

Деструктивное информационное воздействие – осуществление информационного влияния на политические и социально-экономические процессы, деятельность государственных органов, а также на физических и юридических лиц в целях ослабления обороноспособности государства, нарушения общественной безопасности, принятия и заключения заведомо невыгодных решений и международных договоров, ухудшения отношений с другими государствами, создания социально-политической напряженности, формирования угрозы возникновения чрезвычайных ситуаций, разрушения традиционных духовных и нравственных ценностей, создания препятствий для нормальной деятельности государственных органов, причинения иного ущерба национальной безопасности.

Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Информационная инфраструктура – совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации.

Информационный суверенитет Республики Беларусь – неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность.

Информационная сфера – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Информационное пространство – область деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание и собственно информацию.

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности.

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка.

Киберустойчивость – способность информационной системы предвидеть изменения обстановки и своевременно адаптироваться к ним в целях успешного предотвращения негативных последствий или быстрого восстановления после киберинцидента.

Международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

Обеспечение информационной безопасности – система мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз.

Преступления в информационной сфере – предусмотренные Уголовным кодексом Республики Беларусь преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети.

Суверенитет данных – подчиненность отношений по поводу информации в цифровой форме, возникающих на территории Беларуси, национальной юрисдикции Республики Беларусь.

Встречаются случаи, когда одни и те же термины имеют разные определения в разных нормативных документах. Примером этого может служить термин «Защита информации». Определение данного термина, приведенное в государственном стандарте Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения», совершенно не противоречит определению этого же термина из Концепции информационной безопасности Республики Беларусь (в законе «Об информации, информатизации и защите информации» этому термину дано аналогичное определение). В Концепции информационной безопасности Республики Беларусь в определении указано за счет чего обеспечивается защита информации, а в государственном стандарте Республики Беларусь 50922-2006 дано определение «от противного», т. е. через перечень угроз, которые могут нарушить конфиденциальность, целостность, подлинность, доступность и сохранность информации.

1.2 Особенности информации как объекта защиты

Информация как объект защиты обладает рядом особенностей:

– информация не является материальным объектом;

– информация копируется с помощью материального носителя, т. е. является перемещаемой;

– информация является отчуждаемой от собственника.

Комплекс проблем, связанных с защитой информации, не исчерпывается обеспечением ее конфиденциальности, целостности, подлинности, доступности и сохранности. Он также должен рассматривать защиту прав на нее. Таким образом, информация может рассматриваться как объект права собственности.

Право собственности на информацию включает правомочия собственника, к которым относятся:

– право распоряжения;

– право владения;

– право пользования.

Правовое обеспечение защиты информации включает:

– правовые нормы, методы и средства защиты охраняемой информации в Республике Беларусь;

– правовые основы выявления и предупреждения утечки охраняемой информации;

– правовое регулирование организации и проведения административного расследования по фактам нарушения порядка защиты информации.

Документы, регламентирующие информацию в качестве объекта права:

– Гражданский кодекс Республики Беларусь (раздел V (Интеллектуальная собственность));

– Закон Республики Беларусь № 455-З «Об информации, информатизации и защите информации»;

– Закон Республики Беларусь № 170-З «О государственных секретах».

1.3 Виды информации

В соответствии с законом «Об информации, информатизации и защите информации» в зависимости от категории доступа информация делится на следующие виды (статьи 15–17):

– общедоступная информация;

– информация, распространение и (или) предоставление которой ограничено.

К общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены.

Не могут быть ограничены доступ к информации, распространение и (или) предоставление информации:

– о правах, свободах, законных интересах и обязанностях физических лиц, правах, законных интересах и обязанностях юридических лиц и о порядке реализации прав, свобод и законных интересов, исполнения обязанностей;

– деятельности государственных органов, общественных объединений;

– правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

– социально-экономическом развитии Республики Беларусь и ее административно-территориальных единиц;

– чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

– состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;

– состоянии преступности, а также о фактах нарушения законности;

– льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;

– размерах золотого запаса;

– обобщенных показателях по внешней задолженности;

– состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;

– накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

К информации, распространение и (или) предоставление которой ограничено, относится:

– информация о частной жизни физического лица и персональные данные;

– сведения, составляющие государственные секреты;

– служебная информация ограниченного распространения;

– информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;

– информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

– иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

1.4 Модели информационной безопасности

Понятие информационной безопасности, взятое из Концепции информационной безопасности Республики Беларусь и попавшее туда из Концепции национальной безопасности Республики Беларусь не раскрывает состав этого понятия. Используя определение термина «Защита информации», которое указано выше, можно утверждать, что информация, находящаяся в безопасном состоянии, сохраняет свойства конфиденциальности, целостности, подлинности, доступности и сохранности. Набор свойств, которыми должна обладать информация, находящаяся в безопасном состоянии, характеризуется используемой моделью информационной безопасности.

Одной из первых и наиболее используемой моделью информационной безопасности является **модель КЦД**, предложенная в 1975 году Джерри Зальцером и Майклом Шрёдером. Эта модель предполагает, что все возможные нарушения информационной безопасности всегда могут быть отнесены по меньшей мере к одной из трех групп: нарушения конфиденциальности, целостности или доступности (рисунок 1.1). Информационная система находится в состоянии безопасности, если она защищена от нарушений конфиденциальности, целостности и доступности, где:

– **конфиденциальность** – состояние информационной системы, при котором информационные ресурсы доступны только тем пользователям, которым этот доступ разрешен;

– **целостность** – состояние информационной системы, при котором информация, которая в ней хранится и ею обрабатывается, а также процедуры обработки информации не могут быть изменены, удалены или дополнены неавторизованным образом;

– **доступность** – состояние информационной системы, при котором услуги, которые ею оказываются, могут гарантированно и с приемлемой задержкой быть предоставлены пользователям, имеющим на это право.

Одной из наиболее популярных альтернатив триаде КЦД является **гексада Паркера** (рисунок 1.2).

Рисунок 1.1 – Триада КЦД

Рисунок 1.2 – Гексада Паркера

В гексаде Паркера определено шесть базовых видов нарушений, в состав которых, помимо нарушений конфиденциальности, доступности и целостности, входят еще три вида нарушений:

– **аутентичность** – это состояние информационной системы, при котором пользователь не может выдать себя за другого, а документ всегда имеет достоверную информацию о его источнике (авторе);

– **владение** – это состояние информационной системы, при котором физический контроль над устройством или другой средой хранения информации предоставляется только тем, кто имеет на это право;

– **полезность** – это такое состояние информационной системы, при котором обеспечивается удобство практического использования как собственно информации, так и связанных с ее обработкой и поддержкой процедур.

Еще одна модель информационной безопасности – **модель STRIDE** – альтернатива триаде КДЦ и гексаде Паркера. Она используется компанией Microsoft для разработки безопасного программного обеспечения. В соответствии с этой моделью информационная система находится в безопасности, если она защищена от следующих видов нарушений информационной безопасности:

– Spuffing – подмена данных – это такое нарушение, при котором пользователь информационной системы путем подмены данных успешно выдает себя за другого, получая таким образом возможность нанесения вреда;

– Tampering – изменение данных (нарушение целостности);

– Repudiation – отказ в ответственности – заключается в том, что пользователь отказывается от совершенных им ранее действий;

– Information Disclosure – разглашение сведений (нарушение конфиденциальности);

– Denial of Service – отказ в обслуживании (нарушение доступности);

– Elevation of Privilege – захват привилегий – заключается в том, что пользователь или другой субъект информационной системы несанкционированным образом повышает свои полномочия в системе.

Контрольные вопросы

1 В каких официальных документах Республики Беларусь представлены базовые термины и их определения в сфере защиты информации?

2 Дайте понятие защиты информации.

3 Дайте понятие защиты информации от несанкционированного доступа.

4 Что такое система защиты информации?

5 Что понимается под безопасностью информации?

6 Что такое средство защиты информации?

7 Дайте понятие информационной системы.

8 Дайте понятие кибератаки.

9 Что такое информационное пространство?

10 Каковы основные особенности информации как объекта защиты?

11 На какие виды в зависимости от категории доступа делится информация в соответствии с законом «Об информации, информатизации и защите информации»?

12 Что такое конфиденциальность, целостность и доступность информации?

13 Какие требования по безопасности составляют Гексаду Паркера?

2 ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

2.1 Эволюция сетей

Компьютерные сети являются логическим результатом эволюции двух важнейших научно-технических отраслей – компьютерных и телекоммуникационных технологий.

В настоящее время большинство сетевых устройств (оконечное оборудование данных – **Data Terminal Equipment**, **DTE**) как на железнодорожном транспорте, так и во многих других отраслях представляют собой современные компьютеры, которые согласованно решают набор взаимосвязанных задач, обмениваясь данными в автоматическом режиме. Такой обмен данными может осуществляться на значительных расстояниях, что характерно для железнодорожного транспорта в рамках автоматизации управления. При этом применяются технологии и средства телекоммуникационных сетей. В данном пособии для обозначения DTE компьютерных сетей будут использоваться понятия сетевое устройство и компьютер.

Первые компьютеры 1950-х годов – это большие, громоздкие (могли полностью занимать помещение или даже здание) и дорогие устройства. Они не были предназначены для интерактивной работы пользователя, а применялись в режиме пакетной обработки, т. е. строились на базе майнфрейма – мощного и надежного компьютера универсального назначения. Пользователи подготавливали перфокарты, содержащие данные и команды программ, и передавали их в вычислительный центр.

По мере удешевления процессоров в начале 60-х годов появились новые способы организации вычислительного процесса, которые позволили учесть интересы пользователей. В это время начали развиваться интерактивные системы, в которых каждый пользователь получал собственное устройство (терминал), с помощью которого он мог вести диалог с компьютером. Количество одновременно работающих с компьютером пользователей определялось его мощностью. Взаимодействие пользователей с майнфреймом разделялось по времени. Такие системы стали прообразом локальных вычислительных сетей, хотя исторически первыми появились глобальные сети. Это связано с тем, что высокая стоимость компьютеров не позволяла иметь их настолько много, чтобы была необходимость организовывать локальную сеть. Но это не отменяло необходимости связывать между собой

майнфреймы, расположенные на значительном расстоянии друг от друга, что и послужило началом организации **глобальных сетей** (**Wide Area Network**, **WAN**) – сетей, объединяющих территориально рассредоточенные компьютеры, находящихся в различных городах и странах.

Эволюция началась с решения задачи доступа к компьютеру с терминалов, удаленных от него на многие сотни или тысячи километров. Терминалы соединялись с компьютерами при помощи модемов через существующую и имеющую достаточное распространение телефонную сеть. Следующим этапом появились системы, в которых были реализованы удаленные связи между компьютерами. На основе механизма связи между компьютерами по телефонным сетям были реализованы службы обмена файлами, синхронизации баз данных, электронной почты и другие сетевые службы.

До этого в течение многих лет глобальные сети строились на основе телефонных каналов тональной частоты. Такие каналы обладают низкой скоростью передачи дискретной информации и вносят значительные искажения в передаваемые сигналы. Поэтому протоколы глобальных сетей, построенных с использованием каналов связи низкого качества, отличались сложными процедурами контроля и восстановления данных.

Глобальные компьютерные сети очень многое унаследовали от более старых глобальных телефонных сетей, работа которых была организована по принципу коммутации каналов. Однако первые глобальные компьютерные сети отказались от этого принципа. Пульсирующий и в значительной степени не чувствительный к задержкам компьютерный трафик гораздо эффективнее передается сетями, работающими по принципу коммутации пакетов, когда данные разделяются на небольшие порции – пакеты, которые самостоятельно перемещаются по сети благодаря наличию адреса конечного узла в заголовке пакета.

В 1969 году Министерство обороны США инициировало работы по объединению в единую сеть майнфреймов оборонных и научно-исследовательских центров. Эта сеть, получившая название **ARPANET**, стала отправной точкой для создания первой и самой известной ныне глобальной сети – **Интернет**.

Сеть ARPANET объединяла компьютеры разных типов, работавших под управлением различных операционных систем (ОС) с дополнительными модулями, реализующими общие для всех коммуникационные протоколы. ОС этих компьютеров можно считать первыми сетевыми операционными системами. Сетевые ОС позволили не только рассредоточить пользователей между несколькими компьютерами (как в многотерминальных системах), но и организовать распределенное хранение и обработку данных.

В начале 70-х годов в результате технологического прорыва в области производства компьютерных компонентов появились **большие интегральные схемы** (**БИС**). Их невысокая стоимость и хорошие функциональные возможности привели к созданию мини-компьютеров, которые стали конкурентами майнфреймов. В таких условиях организации получили возможность иметь собственные компьютеры, территориально распределенные по предприятию и решающие отдельные задачи. Возникла необходимость в автоматическом режиме обмениваться компьютерными данными между пользователями различных подразделений. Эта потребность привела к появлению первых локальных вычислительных сетей.

Локальные сети (**Local Area Network**, **LAN**) – это объединения компьютеров, сосредоточенных на небольшой территории. Обычно локальная сеть принадлежит одной организации.

Мощным стимулом для их появления послужили персональные компьютеры. Эти массовые продукты стали идеальными элементами построения сетей – с одной стороны, они были достаточно мощными, чтобы обеспечивать работу сетевого программного обеспечения, а с другой – нуждались в объединении своей вычислительной мощности для решения сложных задач, а также разделения дорогих периферийных устройств. Персональные компьютеры стали преобладать в локальных сетях, причем не только в качестве клиентских компьютеров, но и в качестве сетевых серверов.

Первоначально для соединения компьютеров друг с другом использовались нестандартные сетевые технологии. **Сетевая технология** – это согласованный набор программных и аппаратных средств, а также механизмов передачи данных по линиям связи, достаточный для построения вычислительной сети. К середине 80-х годов утвердились стандартные сетевые технологии объединения компьютеров в сеть – Ethernet, Arcnet, Token Ring, Token Bus, FDDI и т. п.

Все стандартные технологии локальных сетей опирались на тот же принцип коммутации, который был с успехом опробован и доказал свои преимущества при передаче трафика данных в глобальных компьютерных сетях, – принцип коммутации пакетов.

В конце XX века выявился явный лидер среди технологий локальных сетей – это семейство технологий **Ethernet**, в которое вошли:

– Ethernet со скоростью передачи 10 Мбит/с;

– Fast Ethernet со скоростью 100 Мбит/с;

– Gigabit Ethernet со скоростью 1000 Мбит/с.

В конце 80-х годов отличия между локальными и глобальными сетями проявлялись весьма отчетливо (протяженность и качество линий связи, сложность методов передачи данных, скорость обмена данными, разнообразие услуг). Затем постепенно различия между ними стали сглаживаться.

Изолированные ранее локальные сети начали объединять друг с другом, при этом в качестве связующей среды использовались глобальные сети. Интеграция локальных и глобальных сетей привела к значительному взаимопроникновению соответствующих технологий.

Сближение в методах передачи данных локальных и глобальных сетей произошло за счет использования одной и той же новой среды передачи данных (оптического волокна) и принципов цифрового кодирования. Волоконно-оптические кабели стали использоваться практически во всех технологиях локальных сетей для высокоскоростного обмена информацией на расстояниях свыше 100 метров, на них же стали строиться магистрали первичных сетей **синхронной цифровой иерархии** (**Synchronous Digital Hierarchy**, **SDH**), **уплотненного волнового мультиплексирования** (**Dense Wave Division Multiplexing**, **DWDM**), а в последствии и **оптических транспортных сетей** (**Optical Transport Network**, **OTN**), предоставляющих свои цифровые каналы для объединения оборудования глобальных компьютерных сетей.

Еще одним признаком сближения локальных и глобальных сетей является появление сетей, занимающих промежуточное положение между локальными и глобальными сетями. **Городские сети** или сети мегаполисов (**Metropolitan Area Network**, **MAN**) предназначены для обслуживания территории крупного города.

Высокое качество цифровых каналов (за счет использования оптических волокон) изменило требования к протоколам глобальных компьютерных сетей. На первый план вместо процедур обеспечения надежности вышли процедуры обеспечения гарантированной средней скорости доставки информации пользователям, а также механизмы приоритетной обработки пакетов особенно чувствительного к задержкам трафика (голосовой трафик).

Большой вклад в сближение локальных и глобальных сетей внесло доминирование протокола IP, который может работать поверх любых технологий локальных и глобальных сетей, объединяя различные подсети в единую составную сеть.

Стало наблюдаться сближение видов услуг, предоставляемых клиентам, а также технологическое сближение сетей, которое происходит на основе цифровой передачи информации различного типа, метода коммутации пакетов и программирования услуг.

Прорывом в процессе конвергенции сетей явилось появление смартфонов – устройств, которые объединили в себе функции мобильных телефонов и персональных компьютеров. Для поддержки таких новых функций телефона мобильная телефонная сеть стала мультисервисной сетью, т. е. она начала предоставлять полный набор как телефонных, так и компьютеризованных информационных услуг (просмотр веб-страниц в такой же удобной форме, как и на экране компьютера, услуги электронной почты и видеоконференций, просмотр фильмов, публикация информации в социальных сетях и т. п.).

Появился новый термин – **инфокоммуникационная сеть,** который прямо говорит о двух составляющих современной сети – информационной (компьютерной) и телекоммуникационной. Такая сеть не может быть создана в результате «победы» какой-нибудь одной технологии или одного подхода. Ее может породить только процесс конвергенции, когда от каждой технологии берется все самое лучшее.

Хронология важнейших событий на пути становления современных глобальных и локальных компьютерных сетей приведена в таблице 2.1.

Таблица 2.1 – **Хронология важнейших событий на пути становления современных глобальных и локальных компьютерных сетей**

Этап	Период времени
Первые глобальные связи компьютеров, первые эксперименты с пакетными сетями	Конец 60-х
Начало передач по телефонным сетям голоса в цифровой форме	Конец 60-х
Появление больших интегральных схем, первые мини-компьютеры, первые нестандартные локальные сети	Начало 70-х
Стандартизация технологии X.25 для построения сети «удаленные терминалы–майнфрейм»	1974
Появление персональных компьютеров, создание Интернета в современном виде, установка на всех узлах стека протоколов TCP/IP	Начало 80-х
Появление стандартных технологий локальных сетей (Ethernet – 1980 г., Token Ring, FDDI – 1985 г.)	Середина 80-х
Начало коммерческого использования Интернета	Конец 80-х
Появление первичных сетей SDH со скоростью передачи до 155 Мбит/с	Конец 80-х
Изобретение Web-технологии	1991
Доминирование Ethernet в локальных сетях, стандартизация Gigabit Ethernet	Конец 90-х
Появление технологии плотного мультиплексирования волн (DWDM) с возможностью передачи 40/80 волн в одном волокне	Конец 90-х
Появление первых смартфонов с ограниченными интернет-функциями	Конец 90-х
Интернет становится мультимедийным (появляется IP-TV и IP-телефония)	Конец 90-х – начало 2000-х
Повышение скорости передачи данных до 10 Гбит/с (10G Ethernet и 10G SDH/OTN)	Начало 2000-х
Смартфоны становятся полнофункциональными интернет-устройствами	Середина 2000-х
Повышение скорости передачи до 100 Гбит/с (100G Ethernet и 100G OTN)	Начало 2010-х

2.2 Интернет как основной фактор развития сетевых технологий

В настоящее время сеть Интернет является вершиной эволюции телекоммуникационных сетей, самой быстрорастущей технической системой в истории человечества. Интернет растет и качественно развивается постоянно, начиная с 80-х годов, и в соответствии с прогнозами специалистов этот процесс будет продолжаться.

Количественно Интернет оценивается количеством подключенных к нему сетевых устройств, количеством пользователей, объемом передаваемого трафика за определенный интервал времени.

На рисунке 2.1 представлена динамика роста количества пользователей сети Интернет в мире и для сравнения с ней – динамика роста населения Земли.

На рисунке 2.2 представлена динамика роста количества сетевых устройств, выполняющих функции серверов (без учета пользовательских устройств). С учетом пользовательских устройств (настольных компьютеров, ноутбуков, планшетов и мобильных телефонов) общее количество сетевых устройств, подключенных к Интернету, составило в 2018 году около 23 миллиардов.

На рисунке 2.3 представлена динамика роста объема трафика, передаваемого по магистралям сети Интернет за месяц.

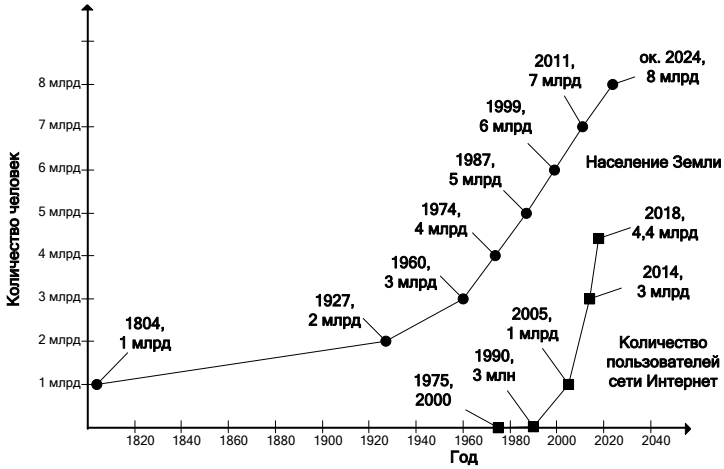

Рисунок 2.1 – Динамика роста количества пользователей сети Интернет в мире

Интернет не «рос» бы так быстро, если бы он не изменялся качественно и оставался все это время только средством передачи файлов и обмена текстовыми сообщениями электронной почты, как это было в 80-х годах.

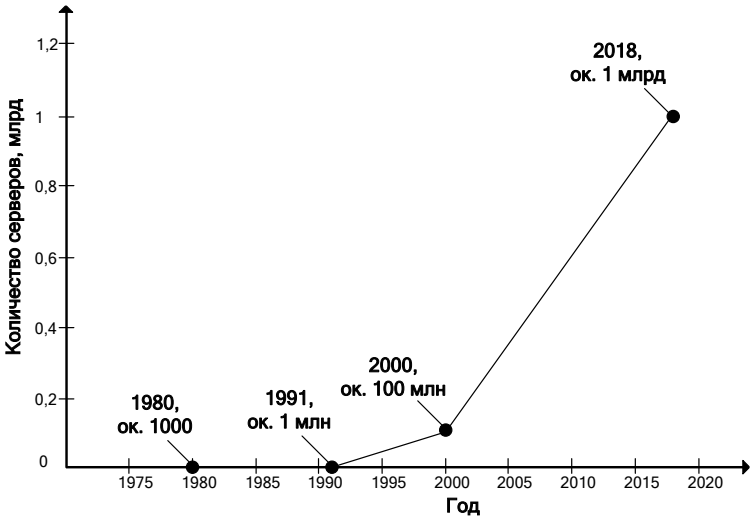

Рисунок 2.2 – Динамика роста роста сетевых устройств,
выполняющих функции серверов

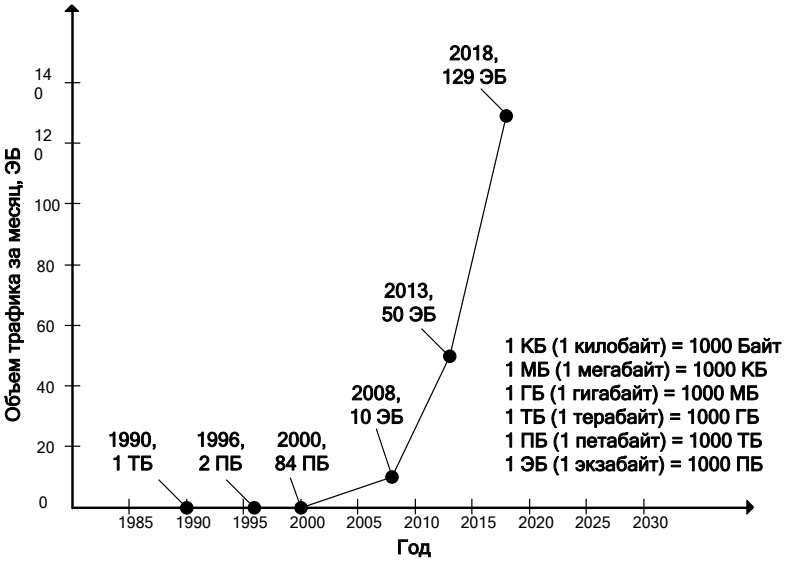

Рисунок 2.3 – Динамика роста объема трафика,
передаваемого по магистралям сети Интернет за месяц

Новые сервисы и новые типы сетевых устройств продолжают делать Интернет привлекательным для все большего числа массовых пользователей. В настоящее время все большее распространение получают не только планшеты и смартфоны, но и встроенные компьютеры, которые работают внутри привычных систем и устройств. Такие компьютеры сами инициируют обмен данными между собой или со своими удаленными центрами управления через Интернет, являясь, по сути, его пользователями. Этот новый класс пользователей породил и новый термин – **интернет вещей** (**Internet of Things**, **IoT**), подчеркивающий отличие от традиционной сети Интернет, в которой преобладают пользователи-люди.

На рисунке 2.4 представлена динамика изменения доли трафика, генерируемого мобильными устройствами и встроенными компьютерами.

Рисунок 2.4 – Динамика изменения доли трафика, генерируемого мобильными устройствами и встроенными компьютерами

Если в 90-е годы и начале 2000-х в общем объеме преобладал трафик приложений, передающих файлы, то уже к 2010 году он уступил лидерство трафику приложений, передающих видеопотоки в реальном масштабе времени.

Новой вехой на пути развития Интернета стали облачные вычисления, которые позволяют разгрузить пользовательский компьютер и перенести

хранение данных и выполнение приложений на некоторые удаленные компьютеры, связанные с пользовательским компьютером через сеть. Облачные вычисления стали еще одной причиной увеличения трафика Интернета, так как пользователи этого сервиса постоянно обращаются к внешним серверам провайдера, вместо того, чтобы производить вычисления и другие манипуляции с данными локально, на своих персональных компьютерах или на корпоративных серверах.

Феноменальный рост и изменчивость Интернета (в различных аспектах) оказывали и оказывают сильнейшее влияние на технологии компьютерных сетей, заставляя их постоянно изменяться и совершенствоваться, приспосабливаясь к новым требованиям пользователей и их количеству.

2.3 Стандартизация Интернет

Основная задача сети связи – это соединение разнообразного оборудования для решения общих для этого оборудования задач. В связи с этим проблема совместимости оборудования является одной из первостепенных задач. Без согласования всеми производителями общепринятых стандартов развивать сетевые технологии было бы значительно сложнее и такой рост глобальной сети Интернет, который был проиллюстрирован в предыдущем разделе, был бы невозможен. Поэтому любая новая технология только тогда приобретает узаконенный статус и становится общедоступна, когда ее содержание закрепляется в соответствующем стандарте.

В компьютерных сетях идеологической основой стандартизации является модель взаимодействия открытых систем. Открытой может быть названа любая система (компьютер, вычислительная сеть, компьютерная программа и т. п.), которая построена в соответствии с открытыми спецификациями.

Под **открытыми спецификациями** понимаются опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами.

Использование открытых спецификаций при организации сетей позволяет впоследствии создавать для них различные средства расширения и модификации.

Если две сети построены с соблюдением принципов открытости, то это дает следующие преимущества:

– возможность построения сети из аппаратных и программных средств различных производителей, придерживающихся одинаковых стандартов;

– безболезненная замена отдельных компонентов сети другими, более совершенными;

– легкость сопряжения сетей между собой.

Интернет является одним из самых наглядных примеров открытой системы. Эта международная сеть развивалась в полном соответствии с требованиями, предъявляемыми к открытым системам. В разработке ее стандартов принимали участие пользователи из различных университетов, научных организаций и фирм – производителей вычислительной аппаратуры и программного обеспечения.

Стандарты, определяющие работу Интернета, имеют название «**Темы для обсуждения**» (**Request For Comments**, **RFC**). Использование открытого подхода в стандартизации позволило сети Интернет объединить в себе разнообразное оборудование и программное обеспечение огромного числа сетей, разбросанных по всему миру. Ввиду постоянно растущей популярности Интернета RFC-документы становятся международными стандартами де-факто, многие из которых затем приобретают статус официальных международных стандартов в результате их утверждения какой-либо организацией по стандартизации, например, **Международной организацией по стандартизации (International Organization for Standartization**, **ISO**) или **Международным союзом телекоммуникаций (International Telecommunications Union**, **ITU**).

В соответствии с принципом открытости Интернета все RFC-документы находятся в свободном доступе. Список RFC-документов можно найти в сети Интернет, например, на сайте www.rfc-editor.org.

Основным организационным подразделением, отвечающим за развитие и стандартизацию архитектуры и протоколов Интернета является **Научно-административное сообщество Интернета** (**Internet Society**, **ISOC**). Под управлением ISOC работает **совет по архитектуре Интернета** (**Internet Architecture Board**, **IAB**). В IAB входят две основные группы:

– **Internet Research Task Force** (**IRTF**) – координирует долгосрочные исследовательские проекты по протоколам TCP/IP;

– **Internet Engineering Task Force** (**IETF**) – занимается решением текущих технических проблем Интернета. Именно она определяет спецификации, которые затем становятся стандартами Интернета.

2.4 Модель OSI

Организация сети для взаимодействия различных сетевых устройств – это достаточно сложная задача. Решение такой задачи проще всего произвести за счет разбиения ее на несколько более простых задач-модулей. При этом необходимо однозначно определить функции каждого модуля, а также порядок их взаимодействия. Каждый модуль можно рассматривать как отдельный блок со стандартизированными функциями, а также входными и выходными форматами данным. В результате такого подхода появляется возможность независимого тестирования, разработки и модификации отдельных модулей.

После представления исходной задачи в виде множества модулей эти модули следует сгруппировать и упорядочить по уровням, образующим иерархию. В результате для каждого промежуточного уровня можно указать непосредственно примыкающие к нему соседние вышележащий и нижележащий уровни.

Межуровневый интерфейс, называемый также **интерфейсом услуг**, определяет набор функций, которые нижележащий уровень предоставляет вышележащему.

В процессе сетевого взаимодействия, когда участвуют как минимум две стороны, необходимо организовать согласованную работу двух иерархий. Для этого оба участника сетевого взаимодействия должны принять множество соглашений о параметрах и видах представления передаваемых данных. Такие соглашения, называемые **протоколами**, должны быть приняты на всех уровнях иерархии.

Термины «протокол» и «интерфейс» обозначают одно и то же – формализованное описание процедуры взаимодействия двух объектов, однако протоколы определяют правила взаимодействия модулей одного уровня в разных узлах, а интерфейсы – правила взаимодействия модулей соседних уровней в одном узле.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется **стеком протоколов**.

В начале 80-х годов ISO, ITU и некоторые другие международные организаций по стандартизации разработали **стандартную модель взаимодействия открытых систем** (**Open System Interconnection**, **OSI**). Эта модель сыграла значительную роль в развитии компьютерных сетей.

Модель OSI имеет дело со стеком протоколов для сетей с коммутацией пакетов. Модель OSI не содержит описаний реализаций конкретного набора протоколов, она определяет уровни взаимодействия, их стандартные названия и функции, которые они должны выполнять.

В модели OSI средства взаимодействия делятся на семь уровней: прикладной, представления, сеансовый, транспортный, сетевой, канальный и физический.

Именно поэтому модель OSI называют также семиуровневой моделью. Каждый уровень связан с вполне определенным аспектом взаимодействия сетевых устройств. На рисунке 2.5 представлена логическая структура модели OSI при взаимодействии двух приложений, работающих на разных компьютерах.

Приложения могут реализовывать собственные протоколы взаимодействия, используя для этих целей многоуровневую совокупность системных средств. Для этого в распоряжение программистов предоставляется **прикладной программный интерфейс** (**Application Program Interface**, **API**).

В соответствии с моделью OSI приложение может обращаться с запросами только к самому верхнему уровню – прикладному, однако на практике это далеко не так, например, программист напрямую может взаимодействовать с протоколами TCP или UDP транспортного уровня.

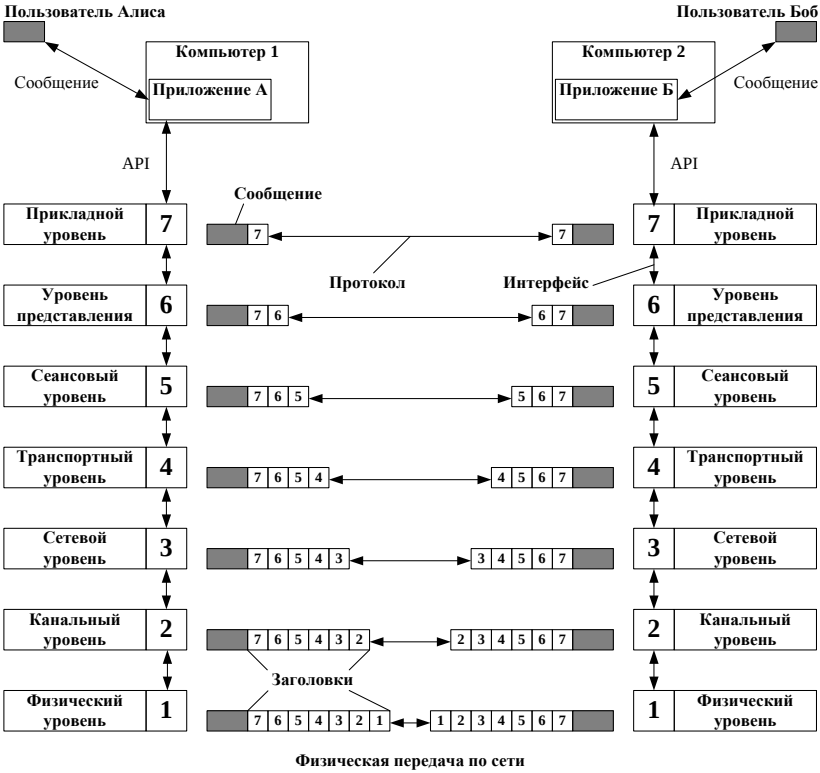

Рисунок 2.5 – Логическая структура модели OSI при взамидействии двух приложений

Физический уровень имеет дело с передачей потока битов по физическим каналам связи (витая пара, волоконно-оптический кабель, радиоканал). Функции физического уровня реализуются на всех устройствах, подключенных к сети, и выполняются сетевым адаптером, входным или выходным интерфейсами. Физический уровень не вникает в смысл информации, которую он передает, для него информация, поступающая от канального уровня, представляет собой однородный поток битов, которые нужно доставить без искажений, в соответствии с заданной тактовой частотой и выбранным способом кодирования.

Канальный уровень предлагает сетевому уровню следующие услуги:

– установление логического соединения между взаимодействующими узлами;

– согласование в рамках соединения скоростей передатчика и приемника информации;

– обеспечение надежной передачи, обнаружение и коррекцию ошибок.

В сетях, построенных на основе разделяемой среды, физический уровень выполняет еще одну функцию – проверяет доступность разделяемой среды.

Протоколы канального уровня обычно работают в пределах локальной сети и реализуются средствами сетевых адаптеров и их драйверов. **Протокольной единицей данных** (**Protocol Data Unit**, **PDU**) канального уровня является **кадр.**

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей и называемой составной сетью, или интернетом (не путать с Интернетом). Технология, позволяющая соединять в единую сеть множество сетей, в общем случае построенных на основе разных технологий, называется технологией межсетевого взаимодействия.

Чтобы связать между собой сети, построенные на основе отличающихся технологий, нужна группа различных по назначению протоколов, предоставляемая сетевым уровнем, и специальные устройства – маршрутизаторы, которые предназначены для физического соединения сетей. Маршрутизатор имеет несколько сетевых интерфейсов, к каждому из которых может быть подключена одна сеть.

Данные, которые необходимо передать через составную сеть, поступают на сетевой уровень от вышележащего транспортного уровня. Эти данные снабжаются заголовком сетевого уровня. Данные вместе с заголовком образуют **пакет** (PDU сетевого уровня).

В соответствии с многоуровневым подходом сетевой уровень для решения своей задачи обращается к канальному уровню. Весь путь через составную сеть разбивается на участки от одного маршрутизатора до другого, причем каждый участок соответствует пути через отдельную сеть.

Чтобы передать пакет через очередную сеть, сетевой уровень помещает его в поле данных кадра (PDU канального уровня) соответствующей канальной технологии. В заголовке кадра указывается адрес канального уровня интерфейса следующего маршрутизатора. Сеть, используя свою канальную технологию, доставляет кадр с инкапсулированным в него пакетом по заданному адресу. Затем маршрутизатор извлекает пакет из прибывшего кадра и после необходимой обработки передает пакет для дальнейшей транспортировки в следующую сеть, предварительно упаковав его в новый кадр канального уровня.

Транспортный уровень обеспечивает приложениям и верхним уровням передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов транспортного сервиса от низшего класса 0 до высшего класса 4. Эти виды сервиса отличаются качеством предоставляемых услуг и способностью к обнаружению и исправлению ошибок передачи. Выбор класса сервиса транспортного уровня определяется, с одной стороны, тем, в какой степени задача обеспечения надежности решается самими приложениями и протоколами более высоких, чем транспортный, уровней. С другой стороны, этот выбор зависит от того, насколько надежной является система транспортировки данных в сети, обеспечиваемая уровнями, расположенными ниже транспортного: сетевым, канальным и физическим.

Все протоколы, начиная от транспортного уровня и выше, реализуются программными средствами конечных узлов сети – компонентами их сетевых операционных систем. В зависимости от используемого протокола PDU транспортного уровня называется **сегментом** или **дейтаграммой.**

Сеансовый уровень управляет взаимодействием сторон: фиксирует, какая из сторон является активной в настоящий момент и предоставляет средства синхронизации сеанса. Эти средства позволяют в ходе длинных передач сохранять информацию о состоянии этих передач в виде контрольных точек, чтобы в случае отказа можно было вернуться назад к последней контрольной точке. На практике немногие приложения используют сеансовый уровень, который редко реализуется в виде отдельных протоколов. Функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Уровень представления обеспечивает представление передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов. На этом уровне могут выполняться шифрование и архивация данных, перекодирование информации в графическом, аудио- или видео-формате.

Прикладной уровень предоставляет услуги пользовательским приложениям: доступ к общим сетевым ресурсам (файлам, принтерам или вебстраницам) или распределенным сетевым сервисам (электронной почте, службам передачи сообщений, базам данных). Как правило, услуги прикладного уровня включают идентификацию и аутентификацию участников сетевого взаимодействия, проверку их доступности и полномочий, опреде-

ление требований к защищенности сеанса обмена. Для запросов к прикладному уровню используются системные вызовы операционной системы, образующие API.

На рисунке 2.6 показаны основные элементы компьютерной сети: компьютеры (хосты), концентраторы, коммутаторы и маршрутизаторы. Полный стек протоколов реализован только на хостах, а другим сетевым устройствам для продвижения пакетов достаточно функциональности нижних трех уровней.

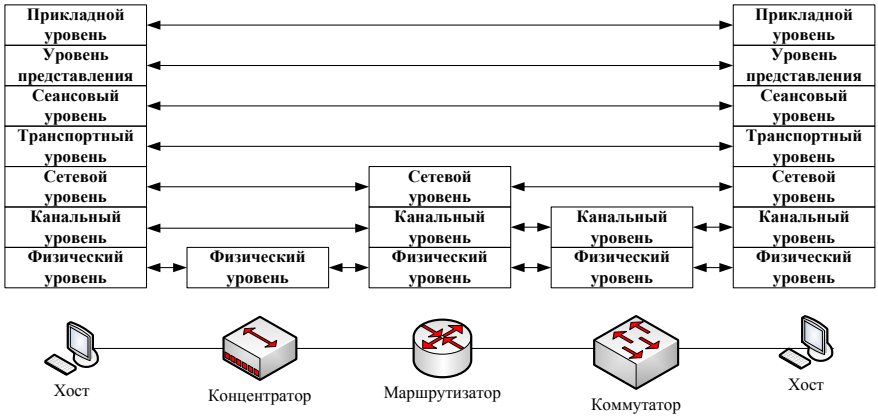

Рисунок 2.6 – Соответствие функций различных устройств сети уровням модели OSI

Концентраторам необходим только физический уровень модели OSI. Они повторяют электрические сигналы, поступающие на одни из их интерфейсов, на других своих интерфейсах.

Коммутаторы локальных сетей поддерживают протоколы двух нижних уровней, что дает им возможность работать в пределах стандартных топологий.

Маршрутизаторы должны поддерживать протоколы всех трех уровней. Сетевой уровень необходим им для объединения сетей различных технологий, а протоколы нижних уровней – для взаимодействия с конкретными сетями, образующими составную сеть.

Каждый из уровней модели OSI выполняет определенные функции. Часть функций, так называемые функции безопасности, касаются вопросов защиты информации, например, шифрование, обеспечение целостности данных, аутентификация субъектов, управление доступом и т. п. В таблице 2.2 представлено распределение функций безопасности по уровням модели OSI.

Таблица 2.2 – **Распределение функций безопасности по уровням модели OSI**

Функция безопасности	Уровни модели OSI						
	1	2	3	4	5	6	7
Аутентификация субъектов	–	–	+	+	–	–	+
Обеспечение доступности данных	–	–	–	–	+	–	+
Мониторинг целостности данных	–	+	+	+	+	–	+
Обеспечение целостности данных (возможность восстановления)	–	–	–	+	–	–	+
Управление доступом	–	+	+	+	+	–	+
Шифрование данных	+	–	+	–	–	+	+

2.5 Топология сети

Объединяя в сеть несколько сетевых устройств, необходимо решить, каким образом выбрать конфигурацию физических связей или их топологию. Под **топологией** сети понимается конфигурация графа, вершинам которого соответствуют конечные узлы сети и коммуникационное оборудование, а ребрам – физические или информационные связи между вершинами.

От выбора топологии связей существенно зависят характеристики сети. Если между двумя узлами имеется несколько путей, то это повышает **надежность сети** и делает возможным распределение загрузки между отдельными каналами. Так же важным является свойство **расширяемости сети** – способности простого присоединения новых узлов.

Полносвязная топология соответствует сети, в которой каждое сетевое устройство непосредственно связано со всеми остальными (рисунок 2.7, *а*). Несмотря на логическую простоту, этот вариант оказывается на практике громоздким и неэффективным. Экономические соображения часто приводят к выбору топологий, для которых характерна минимальная суммарная длина линий связи.

Ячеистая топология получается из полносвязной путем удаления некоторых связей (рисунок 2.7, *б*). Ячеистая топология допускает соединение большого количества сетевых устройств и характерна для крупных сетей.

В сетях с **кольцевой топологией** (рисунок 2.7, *в*) данные передаются по кольцу. Главным достоинством кольца является то, что оно по своей природе обеспечивает резервирование связей за счет наличия двух путей между любыми двумя сетевыми устройствами. Именно кольцевая топология применяется на железнодорожном транспорте при построении первичной волоконно-оптической сети связи. При этом организация колец должна осуществляться исходя из следующих принципов. Сетевые устройства располагаются на территории железнодорожных объектов, а линии связи между ними в основном прокладываются вдоль железных

дорог. В случае, когда железные дороги проходят параллельно, кольца организуются с использованием поперечных направлений или инфраструктуры других ведомственных сетей, например, на опорах линий электропередачи. На линейной сети связи, проложенной вдоль железной дороги, формируются **плоские кольца** – это кольца, в которых для замыкания используются оптические волокна внутри одного кабеля или нескольких кабелей, проложенных параллельно. Учитывая взаимное тяготение узлов, расположенных вдоль железнодорожных магистралей, плоские кольца целесообразно организовывать в пределах диспетчерского участка и отделения железной дороги. Выпуклые кольца большой протяженности организуются на дорожном и магистральном уровнях.

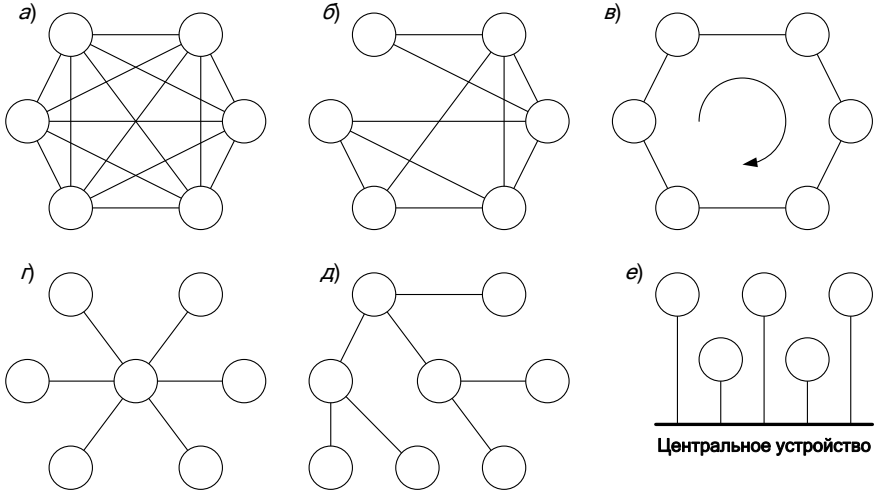

Рисунок 2.7 – Типовые сетевые топологии

Звездообразная топология (рисунок 2.7, *г*) образуется в случае, когда каждое сетевое устройство подключается непосредственно к общему центральному устройству, например, коммутатору или концентратору.

В функции центрального устройства входит направление передаваемой сетевыми устройствами информации одному или всем остальным сетевым устройствам сети. К недостаткам такой топологии относится более высокая стоимость сетевого оборудования из-за необходимости приобретения специализированного центрального устройства. Кроме того, возможности по наращиванию количества узлов в сети ограничиваются количеством портов этого устройства.

При использовании в топологии нескольких центральных устройств по иерархической схеме (рисунок 2.7, *д*) образуется **древовидная топология**

или **иерархическая звезда**. В настоящее время дерево является самой распространенной топологией связей как в локальных, так и глобальных сетях.

Особым частным случаем звезды является **общая шина** (рисунок 2.7, *е*). Здесь в качестве центрального устройства выступает пассивный кабель, к которому по схеме «монтажного ИЛИ» подключается несколько сетевых устройств (такую же топологию имеют многие сети, использующие беспроводную связь – роль общей шины здесь играет общая радиосреда). Передаваемая информация распространяется по кабелю и доступна одновременно всем сетевым устройствам, присоединенным к этому кабелю. Основными преимуществами такой схемы являются ее дешевизна и простота присоединения новых узлов к сети, а недостатками – низкая надежность и невысокая производительность.

Приведенные выше типы топологий характерны для небольших сетей. Для крупных сетей характерно наличие произвольных связей между сетевыми устройствами. Топологию таких сетей называют смешанной (рисунок 2.8). В таких сетях можно выделить отдельные произвольно связанные фрагменты (подсети), имеющие типовую топологию.

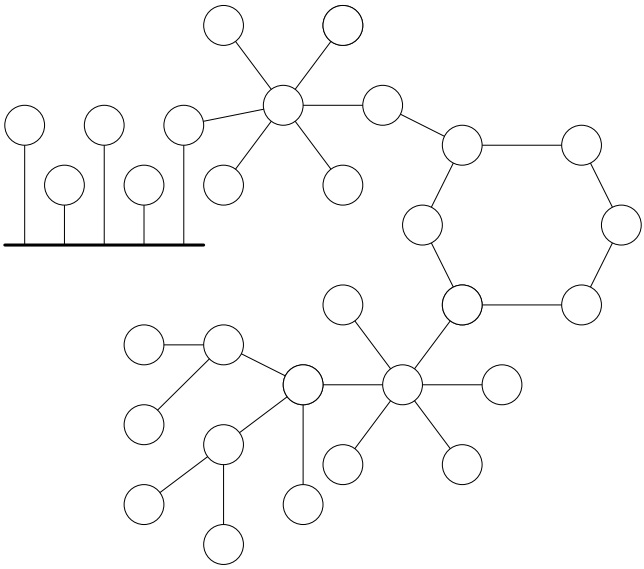

Рисунок 2.8 – Смешанная топология

2.6 Принципы адресации

Для взаимодействия сетевых устройств в сети необходимо, чтобы каждому из них был присвоен уникальный адрес. Благодаря адресу информация

от источника будет передана на конкретный приемник. Однако важно понимать, что адрес при организации адресации сети присваивается не узлу сети, а его сетевому интерфейсу. Один узел может иметь несколько сетевых интерфейсов.

По количеству адресуемых интерфейсов адреса можно классифицировать следующим образом:

– **уникальный адрес** используется для идентификации отдельных интерфейсов;

– **групповой адрес** идентифицирует сразу несколько интерфейсов, поэтому данные, помеченные групповым адресом, доставляются каждому из интерфейсов, входящих в группу;

– **широковещательный адрес** описывает все интерфейсы сети;

– **адрес произвольной рассылки** задает группу адресов, однако данные, посланные по этому адресу, должны быть доставлены не всем адресам данной группы, а лишь любому из них (такой тип адресов определен для IPv6).

Адреса могут быть **числовыми** (например, IP-адрес 129.26.254.254 или MAC-адрес 00:81:00:5e:24:a8) и **символьными** (например, URL https://www.bsut.by). Числовые имена предназначены для программного обеспечения сетевых устройств, а символьные, обычно имеющие смысловую нагрузку, – для запоминания людьми.

Множество всех адресов, которые являются допустимыми в рамках некоторой схемы адресации, называется **адресным пространством.** Адресное пространство может иметь плоскую (линейную) или иерархическую организацию.

При **плоской организации** множество адресов никак не структурировано, как например, MAC-адреса сетевых интерфейсов.

При **иерархической организации** адресное пространство структурируется в виде вложенных друг в друга подгрупп, которые определяют отдельный сетевой интерфейс и сеть, в которую он входит, например, IP-адрес.

При работе нескольких протоколов на разных уровнях модели OSI у интерфейса может быть сразу несколько адресов, например, MAC-адреса на канальном уровне для передачи кадров внутри локальной сети и IP-адрес на сетевом уровне для подключения к сети Интернет.

Кроме того, следует понимать, что конечной целью данных, передаваемых по сети, являются не сетевые интерфейсы, а приложения (процессы). Поэтому в адресе назначения наряду с информацией, идентифицирующей интерфейс устройства, должен указываться адрес процесса, которому предназначены посылаемые по сети данные. Уникальность адреса процесса достаточно обеспечить в рамках устройства, а уникальность устройства обеспечит адрес интерфейса. Примером адресов процессов являются номера портов TCP и UDP, используемые в стеке протоколов TCP/IP.

2.7 Принципы коммутации

Коммутация – это процесс соединения сетевых устройств через сеть с промежуточными (транзитными) сетевыми устройствами. Последовательность транзитных сетевых устройств, лежащих на пути от источника к приемнику в сети, образует **маршрут** передачи данных.

Комплекс технических решений обобщенной задачи коммутации в своей совокупности составляет основу любой сетевой технологии. В общем случае задача коммутации включает в себя следующие подзадачи:

– определение информационных потоков;

– прокладка маршрутов (маршрутизация);

– фиксация маршрутов в конфигурационных параметрах и таблицах сетевых устройств;

– распознавание потоков и передача данных между интерфейсами одного устройства (локальная коммутация в транзитном сетевом устройстве);

– мультиплексирование/демультиплексирование потоков;

– разделение среды передачи (при необходимости).

Информационным потоком или потоком данных называют непрерывную последовательность данных, объединенных набором общих признаков, выделяющих эти данные из общего сетевого трафика, например, адреса источника и приемника данных.

Метка потока – это особый тип признака. Она представляет собой некоторое число, которое несут все данные потока. Глобальная метка назначается данным потока и не меняет своего значения на всем протяжении его пути следования от узла источника до узла назначения, таким образом, она уникально определяет поток в пределах сети. В некоторых технологиях используются локальные метки потока, динамически меняющие свое значение при передаче данных от одного узла к другому.

Среди множества возможных подходов к решению задачи коммутации в сетях выделяют два основополагающих, к которым относят коммутацию каналов и коммутацию пакетов. Каждый из этих двух подходов имеет свои достоинства и недостатки. Существуют традиционные области применения каждой из техник коммутации, например, телефонные сети строились с использованием техники коммутации каналов, а компьютерные сети в подавляющем большинстве основаны на технике коммутации пакетов.

Сети, построенные по принципу **коммутации каналов**, используются не только в классической телефонии. Они находят широкое применение в мире телекоммуникаций, являясь основой первичных сетей, позволяющих создавать высокоскоростные магистральные каналы связи.

Сеть с коммутацией каналов представляет собой множество коммутаторов и конечных абонентских устройств, которые соединены с ближайшим коммутатором персональными абонентскими линиями связи.

В качестве информационных потоков в сетях с коммутацией каналов выступают данные, которыми обмениваются пары абонентов. Время существования информационного потока ограничивается рамками сеанса связи абонентов. Глобальным признаком потока является пара адресов (например, телефонных номеров) абонентов, связывающихся между собой через последовательность коммутаторов.

Для всех возможных потоков заранее определяются маршруты. Маршруты в сетях с коммутацией каналов задаются либо «вручную» администратором сети, либо находятся автоматически с привлечением специальных программных и аппаратных средств. Маршруты фиксируются в таблицах коммутации, в которых признакам потока ставятся в соответствие идентификаторы выходных интерфейсов коммутаторов. На основании этих таблиц происходит продвижение и мультиплексирование данных.

Особенностью сетей с коммутацией каналов является оперирование элементарными каналами. **Элементарный канал** – это базовая техническая характеристика сети с коммутацией каналов, представляющая собой некоторое фиксированное в пределах данного типа сетей значение пропускной способности. Традиционно элементарным каналом в цифровых системах передачи стал оцифрованный канал тональной частоты, предназначенный для передачи телефонного трафика. Такой канал получил название **основного цифрового канала**, условно обозначается как E0 и имеет пропускную способность 64 кбит/с. Любая линия связи в сети с коммутацией каналов имеет пропускную способность, кратную элементарному каналу, принятому для данного типа сети. Таким образом, пропускная способность каждой линии связи в сети с коммутацией каналов должна быть равна целому числу элементарных каналов. Формируемый в такой линии связи канал называется **составным каналом.** Он имеет следующие свойства:

– составной канал на всем своем протяжении состоит из одинакового количества элементарных каналов;

– составной канал имеет постоянную и фиксированную пропускную способность на всем своем протяжении;

– составной канал создается временно на период сеанса связи двух абонентов;

– на время сеанса связи все элементарные каналы, входящие в составной канал, поступают в исключительное пользование абонентов, для которых был создан этот составной канал;

– в течение всего сеанса связи абоненты могут посылать в сеть данные со скоростью, не превышающей пропускную способность составного канала;

– данные, поступившие в составной канал, гарантированно доставляются вызываемому абоненту без дополнительных задержек и потерь;

– после окончания сеанса связи элементарные каналы, входившие в соответствующий составной канал, объявляются свободными для использования другими абонентами.

При отсутствии в линии связи между абонентами составного канала необходимой пропускной способности или занятости всех элементарных каналов абонент, пытающийся установить соединение, получает отказ и вынужден ожидать освобождения канала связи.

Важнейшим принципом функционирования сетей с **коммутацией пакетов** является представление информации, передаваемой по сети, в виде структурно отделенных друг от друга порций данных, которые называются в общем случае пакетами.

Каждый пакет снабжен заголовком, в котором содержится адрес назначения и другая вспомогательная информация, используемая для доставки пакета по адресу назначения. Именно наличие адреса назначения в заголовке пакета позволяет сетевому устройству обрабатывать каждый пакет независимо от других. Помимо заголовка у пакета может иметься еще одно дополнительное поле, размещаемое в конце пакета и поэтому называемое концевиком. В концевике обычно помещается контрольная сумма, которая позволяет проверить целостность информации в пакете.

В зависимости от конкретной реализации технологии коммутации пакетов последние могут иметь фиксированную или переменную длину, может меняться состав информации, размещенной в заголовках пакетов.

Пакеты поступают в сеть в том темпе, в котором их генерирует источник. Если пропускная способность линии, подключенной к сетевому устройству, достаточна, то сеть с коммутацией пакетов всегда готова принять пакет от конечного узла. Пакеты вне зависимости от потоков могут перемешиваться при перемещении по сети, образовывать очереди и «тормозить» друг друга.

Разделение данных на пакеты позволяет передавать неравномерный компьютерный трафик более эффективно, чем в сетях с коммутацией каналов. Это объясняется тем, что пульсации трафика от отдельных компьютеров носят случайный характер и распределяются во времени так, что их пики чаще всего не совпадают. Поэтому когда линия связи передает трафик большого количества конечных узлов, в суммарном потоке пульсации сглаживаются и пропускная способность линии используется более рационально, без длительных простоев.

Главное отличие коммутаторов в сетях с коммутацией пакетов от коммутаторов в сетях с коммутацией каналов состоит в том, что первые имеют внутреннюю буферную память для временного хранения пакетов.

В таблице 2.3 представлено сравнение свойств сетей с коммутацией каналов и с коммутацией пакетов.

Таблица 2.3 – **Сравнение свойств сетей с разными способами коммутации**

Коммутация каналов	Коммутация пакетов
Необходимо предварительно устанавливать соединение	Отсутствует этап установления соединения (дейтаграммный способ)
Адрес требуется только на этапе установления соединения	Адрес и другая служебная информация передаются с каждым пакетом
Сеть может отказать абоненту в установлении соединения	Сеть всегда готова принять данные от абонента
Гарантированная пропускная способность (полоса пропускания) для взаимодействующих абонентов	Пропускная способность сети для абонентов неизвестна, задержки передачи носят случайный характер
Трафик реального времени передается без задержек	Ресурсы сети используются эффективно при передаче пульсирующего трафика
Высокая надежность передачи	Возможны потери данных из-за переполнения буферов
Нерациональное использование пропускной способности каналов, снижающее общую эффективность сети	Автоматическое динамическое распределение пропускной способности физического канала между абонентами

2.8 Принципы маршрутизации

Задача маршрутизации включает в себя две подзадачи:

– определение маршрута – выбор последовательности транзитных узлов и их интерфейсов, через которые надо передавать данные, чтобы доставить их адресату;

– оповещение сети о выбранном маршруте.

При наличии нескольких маршрутов необходимо определить «оптимальный» по некоторому критерию маршрут. В качестве критериев оптимальности могут выступать:

– номинальная пропускная способность и загруженность каналов связи;

– задержки, вносимые каналами;

– количество промежуточных транзитных узлов;

– надежность каналов и транзитных узлов;

– текущая степень загруженности каналов трафиком.

Способ расчета «оптимальности» маршрута заключается во введении количественной оценки – **метрики**, ее расчета для каждого из маршрутов и выбор маршрута с минимальным значением метрики, например, для определения метрики, учитывающей пропускную способность каналов связи, вычисляют значение обратное его пропускной способности умноженное на константу, заведомо большую, чем пропускные способности каналов в сети.

После определения «оптимального» маршрута необходимо оповестить о нем все устройства сети. Для этого используются специальные протоколы,

которые создают записи в таблицах коммутации (маршрутизации) транзитных сетевых устройств. Записи могут также создаваться автоматически или вручную в процессе администрирования сети.

На рисунке 2.9 представлены интерфейсы коммутатора, информационные потоки и таблица коммутации, на основании которой данные потоков продвигаются между интерфейсами коммутатора. **Демультиплексирование** – разделение суммарного потока на несколько составляющих его потоков. Обратная демультиплексированию операция – **мультиплексирование** (агрегирование) – образование из нескольких отдельных потоков общего агрегированного потока, который передается по одному физическому каналу связи. Эти процессы необходимы из-за передачи разных потоков по общим каналам.

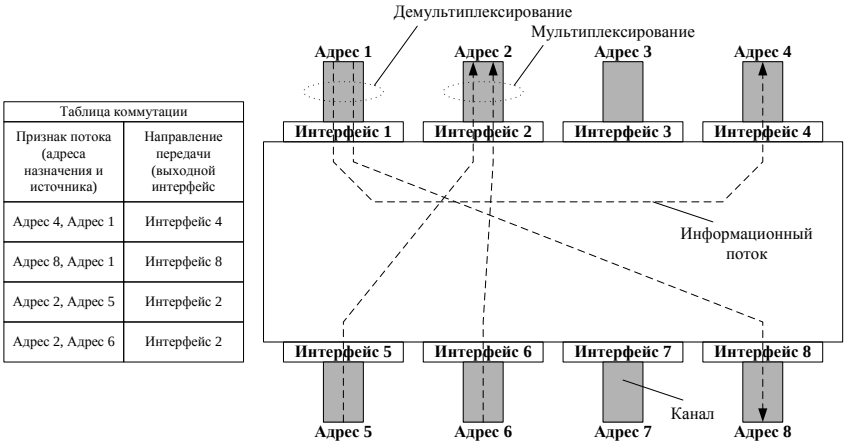

Таблица коммутации

Признак потока (адреса назначения и источника)	Направление передачи (выходной интерфейс
Адрес 4, Адрес 1	Интерфейс 4
Адрес 8, Адрес 1	Интерфейс 8
Адрес 2, Адрес 5	Интерфейс 2
Адрес 2, Адрес 6	Интерфейс 2

Рисунок 2.9 – Таблица коммутации

В соответствии с информацией из таблицы коммутации (маршрутизации) осуществляется продвижение данных между интерфейсами.

Интерфейс коммутатора (называемый также портом) является физическим модулем, состоящим из приемника и передатчика. В том случае, когда передатчик и приемник работают на дуплексный канал связи, они работают независимо друг от друга, обеспечивая одновременную передачу данных в обоих направлениях. Иногда приемную часть интерфейса называют входным интерфейсом, а выходную часть – выходным интерфейсом.

Продвижение данных в сетях с коммутацией каналов происходит в два этапа:

1 В сеть поступает служебное сообщение – запрос, который несет адрес вызываемого абонента и инициирует создание составного канала.

2 По подготовленному составному каналу передается основной поток данных, для передачи которого уже не требуется никакой вспомогательной информации, в том числе адреса вызываемого абонента. Коммутация данных в коммутаторах выполняется на основе локальных признаков потока – номеров выделенных ему элементарных каналов.

Продвижение данных в сетях с коммутацией пакетов может производиться на основании одного из трех методов:

– дейтаграммная передача;

– передача с установлением логического соединения;

– передача с установлением виртуального канала.

Дейтаграммный способ передачи данных основан на том, что все передаваемые пакеты продвигаются независимо друг от друга на основании одних и тех же правил. Каждый отдельный пакет рассматривается сетью как совершенно независимая единица передачи – дейтаграмма. При таком способе продвижения доставка пакета не гарантируется, а выполняется по мере возможности.

При использовании **логического соединения** предполагается процедура согласования двумя конечными узлами сети некоторых параметров процесса обмена. Параметры, о которых договариваются два взаимодействующих узла, называются параметрами логического соединения. Параметры соединения могут быть постоянными, то есть не изменяющимися в течение всего соединения, или переменными, то есть динамически отражающими текущее состояние соединения.

Передача с установлением логического соединения включает три фазы:

– установление логического соединения;

– передача данных;

– разрыв логического соединения.

Передача с установлением соединения предоставляет больше возможностей в плане надежности и безопасности обмена данными, чем дейтаграммная передача, однако этот способ более медленный, так как он подразумевает дополнительные вычислительные затраты на установление и поддержание логического соединения.

Виртуальный канал – это единственный заранее проложенный фиксированный маршрут, соединяющий конечные узлы в сети с коммутацией пакетов. Виртуальные каналы прокладываются для устойчивых информационных потоков за счет использования меток. Как и в сетях с установлением логических соединений, прокладка виртуального канала начинается с установления соединения, в процессе которого назначается метка потока. Затем в таблице каждого из коммутаторов, расположенных на пути от отправителя до получателя, формируется запись с данной меткой, которая указывает на способ обслуживания пакетов с такой меткой. Образовавшийся

виртуальный канал идентифицируется той же меткой. После прокладки виртуального канала сеть может передавать по нему соответствующий поток данных. Во всех пакетах, которые переносят пользовательские данные, адрес назначения уже не указывается, его роль играет метка виртуального канала.

Чтобы определить, на какой интерфейс следует передать поступившие данные, транзитное сетевое устройство должно выяснить, к какому потоку они относятся. Если на входной интерфейс поступает поток, являющийся результатом агрегирования нескольких потоков, то к задаче распознавания потоков добавляется задача демультиплексирования.

Одним из основных способов мультиплексирования потоков является разделение по времени – каждый поток получает физический канал в полное свое распоряжение и передает по нему свои данные в определенные промежутки времени с фиксированным или случайным периодом. Распространено также частотное (спектральное для волоконно-оптических линий связи) разделение канала, когда каждый поток передает данные в выделенном ему частотном (спектральном) диапазоне.

До середины 90-х годов прошлого века в локальных сетях использовался режим передачи, основанный на разделяемой среде. **Разделяемой средой** называется физическая среда передачи данных, к которой непосредственно подключено несколько передатчиков узлов сети. В каждый момент времени только один из передатчиков какого-либо узла сети получает доступ к разделяемой среде и использует ее для передачи данных приемнику другого узла, подключенному к этой же среде.

В настоящее время механизм разделения среды используется только в беспроводных локальных сетях, где разделяемой средой является радиоэфир.

2.9 Классификация сетей

Выборочная классификация сетей по различным признакам представлена на рисунке 2.10.

Первичные сети – это вспомогательные сети, организующие передачу полезной нагрузки вторичных сетей. Они позволяют создавать постоянные физические двухточечные каналы для других сетей. **Вторичные сети** – это все остальные сети, которые предоставляют услуги конечным пользователям и строятся на основе каналов первичных сетей.

Сети операторов связи принадлежат поставщикам услуг связи и предоставляют эти услуги клиентам. **Корпоративные сети** предоставляют услуги только сотрудникам предприятия, которое владеет этой сетью. **Персональные сети** находятся в личном использовании.

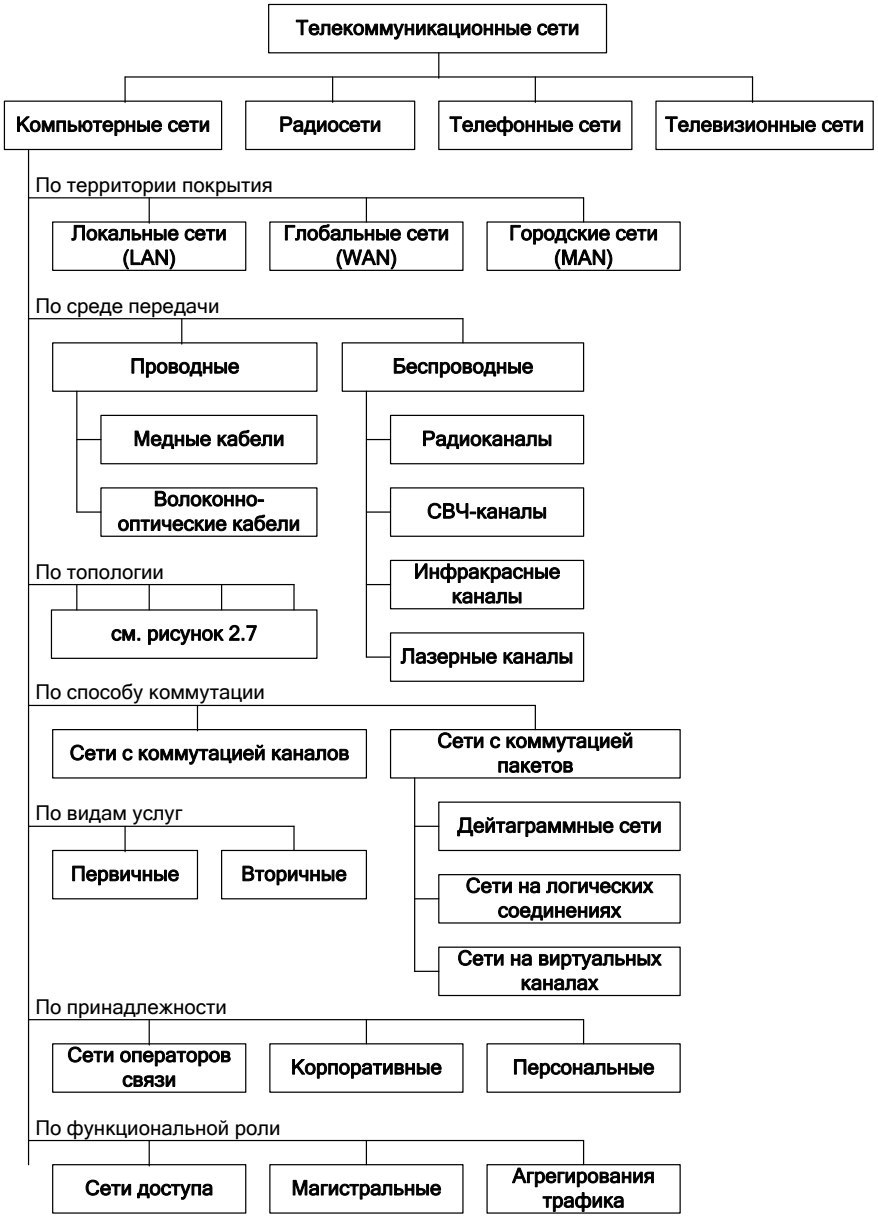

Рисунок 2.10 – Классификация сетей

Сети доступа – это сети, предоставляющие доступ индивидуальным и корпоративным абонентам от их помещений до точки присутствия оператора сети связи или оператора корпоративной сети. **Магистральные сети** – это сети, представляющие собой наиболее скоростную часть (ядро) глобальной сети, которая объединяет многочисленные сети доступа в единую сеть. **Сети агрегирования трафика** – это сети, агрегирующие данные от многочисленных сетей доступа для компактной передачи их по небольшому числу каналов связи в магистральную сеть (не всегда присутствуют в качестве посредника между магистральными сетями и сетями доступа).

В современных компьютерных сетях чаще используются локальные и глобальные сети. Для стационарных сетевых устройств наибольшее распространение получили проводные сети с использованием медных кабелей, а для мобильных – беспроводные с использованием радиоканалов. По топологии чаще всего встречаются сети с древовидной топологией. По способу коммутации подавляющее количество компьютерных сетей использует принцип коммутации пакетов. В зависимости от принадлежности все классы сетей получили достаточное распространение.

Контрольные вопросы

1 Дайте понятие локальной сети.

2 Что такое глобальная сеть?

3 В чем отличие инфокоммуникационной сети от телекоммуникационной?

4 Перечислите основные этапы становления современных глобальных и локальных компьютерных сетей.

5 Приведите примеры того, что Интернет является фактором развития сетевых технологий.

6 Что такое интернет вещей?

7 Какие организации отвечают за развитие Интернета?

8 Назовите уровни модели OSI и решаемые ими задачи.

9 Перечислите уровни модели OSI, задачи которых выполняют коммутаторы.

10 Перечислите уровни модели OSI, задачи которых выполняют маршрутизаторы.

11 Что такое межуровневый интерфейс?

12 Дайте понятие протоколу.

13 Распределите основные функции информационной безопасности по уровням модели OSI.

14 Перечислите типовые топологии сети, их достоинства и недостатки.

15 Назовите основные ствойства полносвязной топологии.

16 Что такое ячеистая топология?

17 В чем заключается преимущество использования кольцевой топологии?

18 В чем заключается основное отличие топологии «плоское кольцо» от кольцевой топологии?

19 Приведите примеры использования звездообразной топологии.

20 Где в настоящее время можно встретить использование топологии «общая шина»?

21 Каковы основные принципы адресации в сетях?

22 Приведите классификацию адресов.

23 Что такое коммутация?

24 Дайте понятие элементарному каналу?

25 В каких системах передачи используется коммутация каналов?

26 В каких системах передачи используется коммутация пакетов?

27 Сравните свойства коммутации каналов и коммутации пакетов.

28 Что такое метрика и для чего она используется?

29 Какие задачи решает маршрутизация?

30 Каким образом организуется дейтаграммный способ передачи данных?

31 Каковы основные фазы передачи информации с установлением логического соединения?

32 Что такое виртуальный канал?

33 Для каких целей используется мультиплексирование трафика?

34 По каким признакам производится классификация сетей?

35 Что такое первичная сеть?

36 В чем основное отличие сетей операторов услуг, корпоративных и персональных сетей?

37 Для каких целей предназначены сети доступа?

38 Что такое сети агрегирования трафика?

39 Дайте понятие вторичной сети.

40 В чем основное отличие первичной и вторичной сетей?

41 Для чего предназначены корпоративные сети?

42 Где применяются персональные сети?

43 Приведите примеры корпоративных и персональных сетей связи.

44 Для чего предназначены магистральные сети?

45 В чем основное отличие магистральных сетей от сетей доступа?

46 Назовите основные классы телекоммуникационных сетей.

3 УГРОЗЫ, УЯЗВИМОСТИ И РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1 Понятие угрозы информационной безопасности

В соответствии с государственным стандартом Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения» **угроза (безопасности информации)** – это совокупность условий и факторов, создающих потенциальную или реальную существующую опасность нарушения безопасности информации.

Угроза безопасности информационной системы – это возможное воздействие на систему, которое прямо или косвенно может нанести ущерб ее безопасности. Угроза, как следует из определения, – это опасность причинения ущерба, то есть в этом определении проявляется связь технических проблем с юридической категорией, каковой является «ущерб».

Проявления возможного ущерба могут быть различны:

– моральный и материальный ущерб деловой репутации организации;

– моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

– материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

– материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

– материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной и т. п.

Угрозами безопасности информации являются нарушения при обеспечении:

– конфиденциальности;

– доступности;

– целостности.

Нарушения при обеспечении конфиденциальности:

– хищение (копирование) информации и средств ее обработки;

– утрата (неумышленная потеря, утечка) информации и средств ее обработки.

Нарушения при обеспечении доступности:

– блокирование информации;

– уничтожение информации и средств ее обработки.

Нарушения при обеспечении целостности:

– модификация (искажение) информации;

– отрицание подлинности информации;

– навязывание ложной информации.

Кроме того, угрозы могут классифицироваться по многим другим признакам, например, по характеру:

– Случайные (отказы, сбои, ошибки, стихийные явления). Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются, как правило, в теории надежности, программировании, инженерной психологии;

– Преднамеренные (злоумышленные действия субъектов). Для несанкционированного доступа к информации нарушитель может воспользоваться штатными каналами доступа, если по отношению к ним не предприняты никакие меры защиты, либо нештатными каналами доступа, к которым принято относить: побочное электромагнитное излучение информации с аппаратуры системы, побочные наводки информации по сети электропитания и заземления, побочные наводки информации на вспомогательных коммуникациях, подключение к внешним каналам связи и т. п.

Совокупность всех угроз $T = \{T_1, T_2, \ldots, T_m\}$ (от англ. *threat*), которые в той или иной степени могут нанести ущерб безопасности системы, формируют реальную среду ее функционирования. Именно на такое функционирование следует рассчитывать при эксплуатации объектов железнодорожного транспорта. Любая угроза не может существовать сама по себе – у нее должен быть источник, который является носителем угрозы безопасности информации. **Источник угрозы безопасности информации** – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Причем источники угроз могут находиться как внутри защищаемой организации – внутренние источники, так и вне ее – внешние источники.

Все источники угроз безопасности информации можно разделить на три основные группы:

1) обусловленные действиями субъекта (антропогенные источники угроз);

2) обусловленные техническими средствами (техногенные источники угроз);

3) обусловленные стихийными источниками.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорить о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети.

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако последствия, вызванные такой деятельностью, вышли из-под контроля человека и существуют сами но себе. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием используемого оборудования, а также отсутствием материальных средств на его обновление.

Третья группа источников угроз объединяет обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию, и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности, как правило, являются внешними по отношению к защищаемому объекту и под ними понимаются, прежде всего, природные катаклизмы.

Примерная классификация и перечень источников угроз приведены в таблице 3.1.

Таблица 3.1 – **Классификация и перечень источников угроз информационной безопасности**

Антропогенные источники	Внешние	Криминальные структуры
		Потенциальные преступники и хакеры
		Недобросовестные партнеры
		Технический персонал поставщиков телекоммуникационных услуг
		Представители надзорных организаций и аварийных служб
		Представители силовых структур
	Внутренние	Основной персонал (пользователи, программисты, разработчики)
		Представители службы защиты информации (администраторы)
		Вспомогательный персонал (уборщики, охрана)
		Технический персонал (жизнеобеспечение, эксплуатация)
Техногенные источники	Внешние	Средства связи
		Сети инженерных коммуникации (водоснабжения, канализации)
		Транспорт
	Внутренние	Некачественные технические средства обработки информации
		Некачественные программные средства обработки информации
		Вспомогательные средства (охраны, сигнализации, телефонии)
		Другие технические средства, применяемые в учреждении
Стихийные источники	Внешние	Пожары
		Землетрясения
		Наводнения
		Ураганы
		Магнитные бури
		Радиоактивное излучение
		Различные непредвиденные обстоятельства
		Необъяснимые явления
		Другие форс-мажорные обстоятельства

3.2 Уязвимости информационных систем

Угрозы как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости, приводящие к нарушению безопасности информации в конкретной информационной системе.

В соответствии с государственным стандартом Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения» **уязвимость информационной системы** – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Уязвимости присущи информационной системе, неотделимы от нее и обусловливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Уязвимости безопасности информации могут быть:

– объективными;

– субъективными;

– случайными.

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации.

Субъективные уязвимости зависят от действий сотрудников и в основном устраняются организационными и программно-аппаратными методами.

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию, угрозам информационной безопасности.

Примерная классификация и перечень уязвимостей информационной безопасности приведены в таблицах 3.2–3.4.

Совокупность уязвимостей информационной системы $V = \{V_1, V_2, \ldots, V_k\}$ (от англ. *vulnerability*) ограничивает сферу ее эксплуатации и режимы функционирования. Максимально полное представление об уязвимостях позволяет применить адекватные меры по их минимизации и тем самым устранить возможные последствия от воздействия угроз.

Таблица 3.2 – **Классификация и перечень объективных уязвимостей информационной безопасности**

Сопутствующие техническим средствам излучения	Электромагнитные (побочные излучения элементов технических средств, кабельных линий, излучения на частотах работы генераторов и самовозбуждения усилителей)
	Электрические (наводки электромагнитных излучений на линии и проводники, просачивание сигналов в цепи электропитания, в цепи заземления, неравномерность потребления тока электропитания)
	Звуковые (акустические, виброакустические)
Активизируемые	Аппаратные закладки (в телефонные линии, в сети электропитания, в помещениях, в технических средствах)
	Программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии ПО)
Определяемые особенностями элементов	Элементы, подверженные воздействию электромагнитного поля (магнитные носители, микросхемы, нелинейные элементы, подверженные ВЧ навязыванию)
Определяемые особенностями защищаемого объекта	Местоположением объекта (отсутствие контролируемой зоны, наличие удаленных и мобильных элементов объекта)
	Организацией каналов обмена информацией (использование радиоканалов, глобальных информационных сетей, арендуемых каналов)

Таблица 3.3 – **Классификация и перечень субъективных уязвимостей информационной безопасности**

Ошибки (халатность)	При подготовке и использовании ПО (при разработке алгоритмов, при инсталляции и загрузке, при эксплуатации, при вводе данных, при настройке сервисов)
	При эксплуатации технических средств (при включении/выключении технических средств, при использовании технических средств охраны)
	Некомпетентные действия (при конфигурировании и управлении сложной системы, при настройке ПО, при организации управления потоками обмена информации, при настройке технических средств, при настройке штатных средств защиты)
	Неумышленные действия (повреждение или удаление ПО, данных, носителей информации, каналов связи
Нарушения	Режима охраны и защиты (доступа на объект, к техническим средствам, соблюдения конфиденциальности)
	Режима эксплуатации технических средств и ПО (энергообеспечения, жизнеобеспечения, установки нештатного оборудования, инсталляции игрового, обучающего, нештатного технологического ПО)

Окончание таблицы 3.3

	Использования информации (обработки и обмена информацией, хранения и уничтожения носителей информации, уничтожения производственных отходов и брака)
Психогенные	Психологические (антагонистические отношения, неудовлетворенность своим положением, действиями руководства, психологическая несовместимость)
	Психические (психические отклонения, стрессовые ситуации)
	Физиологические (физическое состояние, психосоматическое состояние)

Таблица 3.4 – **Классификация и перечень случайных уязвимостей информационной безопасности**

Сбои и отказы	Отказы и неисправности технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа)
	Старение и размагничивание носителей информации (съемных носителей, жестких дисков, элементов микросхем, кабелей и соединительных линий)
	Сбои ПО (операционных систем и СУБД, прикладных программ, сервисных программ, антивирусных программ)
	Сбои электроснабжения (оборудования, обрабатывающего информацию, вспомогательного оборудования)

При наличии множества уязвимостей информационной системы и множества угроз ее безопасности в реальных условиях функционирования велика вероятность реализации одной из таких угроз через какую-либо уязвимость.

Атака – это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости. Атака – это всегда пара «источник – уязвимость», реализующая угрозу и приводящая к ущербу. Взаимосвязь понятий угроза, уязвимость и атака проиллюстрирована на рисунке 3.1. Для того чтобы произошла атака необходимо, чтобы реализовалась конкретная угроза при взаимодействии источника данной угрозы с конкретной уязвимостью информационной системы в обход системы защиты информации (рисунок 3.2). Для каждой из угроз безопасности информационной системы можно определить подмножество уязвимостей $VT \subseteq V$, через которые данная угроза может реализоваться.

Безопасный или защищенный объект – это объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

3.3 Риски информационной безопасности

Управление информационными рисками – системный процесс идентификации, контроля и уменьшения информационных рисков организаций в

соответствии с определенными ограничениями нормативно-правовой базы (НПБ) в области защиты информации и собственной корпоративной политики безопасности.

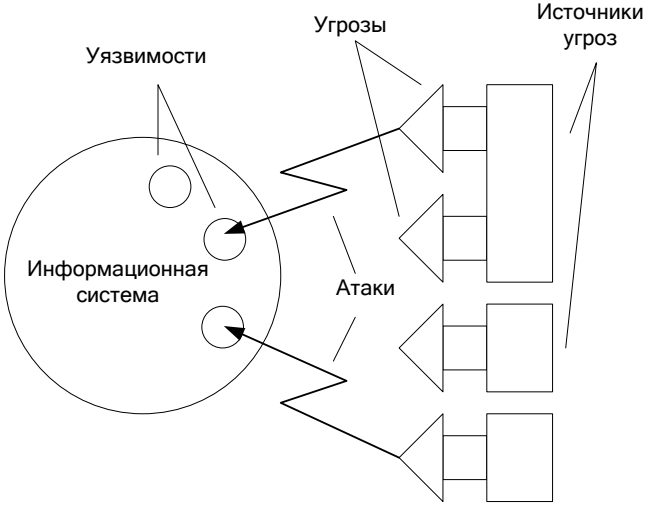

Рисунок 3.1 – Взаимосвязь понятий ургоза, уязвимость и атака

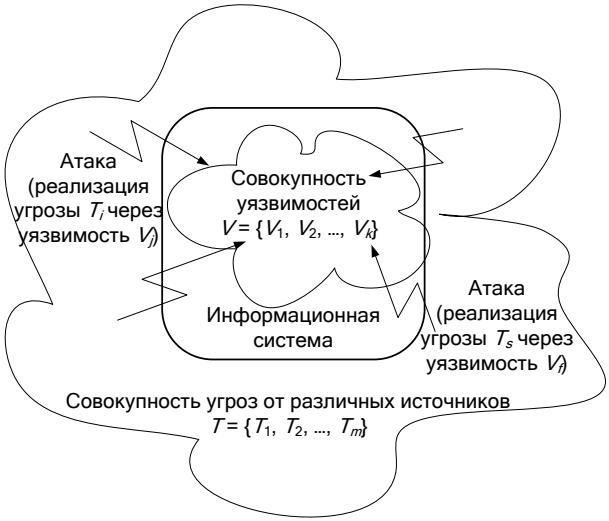

Рисунок 3.2 – Совокупности угроз и уязвимостей безопасности информационной системы

Защита активов связана с деятельностью по предотвращению угроз, классифицируемых в зависимости от характера ущерба, который они могут нанести этим активам. Во внимание должны приниматься все угрозы, но в первую очередь те, которые связаны со случайными и преднамеренными действиями человека.

Согласно СТБ 34.101.1–2014 **риск нарушения безопасности** – это возможность реализации угрозы, которая нанесет ущерб владельцу. В основном ущерб наносится активам организации.

Активы организации – это все то, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении. К активам организации могут относиться:

– информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т. д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);

– выпускаемая продукция и/или оказываемые услуги;

– аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, коммуникационные линии, серверы, маршрутизаторы;

– программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы;

– данные: обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, передаваемые по коммуникационным линиям;

– пользователи, обслуживающий персонал;

– документация: по программам, по аппаратуре, системная, по административным процедурам;

– расходные материалы: бумага, формы и т. д.

Защита активов связана с деятельностью по предотвращению угроз, классифицируемых в зависимости от характера ущерба, который они могут нанести этим активам. Во внимание должны приниматься все угрозы, но в первую очередь те, которые связаны со случайными и преднамеренными действиями человека. На рисунке 3.3 приведены концептуальные понятия безопасности и их взаимосвязь, регламентируемые СТБ 34.101.1–2014 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

В защите активов заинтересованы их собственники (владельцы). Но эти активы представляют интерес и для нарушителей, которые стремятся использовать активы в своих целях, вопреки интересам владельцев. Наруше-

ния безопасности обычно включают (но не ограничиваются только этими категориями): несанкционированное раскрытие (потерю конфиденциальности), несанкционированную модификацию (потерю целостности) или несанкционированное лишение доступа к активам (потерю доступности).

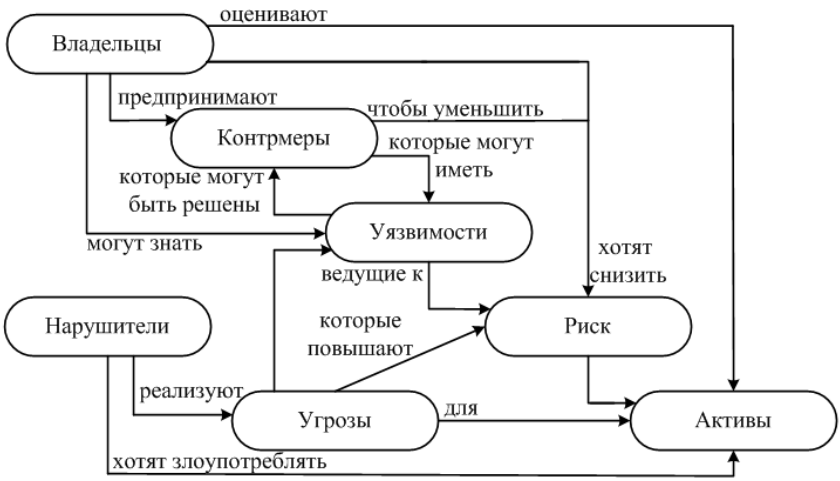

Рисунок 3.3 – Схема концептуальных понятий безопасности и их взаимосвязь

Владельцы активов должны проводить анализ риска, т. е. определять угрозы, уязвимые места, возможный ущерб от реализации каждой угрозы и контрмеры. Чтобы выполнялась требуемая владельцем политика безопасности активов, необходимо принять меры по уменьшению числа уязвимых мест, так как нарушители могут их использовать.

Еще до ввода в эксплуатацию информационной системы владелец заинтересован в оценке эффективности мер противодействия угрозам. Результатом такой оценки является заключение о степени гарантии, с которой меры противодействия уменьшают риск для активов. Гарантией называется основание для уверенности в том, что информационная система отвечает задачам безопасности.

Для оценки рисков существуют качественные и количественные методы. Качественная методика предназначена для проведения общей и частных оценок, позволяющих руководителю организации принять обоснованное решение о необходимости защиты конфиденциальной информации, циркулирующей внутри организации, от конкурентов с оценкой предстоящих расходов на защиту. Методика позволяет быстро и достаточно объективно провести экспресс-оценку необходимости защиты конфиденциальной информации и на ее основе оперативно принять соответствующее решение,

т. е. она позволяет руководителю избежать больших коммерческих неудач и потерь прибыли из-за доступности информации конкурентам.

Суть количественной оценки рисков сводится к поиску единственного оптимального решения из множества существующих. К количественным методикам управления рисками относятся методики CRAMM, MethodWare и др.

Для количественной оценки риска используется следующая формула:

$$R = P_{\text{А}} U, \tag{3.1}$$

где R – риск от реализации угрозы;

$P_{\text{А}}$ – вероятность реализации угрозы;

U – величина ущерба.

Вероятность реализации угрозы состоит из вероятности появления источника угрозы и его готовности атаковать, а также включает вероятности наличия у информационной системы подходящей уязвимости и ее доступность для угрозы:

$$P_{\text{А}} = P_{\text{УГ}} P_{\text{УЯЗ}}, \tag{3.2}$$

где $P_{\text{УГ}}$ – вероятность появления источника угрозы и его готовности атаковать;

$P_{\text{УЯЗ}}$ – вероятность наличия у информационной системы подходящей уязвимости и ее доступность для угрозы.

Уровень защищенности информационной системы – это мера, определяющая возможность предотвращения ущерба, наносимого владельцу информационной системы, в следствии использования конкретного комплекса средств защиты информации при реализации угроз безопасности через установленные уязвимости этой информационной системы.

Уровень защищенности

$$Z = \frac{1}{P_{\text{А}} U P_{\text{ПСЗ}}}, \tag{3.3}$$

где Z – защищенность информационной системы от воздействия конкретной угрозы;

$P_{\text{ПСЗ}}$ – вероятность преодоления средства защиты информации информационной системы в процессе реализации угрозы.

При анализе защищенности информационной системы от нескольких угроз оценка уровня защищенности будет рассчитываться по следующей формуле:

$$Z = \frac{N}{\sum_{i=1}^{N} \left(P_{\text{А}i} U_i P_{\text{ПСЗ}i} \right)}, \tag{3.4}$$

где N – количество угроз.

Существует четыре метода оценки эффективности безопасности, основанных на анализе рисков:

1 **Базовый метод** основан на использовании стандартов информационной безопасности.

2 **Метод детального анализа рисков** предполагает систематический анализ исходных данных для конкретной информационной системы с целью оценки рисков нарушения ее безопасности и выбора средств защиты, соответствующих заданным требованиям.

3 **Экспертный метод** основан на проведении неформального анализа рисков, результат которого основан на знаниях и опыте экспертов.

4 **Комбинированный метод** предполагает использование в различных сочетаниях трех предыдущих методов.

Первые три метода имеют свои преимущества и недостатки. Первый метод прост и надежен, однако опирается на базовый набор требований и предполагает использование штатных методов защиты информации. Второй метод достаточно сложен в реализации, требует максимальных затрат времени и усилий. Третий метод достаточно субъективен и не систематичен.

В связи с этим для информационных объектов железнодорожного транспорта будет оптимальным использовать комбинированный метод оценки эффективности безопасности. При этом, опираясь на действующие стандарты информационной безопасности (базовый метод), детально прорабатываются риски безопасности информационных систем с учетом множества угроз их безопасности (метод детального анализа рисков), а для оценки вероятностей реализации угроз через конкретные уязвимости в обход системы защиты, а также величины возможного ущерба, который будет при этом нанесен, используется экспертная оценка (экспертный метод).

Оценку рисков безопасности информационной системы железнодорожного транспорта следует начать с определения множества угроз безопасности. Для каждой из угроз экспертам предлагается дать оценку по двум критериям:

– критерий C_1 (от англ. *Criterion*) – возможность возникновения источника угрозы в достаточном окружении от информационной системы для реализации угрозы (если возможность возникновения источника угрозы высока, то эксперт ставит высокую оценку, если мала – низкую);

– критерий C_2 – степень готовности источника угрозы реализовать угрозу.

Критерии оцениваются экспертами по десятибалльной шкале (дискретно от 1 до 10).

Следующим шагом определяется множество уязвимостей информационной системы. Для каждой уязвимости экспертам предлагается дать оценку также по двум критериям:

– критерий C_3 – распространенность уязвимости по информационной системе или частота ее появления;

– критерий C_4 – доступность уязвимости для реализации через нее угроз.

Затем для каждой из угроз определяется подмножество уязвимостей, через которые угроза может быть реализована (таблица 3.5). Угрозы, для которых подмножество уязвимостей является пустым, удаляются из списка угроз. Для каждой уязвимости из подмножества экспертами определяется критерий C_5 – фатальность от реализации угрозы источником угрозы через уязвимость информационной системы.

Оценка риска от реализации каждой из угроз при использовании оценок экспертов производится по следующей формуле:

$$R_i = \frac{\sum_{j=1}^{M} C_{1j} \sum_{j=1}^{M} C_{2j} \sum_{j=1}^{M} C_{3j} \sum_{j=1}^{M} C_{4j} \sum_{j=1}^{M} C_{5j}}{M^5}, \qquad (3.5)$$

где M – количество экспертов;

C_{ij} – значение i-го критерия, выставленного j-м экспертом.

В данной формуле, в отличии от формул (3.1) и (3.2) применяются не значения вероятностей и величины ущерба, а оценки экспертов, что не позволит получить уровень ущерба в единицах, в которых измеряется ущерб. Однако это позволит сопоставлять уровень нанесенного ущерба владельцу информационной системы посредством реализации разного набора угроз безопасности. В формуле (3.5) критерии C_1 и C_2 соответствуют $P_{УГ}$ из формулы (3.2), C_3 и C_4 – $P_{УЯЗ}$ из этой же формулы, а C_5 – U из формулы (3.1).

Таблица 3.5 – **Выбор подмножеств уязвимостей информационной системы для конкретных угроз**

Угроза безопасности	Уязвимость информационной системы					
	№ 1	№ 2	№ 3	№ 4	№ 5	и т. д.
№ 1	×	×	×			
№ 2		×		×	×	
№ 3						
№ 4	×		×			
и т. д.						

При наличии M экспертов для упрощения формулы (3.5) критерии C_1 и C_2 удобно представить параметром $C_{УГ}$:

$$C_{УГ} = \sum_{j=1}^{M} C_{1j} \sum_{j=1}^{M} C_{2j}. \qquad (3.6)$$

Критерии C_3, C_4 и C_5 выбираются только для одной из уязвимостей подмножества. Эта уязвимость имеет максимальное значение произведения данных критериев, выставленных всеми экспертами и для удобства представляется параметром $C_{\text{УЯЗ}}$:

$$C_{\text{УЯЗ}} = \sum_{j=1}^{M} C_{3j} \sum_{j=1}^{M} C_{4j} \sum_{j=1}^{M} C_{5j} \to \max. \tag{3.7}$$

При таком расчете максимальное значение риска реализации угрозы при выставлении экспертами только максимальных баллов по всем критериям будет равно 10^5. Минимальное значение риска (все эксперты выставили только минимальные баллы) – 1.

При оценке фатальности (критерий C_5) от реализации угрозы для информационных объектов железнодорожного транспорта важно не только принимать во внимание нарушение информационной безопасности, но также учитывать и функциональную безопасность. В таблице 3.6 представлены рекомендации для экспертов при выставлении баллов по данному критерию исходя из соображений первостепенной важности обеспечения функциональной безопасности для объектов железнодорожного транспорта.

Функциональная безопасность – это совокупность таких условий функционирования информационной системы, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных воздействий, приводящих к нарушению процесса штатного ее функционирования.

Для оценки уровня защищенности информационной системы необходимо ввести дополнительный критерий C_6 – степень преодоления средства защиты информации в процессе реализации угрозы. Для оценки эффективности защищенности можно выбирать отдельные средства защиты информации или их комбинации.

Комплекс средств защиты – совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности объекта.

Для каждого средства защиты информации эксперты также по десятибалльной шкале (дискретно от 1 до 10) определяют критерий C_6. При комбинировании средств защиты информации используется только одно максимальное значение данного критерия из его значений для каждого из средств защиты информации по отдельности. При наличии M экспертов для упрощения данный критерий удобно представить параметром $C_{\text{СЗИ}}$:

$$C_{\text{СЗИ}} = \sum_{j=1}^{M} C_{6j}. \tag{3.8}$$

Таблица 3.6 – **Значения баллов критерия фатальности от реализации угрозы**

Балл	Уровень нарушения безопасности информационной системы					
	нарушение конфиденциальности информации	нарушение доступности информации	нарушение сохранности информации	нарушение целостности и подлинности информации	частичное нарушение функциональной безопасности	выход из строя информационной системы
1	+					
2		+				
			+			
3				+		
4	+			+		
		+		+		
			+	+		
	+	+		+		
		+	+	+		
	+		+	+		
5	+	+	+	+		
6			+		+	
		+			+	
	+				+	
7	+	+			+	
		+	+		+	
	+		+		+	
8	+			+	+	
		+		+	+	
			+	+	+	
	+	+		+	+	
		+	+	+	+	
	+		+	+	+	
9	+	+	+	+	+	
10						+

Используя формулы (3.3), и (3.5)–(3.8) значение уровня защищенности информационной системы от одной из угроз определяется по формуле:

$$Z = \frac{M^6}{C_{\text{уг}} C_{\text{уяз}} C_{\text{СЗИ}}}. \qquad (3.9)$$

Тогда при анализе защищенности информационной системы от нескольких угроз оценка уровня защищенности

$$Z = \frac{NM^{6}}{\sum_{i=1}^{N}\left(C_{\text{УГ}i}C_{\text{УЯЗ}i}C_{\text{СЗИ}i}\right)}. \qquad (3.10)$$

Такой подход позволяет количественно сравнить уровень защищенности информационных систем железнодорожного транспорта при использовании различных систем защиты информации и их комбинаций. При оценке уровня защищенности информационной системы без использования средств защиты информации параметр $C_{\text{СЗИ}}$ в формуле (3.9) и $C_{\text{СЗИ}i}$ в формуле (3.10) следует принять равными 10.

3.4 Модель нарушителя информационной безопасности

Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, технических и материальных средствах и т. д.

Правильно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности. Опираясь на построенную модель, можно строить адекватную систему информационной защиты.

Чаще всего строится неформальная модель нарушителя, отражающая причины и мотивы его действий, возможности, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей: способы реализации исходящих от него угроз, место и характер действия, возможная тактика и т. п. Для достижения поставленных целей нарушитель должен приложить определенные усилия и затратить некоторые ресурсы. Например, модель нарушителя может быть представлена в форме таблицы, которая описывает характеристики некоторого нарушителя (таблица 3.7).

Таблица 3.7 – **Форма представления модели нарушителя информационной безопасности**

Характеристика	Нарушитель
Вычислительная мощность технических средств	
Доступ к интернету, тип каналов доступа	
Финансовые возможности	
Уровень знаний в области IT	
Используемые технологии	
Знания о построении системы защиты объекта	
Преследуемые цели	
Характер действий	
Глубина проникновения	

Определив основные причины нарушений, представляется возможным оказать на них влияние или необходимым образом скорректировать требования к системе защиты от данного типа угроз. При анализе нарушений защиты необходимо уделять внимание субъекту (личности) нарушителя. Устранение причин или мотивов, побудивших к нарушению, в дальнейшем может помочь избежать повторения подобного случая.

Модель может быть не одна, целесообразно построить несколько отличающихся моделей разных типов нарушителей информационной безопасности объекта защиты.

Для построения модели нарушителя используется информация, полученная от служб безопасности и аналитических групп, данные о существующих средствах доступа к информации и ее обработки, о возможных способах перехвата данных на стадиях их передачи, обработки и хранении, данные про обстановку в коллективе и на объекте защиты, сведения о конкурентах и ситуации на рынке, об имевших место свершившихся случаях нарушения информационной безопасности и т. п.

Кроме этого оцениваются реальные оперативные технические возможности нарушителя для воздействия на систему защиты или на защищаемый объект. Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать нарушитель в процессе совершения действий, направленных против системы информационной защиты.

В последнее время модель нарушителя информационной безопасности перестает быть простой формальностью и начинает оказывать большое влияние на перечень актуальных угроз для информационной системы. В перечне угроз для информационной системы для каждой угрозы задан тип и потенциал нарушителя, который может ее реализовать. За счет этого устанавливается взаимосвязь между перечнями угроз и нарушителями информационной безопасности.

Потенциал нарушителя может быть высоким, средним или низким. Для каждого из вариантов задан свой набор возможностей.

Так, нарушители с низким потенциалом могут для реализации атак использовать информацию только из общедоступных источников. К нарушителям с низким потенциалом можно отнести любых внешних лиц, а также внутренний персонал и пользователей информационной системы.

Внешние нарушители, к которым могут относиться и бывшие сотрудники, имеют возможность самостоятельно создавать способы атак, проводить их подготовку и реализацию только за пределами контролируемой зоны. Внутренний персонал имеет возможность проводить атаки в пределах контролируемой зоны с возможным физическим доступом к аппаратным средствам, на которых реализована ИС, в зависимости от величины штатных полномочий.

Нарушители со средним потенциалом имеют возможность проводить анализ кода прикладного программного обеспечения, самостоятельно находить в нем уязвимости и использовать их. К таким нарушителям можно относить террористические и криминальные группы, конкурирующие организации, администраторов системы и разработчиков программного обеспечения (ПО). Эти нарушители имеют возможность привлекать специалистов с опытом разработки и анализа систем комплексной защиты информации (СКЗИ).

Нарушители с высоким потенциалом имеют возможность вносить закладки в программно-техническое обеспечение системы, проводить специальные исследования и применять специальные средства проникновения и добывания информации. К таким нарушителям следует относить только иностранные и отечественные спецслужбы. Они имеют возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (специалисты в области использования атак недокументированных возможностей аппаратного и программного компонентов среды функционирования информационных систем).

Нарушители информационной безопасности бывают внутренними и внешними. Среди внутренних нарушителей в первую очередь можно выделить:

– непосредственных пользователей и операторов информационной системы, в том числе руководителей различных уровней;

– администраторов вычислительных сетей и информационной безопасности;

– прикладных и системных программистов;

– сотрудников службы безопасности;

– технический персонал по обслуживанию зданий и вычислительной техники (от уборщицы до сервисного инженера);

– вспомогательный персонал и временных работников.

Среди причин, побуждающих сотрудников к неправомерным действиям, можно указать:

– безответственность;

– ошибки пользователей и администраторов;

– демонстрацию своего превосходства (самоутверждение);

– «борьбу с системой»;

– корыстные интересы пользователей системы;

– недостатки используемых информационных технологий.

Группу внешних нарушителей могут составлять:

– клиенты;

– приглашенные посетители;

– представители конкурирующих организаций;

– сотрудники органов ведомственного надзора и управления;

– нарушители пропускного режима;

– наблюдатели за пределами охраняемой территории.

Помимо этого классификацию можно проводить по следующим параметрам.

Используемые методы и средства:

– сбор информации и данных;

– пассивные средства перехвата;

– использование средств, входящих в информационную систему или систему ее защиты, и их недостатков;

– активное отслеживание модификаций существующих средств обработки информации, подключение новых средств, использование специализированных утилит, внедрение программных закладок и «черных ходов» в систему, подключение к каналам передачи данных.

Уровень знаний нарушителя относительно организации информационной структуры:

– типовые знания о методах построения вычислительных систем, сетевых протоколов, использование стандартного набора программ;

– высокий уровень знаний сетевых технологий, опыт работы со специализированными программными продуктами и утилитами;

– глубокие знания в области программирования, системного проектирования и эксплуатации вычислительных систем;

– обладание сведениями о средствах и механизмах защиты атакуемой системы;

– нарушитель являлся разработчиком или принимал участие в реализации системы обеспечения информационной безопасности.

Время информационного воздействия:

– в момент обработки информации;

– в момент передачи данных;

– в процессе хранения данных (учитывая рабочее и нерабочее состояния системы).

По месту осуществления воздействия:

– удаленно с использованием перехвата информации, передающейся по каналам передачи данных, или без ее использования;

– доступ на охраняемую территорию;

– непосредственный физический контакт с вычислительной техникой, при этом можно выделить: доступ к рабочим станциям, серверам организации, системам администрирования, контроля и управления информационной системой, программам управления системой обеспечения информационной безопасности.

В таблице 3.8 приведены примеры моделей нарушителей информационной безопасности и их сравнительная характеристика.

Таблица 3.8 – **Сравнительная характеристика нескольких моделей нарушителя**

Характеристика	Хакер-одиночка	Группа хакеров	Конкуренты	Госструктуры, спецподразделения
Вычислительная мощность технических средств	Персональный компьютер	ЛВС, использование чужих вычислительных сетей	Мощные вычислительные сети	Неограниченная вычислительная мощность
Доступ к интернету, тип каналов доступа	Модем или выделенная линия	Использование чужих каналов с высокой пропускной способностью	Собственные каналы с высокой пропускной способностью	Самостоятельный контроль над маршрутизацией трафика в Интернете
Финансовые возможности	Сильно ограничены	Ограничены	Большие возможности	Практически неограниченные
Уровень знаний в области IT	Невысокий	Высокий	Высокий	Высокий, разработчики стандартов
Используемые технологии	Готовые программы, известные уязвимости	Поиск новых уязвимостей, изготовление вредоносных программ	Современные методы проникновения в информационные системы и воздействия на потоки данных в ней	Доскональные знания информационных технологий: возможные уязвимости и недостатки
Знания о построении системы защиты объекта	Недостаточные знания о построении информационной системы	Могут предпринимать усилия для получения представления о принципах функционирования системы защиты	Могут предпринимать усилия для получения представления о принципах функционирования системы защиты, внедрять своего представителя в службу безопасности	В процессе сертификации системы представители госорганов могут получать достаточно полную информацию о ее построении

Окончание таблицы 3.8

Характеристика	Хакер-одиночка	Группа хакеров	Конкуренты	Госструктуры, спецподразделения
Преследуемые цели	Эксперимент	Внесение искажений в работу системы	Блокировка функционирования системы, подрыв имиджа, разорение	Непредсказуемые
Характер действий	Скрытый	Скрытый	Скрытый или открытый демонстративный	Может не утруждать себя сокрытием своих действий
Глубина проникновения	Чаще всего останавливается после первого успешного воздействия	До момента достижения поставленной цели или появления серьезного препятствия	До победного конца	Ничто не способно их остановить

Контрольные вопросы

1 Дайте понятие угрозы безопасности информационной системы.
2 Что является источником угрозы?
3 Перечислите основные группы источников угроз.
4 Дайте понятие уязвимости информационной системы.
5 Перечислите основные классы уязвимостей информационных систем.
6 Дайте понятие атаки на информационную систему.
7 Что такое управление информационными рисками?
8 Дайте понятие риску нарушения безопасности.
9 Что относится к активам организации?
10 Дайте понятие уровню защищенности информационной системы.
11 Приведите классификацию методов оценки эффективности безопасности, основанную на анализе рисков.
12 Что такое функциональная безопасность?
13 Дайте понятие комплексу средств защиты.
14 Что такое модель нарушителя информационной безопасности?

4 МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ФИЗИЧЕСКОМ УРОВНЕ

4.1 Классификация методов защиты информации

Совокупность защитных методов и средств включает в себя программные методы, аппаратные средства, защитные преобразования, а также организационные мероприятия (рисунок 4.1).

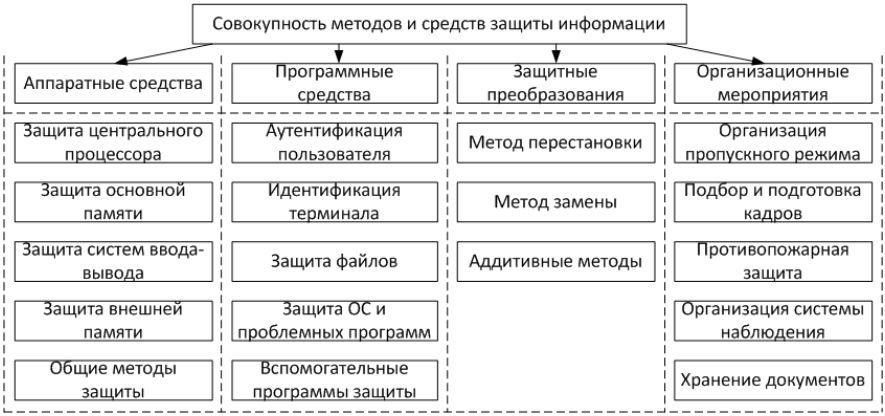

Рисунок 4.1 – Совокупность методов и средств защиты информации

Сущность **аппаратной** или **схемной защиты** состоит в том, что в устройствах и технических средствах обработки информации предусматривается наличие специальных технических решений, обеспечивающих защиту и контроль информации, например экранирующие устройства, локализующие электромагнитные излучения или схемы проверки информации на четность, осуществляющей контроль за правильностью передачи информации между различными устройствами информационной системы.

Программные методы защиты – это совокупность алгоритмов и программ, обеспечивающих разграничение доступа и исключение несанкционированного использования информации.

Сущность **методов защитных преобразований** состоит в том, что информация, хранимая в системе и передаваемая по каналам связи на физи-

ческом уровне модели OSI, представляется в некотором коде, исключающем возможность ее непосредственного использования.

Организационные мероприятия по защите включают в себя совокупность действий по подбору и проверке персонала, участвующего в подготовке и эксплуатации программ и информации, строгое регламентирование процесса разработки и функционирования информационной системы.

Лишь комплексное использование различных защитных мероприятий может обеспечить надежную защиту, так как каждый прием или метод имеет свои слабые и сильные стороны.

Другой возможный вариант классификации методов защиты информации представлен на рисунке 4.2.

Рисунок 4.2 – Классификация методов и средств защиты информации

4.2 Методы защиты информации на физическом уровне модели OSI

Физический уровень модели OSI описывает процессы, происходящие на уровне среды передачи. Информация, обрабатываемая в сетевых устройствах, представлена в дискретном виде и при передаче в зависимости от характеристик среды представляется цифровым сигналом с кодированием и модуляцией. Стандарты физического уровня описывают требования к эле-

ментам среды передачи: кабельной системе, разъемам, виду сигналов и форме импульсов при кодировании и модуляции.

Обеспечить защиту информации на физическом уровне модели OSI можно за счет структуризации физических связей между узлами сети.

Основными угрозами на физическом уровне являются:

– физический доступ к носителям информации;

– угроза оборудованию;

– угроза кабельной системе;

– возможность съема и модификации информации в процессе ее передачи.

Защита носителей информации, сетевых устройств и помещений, в которых они располагаются, от несанкционированного к ним доступа осуществляется за счет использования следующих организационных мероприятий:

– разграничение доступа на территорию организации и в отдельные помещения, в которых располагается сетевое оборудование;

– использование систем аутентификации пользователей при работе с сетевыми устройствами;

– использование системы видеонаблюдения и охранной сигнализации.

При защите кабельной системы наиболее уязвимыми являются сети, построенные по топологии «общая шина» или использующие концентраторы для соединения сетевых устройств, фактически образуя единую среду передачи соответствующую топологии «общая шина». В таких сетях, если нарушитель является одним из пользователей сети, то ему доступен весь сетевой трафик для мониторинга и у него есть возможность управлять процессом передачи информации в сети. Нарушение целостности кабельного сегмента приводит к отказу всей сети.

Если в сети используется звездная или древовидная топология, то нарушение целостности среды одного кабельного сегмента не влияет на работоспособность всей сети. Наиболее уязвимым элементом сети является центральное коммуникационное устройство (коммутатор). Коммутаторы используются для осуществления попеременного доступа узлов к среде передачи. Разделение физической среды передачи между узлами во времени затрудняет прослушивание сети нарушителем и создает дополнительную преграду для осуществления атак отказа в доступе, основанных на широковещательной рассылке.

При наличии у нарушителя физического доступа к системе электропитания сетевых устройств он может вызвать отказ всей сети. Для медных кабельных систем, используемых в качестве среды передачи, опасным является наличие побочного электромагнитного излучения и наводок (ПЭМИН), которые позволяют нарушителю анализировать пики сетевой активности, а при наличии анализатора спектра электромагнитного излучения – осуществить перехват передаваемой информации. При использовании волоконно-

оптических кабелей связи ПЭМИН отсутствует, что существенно затрудняет перехват информации в процессе ее передачи.

Прокладка сетевого кабеля должна осуществляться в скрытой проводке либо в закрываемых кабель-каналах с возможностью опечатывания. Магистральный кабель, выходящий за территорию организации, защитить гораздо сложнее. Для защиты информации от несанкционированного к ней доступа и модификации используются методы криптографического преобразования, а для защиты от повреждения кабеля (нарушение доступности информации) – резервные линии связи.

4.3 Особенности беспроводной среды передачи

Основные проблемы беспроводной среды передачи с точки зрения защиты информации заключаются в невозможность полностью контролировать территорию, на которую распространяется электромагнитное излучения базовых станций и невысокое качество радиоканалов за счет воздействия на них электромагнитных помех и преднамеренного электромагнитного воздействия. **Интенсивность битовых ошибок (Bit Error Rate, BER)** в беспроводных линиях связи может достигать величины 10^{-3} (для сравнения в проводных линиях связи она равна 10^{-9}–10^{-10}).

Для зашиты беспроводных сетей на физическом уровне модели OSI применяется **техника расширения спектра**, которая позволяет повысить помехоустойчивость передаваемых данных для сигналов малой мощности. Выделяют следующие методы расширения спектра сигнала:

– расширение спектра **скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS)**;

– **прямого последовательного расширения спектра (Direct Sequence Spread Spectrum, DSSS)**.

Совместно с FHSS и DSSS дополнительно может использоваться метод **множественного доступа с кодовым разделением (Code Division Multiplexing Access, CDMA)**.

Метод FHSS используется для того, чтобы радиообмен нельзя было перехватить или подавить узкополосным шумом. Для этого радиопередачу производят с постоянной сменой несущей в пределах широкого диапазона частот. Мощность сигнала распределяется по всему выделенному диапазону частот, и прослушивание какой-либо определенной частоты не позволяет прослушивать сигнал целиком.

Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел. Псевдослучайная последовательность зависит от некоторого параметра, который называют начальным числом. Если приемнику и передатчику известны алгоритм и значение начального числа, то они меняют частоты в одинаковой последовательности.

Методы FHSS применяются в беспроводных технологиях IEEE 802.11 (Wi-Fi) и Bluetooth.

В методе DSSS частотный диапазон расширяется за счет того, что каждый бит информации заменяется N битами, поэтому тактовая скорость передачи сигналов увеличивается в N раз. Спектр сигнала также расширяется в N раз.

Цель кодирования методом DSSS та же, что и методом FHSS – повышение помехоустойчивости. Узкополосная помеха будет искажать только определенные частоты спектра сигнала, так что приемник с большой степенью вероятности сможет правильно распознать передаваемую информацию.

Код, которым заменяется двоичная единица исходной информации, называется расширяющей последовательностью. Двоичный нуль кодируется инверсным значением расширяющей последовательности. Приемники должны знать расширяющую последовательность, которую использует передатчик, чтобы понять передаваемую информацию.

Примером расширяющей последовательности является последовательность Баркера, которая состоит из 11 бит. Для двоичной единицы она имеет вид: 10110111000, для нуля – 01001000111.

Последовательность Баркера позволяет приемнику быстро синхронизироваться с передатчиком, то есть надежно выявлять начало последовательности. Приемник определяет такое событие, поочередно сравнивая получаемые биты с образцом последовательности.

Метод CDMA заключается в том, что каждый узел сети задействует собственное значение расширяющей последовательности, которое выбирается так, чтобы принимающий узел мог выделить данные передающего узла из суммарного сигнала, образующегося в результате одновременной передачи информации несколькими узлами.

Каждый узел сети, работающий по методу CDMA, посылает данные в разделяемую среду без какой-либо синхронизации с другими узлами сети. Комбинации расширяющихся последовательностей должны обладать свойством ортогональности, которое необходимо для возможности выделения кода отдельного узла из общего сигнала.

4.4 Криптографические методы защиты информации

Криптология – это наука, изучающая математические методы защиты информации путем ее преобразования. Она разделяется на два направления – криптографию и криптоанализ.

Под **криптографической защитой информации** понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования субъектами, не имеющими на это полномочий.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на следующие группы:

– сжатие или архивация информации;

– кодирование информации;

– шифрование информации;

– стеганография.

В некоторых источниках кодирование и сжатие информации относятся к отраслям знаний, смежных с криптографией, но не входящих в нее.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Эти методы не предназначены для сохранения конфиденциальности информации, основной их целью является сокращение объема информации при хранении или передачи по линиям связи. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

Содержанием процесса **кодирования информации** является замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях автоматизированных систем управления. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Основным видом криптографического преобразования информации в информационных системах является шифрование. Под **шифрованием** понимается процесс преобразования открытой информации в зашифрованную (шифротекст). Процесс преобразования закрытой информации в открытую – **расшифрование.**

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов или двоичных кодов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая шифрованию, и ключ шифрования. **Ключ** – конкретное значение некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор преобразования из семейства. Он содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. **Методом шифрования (шифром)** называется совокупность обратимых преобразований открытой информации в закрытую в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, но некоторые используются и до сих пор. Появление компьютеров инициировало процесс разработки новых шифров, учитывающих их возможности как для шифрования, так и для дешифрования информации **Дешифрованием** называют процесс восстановления первоначального открытого текста на основе шифрованного без знания ключа.

Современные методы шифрования должны соответствовать следующим требованиям:

– стойкость шифра к криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;

– криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;

– шифротекст не должен существенно превосходить по объему исходную информацию;

– ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

– время шифрования не должно быть большим;

– стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифротексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь уязвимостей (скрытых слабых мест), которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации – перебор комбинаций ключа и выполнение алгоритма дешифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

В конце 70-х годов использование ключа длиной в 56 бит гарантировало, что для раскрытия шифра потребуется несколько лет непрерывной работы самых мощных по тем временам компьютеров. Прогресс в области вычислительной техники позволил значительно сократить время определения ключа путем полного перебора.

Эндрю Танненбаум и Джеймс Уэзеролл в своей книге «Компьютерные сети» (5-е издание 2012 года) приводят шуточную классификацию криптостойкости PGP (Pretty Good Privacy – довольно хорошая конфиденциальность) с использованием алгоритма RSA в зависимости от длины ключа шифрования:

1) Несерьезная (384 бит): шифр может быть взломан сегодня же организациями с большим бюджетом.

2) Коммерческая (512 бит): возможно, шифр смогут взломать организации из трех букв.

3) Военная (1024 бит): никто на Земле не сможет взломать этот шифр.

4) Межпланетная (2048 бит): никто во всей Вселенной не сможет взломать шифр.

Современная криптография включает в себя четыре основные группы криптографических методов защиты информации:

– симметричные криптосистемы (криптосистемы с закрытым ключом);

– асимметричные криптосистемы (криптосистемы с открытым ключом);

– системы электронной цифровой подписи;

– системы управления ключами.

В симметричных криптосистемах для шифрования и расшифрования используется один и тот же ключ (рисунок 4.3).

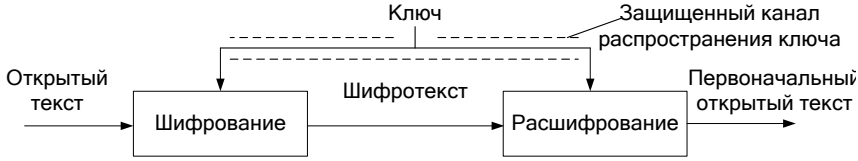

Рисунок 4.3 – Шифрование и расшифрование с одним ключом

К традиционным (классическим) симметричным методам шифрования относятся шифры перестановки, шифры простой и сложной замены, а также некоторые их модификации и комбинации. Комбинации шифров перестановок и шифров замены образуют все многообразие применяемых на практике симметричных шифров.

При шифровании перестановкой символы шифруемого текста переставляются по определенному правилу в пределах блока этого текста. Шифры перестановки являются самыми простыми и самыми древними шифрами.

Одним из самых простых шифров перестановки является шифрующая таблица. В качестве ключа в шифрующих таблицах используются: размер таблицы, слово или фраза, задающие перестановку, особенности структуры таблицы.

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита по одному правилу на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки. Примерами шифров простой замены являются шифр Цезаря и Аффинная система подстановок Цезаря.

Обычно криптоаналитическая атака против системы одноалфавитной замены начинается с подсчета частот появления символов: определяется число появлений каждой буквы в шифротексте. Затем полученное распределение частот букв в шифротексте сравнивается с распределением частот букв в алфавите исходных сообщений. Буква с наивысшей частотой появления в шифротексте заменяется на букву с наивысшей частотой появления в алфавите и т. д. Вероятность успешного вскрытия системы шифрования повышается с увеличением длины шифротекста. Вместе с тем идеи, заложенные в системе шифрования Цезаря, оказались весьма плодотворными, о чем свидетельствуют их многочисленные модификации.

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты. Эффект использования многоалфавитной подстановки заключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исходного алфавита может быть преобразован в несколько различных символов шифровальных алфавитов. Примерами шифров сложной замены являются шифры с использованием таблицы Вижинера и диска Альберти.

Почти все применяемые на практике шифры характеризуются как условно надежные, поскольку они могут быть в принципе раскрыты при наличии неограниченных вычислительных возможностей. Абсолютно надежные шифры нельзя разрушить даже при использовании неограничен-

ных вычислительных возможностей. Это достигается за счет того, что существует единственный такой шифр, применяемый на практике, – одноразовая система шифрования. Характерной особенностью одноразовой системы шифрования является одноразовое использование ключевой последовательности.

Этот шифр абсолютно надежен, если набор используемых им ключей действительно случаен и непредсказуем. Если криптоаналитик попытается использовать для заданного шифротекста все возможные наборы ключей и восстановить все возможные варианты исходного текста, то они все окажутся равновероятными. Теоретически доказано, что одноразовые системы являются недешифрируемыми системами, поскольку их шифротекст не содержит достаточной информации для восстановления открытого текста.

Возможности применения одноразовой системы ограничены чисто практическими аспектами. Существенным моментом является требование одноразового использования случайной ключевой последовательности. Ключевая последовательность с длиной, не меньшей длины сообщения, должна передаваться получателю сообщения заранее или отдельно по некоторому секретному каналу. Такое требование сложно осуществить на практике для современных систем обработки информации, где требуется шифровать в реальном режиме времени с высокими скоростями.

Под гаммированием понимают процесс наложения по определенному закону гаммы шифра на открытые данные. **Гамма шифра** – это псевдослучайная последовательность, выработанная по заданному алгоритму для шифрования открытых данных и расшифрования принятых данных.

Процесс шифрования заключается в генерации гаммы шифра и наложении полученной гаммы на исходный открытый текст обратимым образом, например, с использованием операции сложения по модулю 2.

Перед шифрованием открытые данные разбивают на блоки одинаковой длины (64, 128, 256 и т. д. бит). Гамма шифра вырабатывается в виде последовательности аналогичной длины. Процесс расшифрования сводится к повторной генерации гаммы шифра и наложению этой гаммы на принятые данные.

Получаемый этим методом шифротекст достаточно труден для раскрытия, поскольку теперь ключ является переменным. По сути дела, гамма шифра должна изменяться случайным образом для каждого шифруемого блока. Если период гаммы превышает длину всего шифруемого текста и нарушителю неизвестна никакая часть исходного текста, то такой шифр можно раскрыть только прямым перебором всех вариантов ключа. В этом случае криптостойкость шифра определяется длиной ключа.

Исторически различают шифраторы с внешней и внутренней гаммами. В шифраторах с внешней гаммой в качестве ключа используется случайная последовательность однократного использования, длина которой равна

длине шифруемого сообщения. В шифраторах с внутренней гаммой в качестве ключа применяется многократно используемая случайная последовательность длиной, много меньшей длины шифруемого текста, на основе которой формируется гамма шифра. Шифраторы с внутренней гаммой, т. е. обладающие свойством практической стойкости, в настоящее время являются преобладающими при построении систем шифрованной связи. Основным их достоинством является простота в управлении ключами, т. е. их заготовка, распределение, доставка и уничтожение. Данное преимущество позволяет на основе шифраторов с внутренней гаммой создавать системы шифрованной связи практически любых размеров, не ограничивая их географию и количество абонентов.

Американский стандарт шифрования данных (Data Encryption Standard, DES) опубликован в 1977 г. Национальным бюро стандартов США. Он предназначен для защиты от несанкционированного доступа к важной, но не секретной информации в государственных и коммерческих организациях США.

Основные достоинства алгоритма DES:

– используется только один ключ длиной 56 бит;

– относительная простота алгоритма обеспечивает высокую скорость обработки;

– достаточно высокая стойкость алгоритма.

Алгоритм DES основан на комбинировании методов подстановки и перестановки и состоит из чередующейся последовательности блоков перестановки и подстановки. DES осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значимыми являются 56 бит (остальные 8 бит – проверочные биты для контроля на четность). Расшифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности. Обобщенная схема процесса шифрования в алгоритме DES показана на рисунке 4.4.

Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, в конечной перестановке битов.

Чтобы воспользоваться алгоритмом DES для решения разнообразных криптографических задач, разработаны четыре рабочих режима:

– электронная кодовая книга (Electronic Code Book, ECB);

– сцепление блоков шифра (Cipher Block Chaining, CBC);

– обратная связь по шифротексту (Cipher Feed Back, CFB);

– обратная связь по выходу (Output Feed Back, OFB).

В режиме «Электронная кодовая книга» файл M с данными для шифрования разбивают на 64-битовые отрезки (блоки) : $M = M_1, M_2, ..., M_n$ по 8 байт.

Каждый из этих блоков шифруют независимо от использования одного и того же ключа шифрования (рисунок 4.5). Основное достоинство – простота реализации. Недостаток – относительно слабая устойчивость против квалифицированных криптоаналитиков. Из-за фиксированного характера шифрования при ограниченной длине блока в 64 бита возможно проведение атаки с перебором «по словарю». Блок такого размера может повториться в сообщении вследствие большой избыточности в тексте на естественном языке. Это приводит к тому, что идентичные блоки открытого текста в сообщении будут представлены идентичными блоками шифротекста, что дает криптоаналитику некоторую информацию о содержании сообщения.

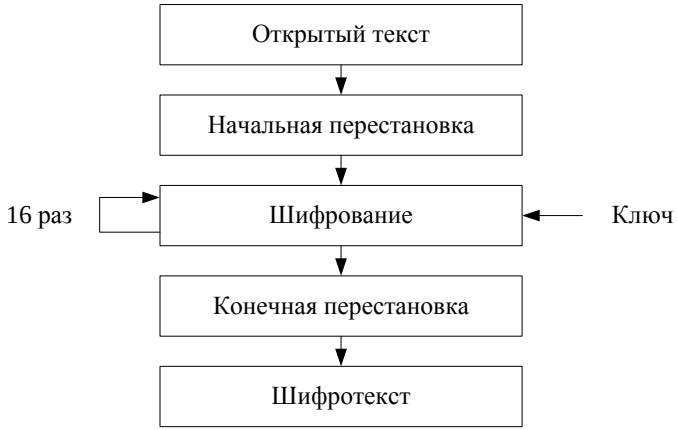

Рисунок 4.4 – Обобщенная схема шифрования в алгоритме DES

В режиме «Сцепление блоков шифра» исходный файл для шифрования разбивается на 64-битовые блоки. Первый блок M_1 складывается по модулю 2 с 64-битовым начальным вектором IV, который меняется ежедневно и держится в секрете (рисунок 4.6). Полученная сумма затем шифруется с использованием ключа DES, известного и отправителю, и получателю информации. Полученный 64-битовый шифр C_1 складывается по модулю 2 со вторым блоком текста, результат шифруется и получается второй 64-битовый шифр C_2 и т. д. Процедура повторяется до тех пор, пока не будут обработаны все блоки текста. Таким образом, для всех $i = 1 \ldots n$ (n – число блоков) результат шифрования C_i определяется следующим образом: $C_i = \text{DES}\,(M_i \oplus C_{i-1})$, где $C_0 = \text{IV}$ – начальное значение шифра, равное начальному вектору (вектору инициализации). Последний 64-битовый блок шифротекста является функцией секретного ключа, начального вектора и каждого бита открытого текста независимо от его длины. Этот блок шифротекста называют кодом аутентификации сообщения (КАС). Код КАС может быть легко проверен получателем, владеющим секретным ключом и начальным вектором, путем

повторения процедуры, выполненной отправителем. Посторонний, однако, не может осуществить генерацию КАС, который воспринялся бы получателем как подлинный, чтобы добавить его к ложному сообщению либо отделить КАС от истинного сообщения для использования его с измененным или ложным сообщением.

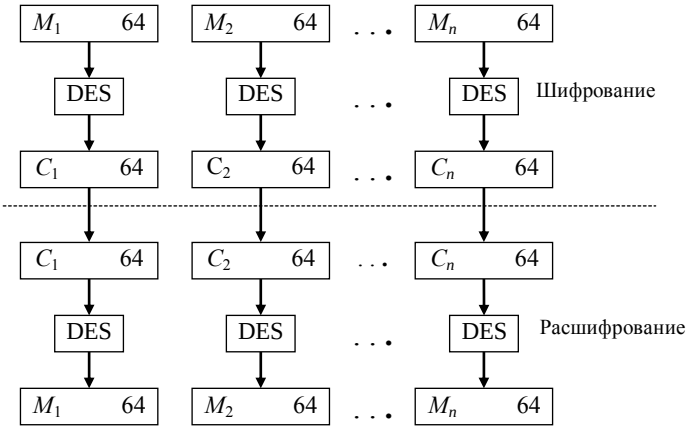

Рисунок 4.5 – Схема алгоритма DES в режиме электронной кодовой книги

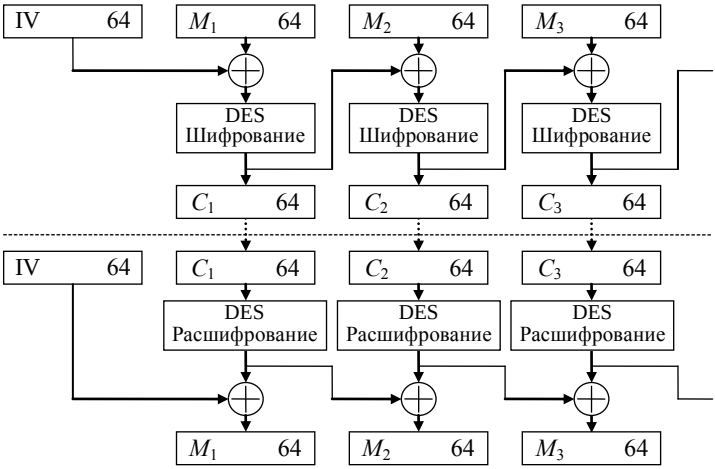

Рисунок 4.6 – Схема алгоритма DES в режиме сцепления блоков шифра

Достоинство данного режима в том, что он не позволяет накапливаться ошибкам при передаче. Блок M_i является функцией только C_{i-1} и C_i. Поэто-

му ошибка при передаче приведет к потере только двух блоков исходного текста.

В режиме «Обратная связь по шифру» размер блока может отличаться от 64 бит. Файл, подлежащий шифрованию (расшифрованию), считывается последовательными блоками длиной k битов (k = 1, …, 64). Входной блок (64-битовый регистр сдвига) в начале содержит вектор инициализации, выровненный по правому краю.

Режим «Обратная связь по выходу» тоже использует переменный размер блока и сдвиговый регистр, инициализируемый так же, как и в предыдущем режиме, а именно – входной блок в начале содержит вектор инициализации IV, выровненный по правому краю.

В **асимметричных криптосистемах** используются два ключа – открытый и секретный, которые математически связаны друг с другом (рисунок 4.7). Информация шифруется с помощью открытого ключ, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

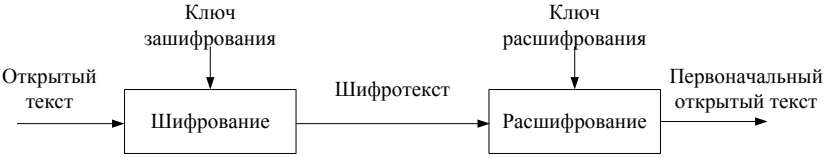

Рисунок 4.7 – Шифрование и расшифрование с двумя ключами

Алгоритм RSA предложили в 1978 г. три автора: Рональд Рин Ривест, Ади Шамир и Леонард Макс Адлеман. Алгоритм получил свое название по первым буквам фамилий его авторов.

Надежность алгоритма основывается на трудности факторизации больших чисел в произведение простых множителей. В криптосистеме RSA открытый ключ $K_в$, секретный ключ $k_в$, сообщение M и криптограмма C принадлежат множеству целых чисел Z_N = {0, 1, 2, ..., N – 1}, где N – модуль, $N = PQ$. Здесь P и Q – случайные большие простые числа. Для обеспечения максимальной безопасности выбирают P и Q равной длины и хранят в секрете. Множество Z_N с операциями сложения и умножения по модулю N образует арифметику по модулю N. Открытый ключ $K_в$ выбирают случайным образом так, чтобы выполнялись условия: $1 < K_в \le \varphi(N)$, НОД($K_в$, $\varphi(N)$) = 1, $\varphi(N) = (P - 1)(Q - 1)$, где $\varphi(N)$ – функция Эйлера. Второе из указанных выше условий означает, что открытый ключ $K_в$ и значение функции Эйлера $\varphi(N)$ должны быть взаимно простыми. Далее, используя расширенный алгоритм Евклида, вычисляют секретный ключ

$$k_в K_в \equiv 1 \ [\mathrm{mod}\ \varphi(N)] \text{ или } k_в = K_в^{-1} \ [\mathrm{mod}(P - 1)(Q - 1)]. \qquad (4.1)$$

Это можно осуществить, так как при известной паре простых чисел (P, Q) можно легко найти $\varphi(N)$. $k_в$ и N должны быть взаимно простыми. Открытый ключ $K_в$ используют для шифрования данных, а секретный ключ $k_в$ – для расшифрования.

Преобразование шифрования определяет криптограмму C через пару «открытый ключ $K_в$, сообщение M» в соответствии со следующей формулой:

$$C = E_{K_в}(M) = E_в(M) = M^{K_в} \pmod N. \qquad (4.2)$$

В качестве алгоритма быстрого вычисления значения C используют ряд последовательных возведений в квадрат целого M и умножений на M с приведением по модулю N.

Обращение функции $C = M^{K_в} \pmod N$, т. е. определение значения M по известным значениям C, $K_в$ и N, практически не осуществимо при $N \approx 2^{512}$. Однако обратную задачу, т. е. задачу расшифрования криптограммы C, можно решить, используя пару «секретный ключ $k_в$, криптограмма C» по следующей формуле:

$$M = D_{K_в}(C) = D_в(C) = C^{k_в} \pmod N. \qquad (4.3)$$

Подставляя в это уравнение значение C, получаем

$$\left(M^{K_в}\right)^{k_в} = M \pmod N \text{ или } M^{K_в k_в} = M \pmod N. \qquad (4.4)$$

Сопоставляя это выражение с формулой расшифрования, получаем $K_в k_в = n\,\varphi(N) + 1$ или, что то же самое, $K_в k_в \equiv 1[\mathrm{mod}\ \varphi(N)]$.

Следовательно, если криптограмму $C = M^{K_в} \pmod N$ возвести в степень $k_в$, то в результате восстанавливается исходный открытый текст M, так как

$$\left(M^{K_в}\right)^{k_в} = M^{K_в k_в} = M^{n\varphi(N)+1} \equiv M \pmod N. \qquad (4.5)$$

Таким образом, получатель, который создает криптосистему, защищает два параметра: секретный ключ $k_в$ и пару чисел (P, Q), произведение которых дает значение модуля N. С другой стороны, отправителю известны значения модуля N и открытого ключа $K_в$. Противнику известны лишь значения $K_в$ и N. Если бы он смог разложить число N на множители P и Q, то он узнал бы тройку чисел $\{P, Q, K_в\}$, вычислил бы значение функции Эйлера $\varphi(N) = (P-1)(Q-1)$ и определил значение секретного ключа $k_в$.

Разложение очень большого N на множители вычислительно не осуществимо, при условии, что длины выбранных P и Q составляют не менее 100 десятичных знаков.

Чтобы алгоритм RSA имел практическую ценность, необходимо иметь возможность без существенных затрат генерировать большие простые числа, уметь оперативно вычислять значения ключей $K_в$ и $k_в$.

Криптосистемы RSA реализуются как аппаратным, так и программным путем. Для аппаратной реализации операций шифрования и расшифрования RSA разработаны специальные процессоры. Аппаратная реализация RSA примерно в 1000 раз медленнее аппаратной реализации симметричного криптоалгоритма DES. Программная реализация RSA примерно в 100 раз медленнее программной реализации DES. С развитием технологии эти оценки могут несколько изменяться, но асимметричная криптосистема RSA никогда не достигнет быстродействия симметричных криптосистем. Малое быстродействие криптосистем RSA ограничивает область их применения, но не уменьшает их ценность.

Схема Эль Гамаля, предложенная в 1985 г., может быть использована как для шифрования, так и для цифровых подписей. Безопасность схемы Эль Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

Для того чтобы генерировать пару ключей (открытый ключ – секретный ключ), сначала выбирают некоторое большое простое число P и большое целое число G, причем $G < P$. Числа P и G могут быть распространены среди группы пользователей. Затем выбирают ключ X – случайное целое число, причем $X < P$. Число X является секретным ключом и должно храниться в секрете. Далее вычисляют $Y = G^X \bmod P$. Число Y является открытым ключом.

Для того чтобы зашифровать сообщение M, выбирают случайное целое число $1 < K < P - 1$, такое, что числа K и $(P - 1)$ являются взаимно простыми. Затем вычисляют числа $a = G^K \bmod P$, $b = Y^K M \bmod P$. Пара чисел (a, b) является шифротекстом. Длина шифротекста вдвое больше длины исходного открытого текста M.

Для того чтобы расшифровать шифротекст (a, b), вычисляют

$$M = b/a^X \bmod P. \tag{4.6}$$

В реальных схемах шифрования необходимо использовать в качестве модуля P большое целое простое число, имеющее в двоичном представлении длину от 512 до 1024 бит.

Главным достоинством криптосистем с открытым ключом является их потенциально высокая безопасность: нет необходимости ни передавать, ни сообщать кому бы то ни было значения секретных ключей, ни убеждаться в их подлинности. В симметричных криптосистемах существует опасность раскрытия секретного ключа во время передачи. Однако алгоритмы, лежащие в основе криптосистем с открытым ключом, имеют следующие недостатки:

– генерация новых секретных и открытых ключей основана на генерации

новых больших простых чисел, а проверка простоты чисел занимает много процессорного времени;

– процедуры шифрования и расшифрования, связанные с возведением в степень многозначного числа, достаточно громоздки.

Именно поэтому быстродействие криптосистем с открытым ключом обычно в сотни и более раз меньше быстродействия симметричных криптосистем с секретным ключом.

Комбинированный (гибридный) метод шифрования позволяет сочетать преимущества высокой секретности, присущие асимметричным криптосистемам с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом. При таком подходе криптосистема с открытым ключом применяется для шифрования, передачи и последующего расшифрования только секретного ключа симметричной криптосистемы. А симметричная криптосистема применяется для шифрования и передачи исходного открытого текста. В результате криптосистема с открытым ключом не заменяет симметричную криптосистему с секретным ключом, а лишь дополняет ее, позволяя повысить в целом защищенность передаваемой информации. Такой подход иногда называют схемой электронного цифрового конверта.

Если пользователь *A* хочет передать зашифрованное комбинированным методом сообщение *M* пользователю *B*, то порядок его действий будет таков:

1 Создать (например, сгенерировать случайным образом) симметричный ключ, называемый в этом методе сеансовым ключом $K_с$.

2 Зашифровать сообщение *M* на сеансовом ключе $K_с$.

3 Зашифровать сеансовый ключ $K_с$ на открытом ключе $K_в$ пользователя *B*.

4 Передать по открытому каналу связи в адрес пользователя *B* зашифрованное сообщение вместе с зашифрованным сеансовым ключом.

Действия пользователя *B* при получении зашифрованного сообщения и зашифрованного сеансового ключа должны быть обратными:

1 Расшифровать на своем секретном ключе $k_в$ сеансовый ключ $K_с$.

2 С помощью полученного сеансового ключа $K_с$ расшифровать и прочитать сообщение *M*.

При использовании комбинированного метода шифрования можно быть уверенным в том, что только пользователь *B* сможет правильно расшифровать ключ $K_с$ и прочитать сообщение *M*.

Комбинированный метод шифрования является наиболее рациональным, объединяя в себе высокое быстродействие симметричного шифрования и высокую криптостойкость, гарантируемую системами с открытым ключом.

Электронной цифровой подписью (**ЭЦП**) называется присоединение к тексту его криптографического преобразования, которое позволяет при по-

лучении текста другим пользователем проверить авторство и целостность сообщения.

При обмене электронными документами по сети связи возникает проблема аутентификации автора документа и самого документа, т. е. установления подлинности автора и отсутствия изменений в полученном документе. В обычной (бумажной) информатике эти проблемы решаются за счет того, что информация в документе и рукописная подпись автора жестко связаны с физическим носителем (бумагой). В электронных документах такой связи нет.

ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает ее основными достоинствами:

– удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

– не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;

– гарантирует целостность подписанного текста.

Цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом. Система ЭЦП включает две процедуры: 1) постановки подписи; 2) проверки подписи. В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя.

При формировании ЭЦП отправитель прежде всего вычисляет хэш-функцию $h(M)$ подписываемого текста M. Вычисленное значение хэш-функции $h(M)$ представляет собой один короткий блок информации m, характеризующий весь текст M в целом. Хэш-функция предназначена для сжатия подписываемого документа M до нескольких десятков или сотен бит. Хэш-функция $h(M)$ принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение $h(M) = m$ фиксированной длины. Обычно хэшированная информация является сжатым двоичным представлением основного сообщения произвольной длины. Значение хэш-функции $h(M)$ сложным образом зависит от документа M и не позволяет восстановить сам документ M.

Затем число m шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного текста M.

При проверке ЭЦП получатель сообщения снова вычисляет хэш-функцию $m = h(M)$ принятого по каналу сообщения M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции.

Функция $h(M)$ является хэш-функцией, если она удовлетворяет следующим условиям:

– исходный текст может быть произвольной длины;

– само значение $h(M)$ имеет фиксированную длину;

– значение функции $h(M)$ легко вычисляется для любого аргумента;

– восстановить аргумент по значению с вычислительной точки зрения – практически невозможно;

– функция $h(M)$ – однозначна.

Из определения следует, что для любой хэш-функции есть тексты-близнецы, имеющие одинаковое значение хэш-функции, так как мощность множества аргументов неограниченно больше мощности множества значений. Такой факт получил название «эффект дня рождения».

Наиболее известные из хэш-функций – Message Digest Algorithm разных версий (MD2, MD4, MD5) и Secure Hash Algorithm (SHA).

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей. Каждая подпись содержит следующую информацию:

– дату подписи;

– срок окончания действия ключа данной подписи;

– информацию о лице, подписавшем файл (Ф. И. О., должность, краткое наименование фирмы);

– идентификатор подписавшего (имя открытого ключа);

– собственно цифровую подпись.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа. Иначе говоря, открытый ключ является необходимым инструментом, позволяющим проверить подлинность электронного документа и автора подписи. Открытый ключ не позволяет вычислить секретный ключ.

Для генерации пары ключей (секретного и открытого) в алгоритмах ЭЦП, как и в асимметричных системах шифрования, используются разные математические схемы, основанные на применении однонаправленных функций. Эти схемы разделяются на две группы. В основе такого разделения лежат известные сложные вычислительные задачи:

– факторизации (разложения на множители) больших целых чисел;

– дискретного логарифмирования.

Управление ключами – это процесс системы обработки информации, вырабатывающий и распределяющий ключи (открытые и секретные) между пользователями.

Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в системе, где количество пользователей составляет десятки и сотни управление ключами – это серьезная проблема.

Под ключевой информацией понимается совокупность всех действующих в системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации.

Управление ключами включает в себя три элемента:

– генерацию ключей;

– накопление ключей;

– распределение ключей.

В реальных системах используются специальные аппаратные и программные методы генерации случайных ключей. Как правило, используют датчики случайных чисел. Однако степень случайности их генерации должна быть достаточно высокой. Идеальными генераторами являются устройства на основе «натуральных» случайных процессов. Например, генерация ключей на основе белого радиошума. Другим случайным математическим объектом являются десятичные знаки иррациональных чисел, например π или e, которые вычисляются с помощью стандартных математических методов.

В системах со средними требованиями защищенности вполне приемлемы программные генераторы ключей, которые вычисляют случайные числа как сложную функцию от текущего времени и (или) числа, введенного пользователем.

Под накоплением ключей понимается организация их хранения, учета и удаления. Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей следует уделять особое внимание.

Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован.

В достаточно сложной системе один пользователь может работать с большим объемом ключевой информации, и иногда даже возникает необходимость организации мини-баз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей.

Каждая информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие информацию о ключах, называются мастер-ключами. Желательно, чтобы мастер-ключи каждый пользователь знал наизусть и не хранил их вообще на каких-либо материальных носителях.

Очень важным условием безопасности информации является периодическое обновление ключевой информации в системе. При этом переназначаться должны как обычные ключи, так и мастер-ключи. В особо ответственных системах обновление ключевой информации необходимо производить ежедневно.

Вопрос обновления ключевой информации связан и с третьим элементом управления ключами – распределением ключей.

Распределение ключей – самый ответственный процесс в управлении ключами. К нему предъявляются два требования:

– оперативность и точность распределения;

– скрытность распределяемых ключей.

В последнее время заметен сдвиг в сторону использования криптосистем с открытым ключом, в которых проблема распределения отпадает. Тем не менее распределение ключевой информации в системе требует новых эффективных решений.

Распределение ключей между пользователями реализуется двумя разными подходами:

1 Путем создания одного или нескольких центров распределения ключей. Недостаток такого подхода состоит в том, что в центре распределения известно, кому и какие ключи назначены, и это позволяет читать все сообщения, циркулирующие в системе. Возможные злоупотребления существенно влияют на защиту.

2 Прямой обмен ключами между пользователями системы. В этом случае проблема состоит в том, чтобы надежно удостоверить подлинность субъектов.

Для распределения ключей весьма эффективным оказался алгоритм Диффи – Хелмана, позволяющий двум пользователям без посредников обменяться ключом, который может быть использован затем для симметричного шифрования.

В отличие от других методов криптографического преобразования информации, методы **стеганографии** позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в компьютерных системах открыла практически

неограниченные возможности перед стеганографией. Графическая и звуковая информации представляются в числовом виде.

В графических объектах наименьший элемент изображения (пиксель) может, для примера, кодироваться тремя байтами (по одному байту на канал интенсивности красного, зеленого и синего цветов в формате RGB). Биты двух младших разрядов каждого из байтов можно произвольно изменять без существенного искажения исходного изображения (полученные при таких изменениях искажения не доступны человеческому глазу).

Полный текст романа Льва Николаевича Толстого «Война и мир» содержит чуть менее 3600000 символов с учетом пробелов. Используя сжатие информации и последующее шифрование, текст этого романа можно представить объемом 1400000 байт. При сокрытии 6 бит информации в один пиксель для этого романа понадобится 1866667 пикселей, которые умещаются в изображении размером 1600 на 1200 пикселей.

С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Контрольные вопросы

1 Что относится к методам аппаратной защиты информации?

2 Что относится к методам программной защиты информации?

3 По каким критериям производится классификация методов и средств защиты информации?

4 Какие основные методы защиты информации используются на физическом уровне модели OSI?

5 В чем заключается метод скачкообразной перестройки в радиоканалах?

6 В чем заключается метод прямого последовательного расширения спектра в радиоканалах?

7 В чем заключается метод множественного доступа с кодовым разделением каналов?

8 Какие методы преобразования информации относятся к криптографическим?

9 Что такое шифрование информации?

10 Какие требования предъявляются к современным методам шифрования?

11 Опишите процесс симметричного шифрования информации.

12 Опишите процесс асимметричного шифрования информации.

13 Для каких целей используется электронная цифровая подпись?

14 Что такое стеганография?

5 ТЕХНОЛОГИИ КАНАЛЬНОГО УРОВНЯ

5.1 Технология Ethernet

Технология Ethernet была изобретена 22 мая 1973 года Робертом Меткалфом. В настоящее время она является наиболее распространенной технологией, которая используется на канальном уровне как в локальных, так и в глобальных проводных сетях. Хотя, те технологии, которые сейчас называются технологиями Ethernet, далеко продвинулись по сравнению с первоначальной технологией Ethernet. До середины 2000-х годов она применялась исключительно в локальных сетях. Еще раньше, до 80-х годов прошлого века в этой технологии использовалась разделяемая среда – как удобное и экономичное средство объединения компьютеров на физическом уровне. С середины 90-х стали применяться коммутируемые версии технологии. Преимуществом коммутируемых локальных сетей является возможность логической структуризации сети с разделением ее на отдельные сегменты, называемые виртуальными локальными сетями. Успех Ethernet в локальных сетях привел к тому, что стало целесообразным ее применение и в глобальных сетях. В результате появилась версия Ethernet операторского класса (Carrier Grade Ethernet).

Технология Ethernet регламентируется стандартом IEEE 802.3, в соответствии с которым для нее выделены три функциональных уровня, вписывающихся в уровни модели OSI (рисунок 5.1):

– физический уровень, который полностью соответствует определению физического уровня модели OSI;

– уровень доступа к среде (Media Access Control, MAC) предоставляет сетевому устройству доступ к разделяемой среде и обеспечивает доставку кадра к узлу назначения в соответствии с его адресом;

– уровень управления логическим каналом (Logical Link Control, LLC) обеспечивает надежную доставку кадра от источника к приемнику в сети Ethernet.

На уровне LLC определено три типа услуг:

1 Услуга LLC1 – услуга без установления соединения и без подтверждения получения данных.

2 Услуга LLC2 – услуга, позволяющая пользователю установить логическое соединение перед началом передачи любого блока данных и, если это

требуется, выполнить процедуры восстановления после ошибок и упорядочивание потока блоков в рамках установленного соединения.

3 Услуга LLC3 – услуга без установления соединения, но с подтверждением получения данных.

Выбор режима работы уровня LLC зависит от требований протокола верхнего уровня. Для технологии Ethernet изначально был заложен и поддерживается в настоящее время наиболее простой дейтаграммный режим, который формально является режимом LLC1.

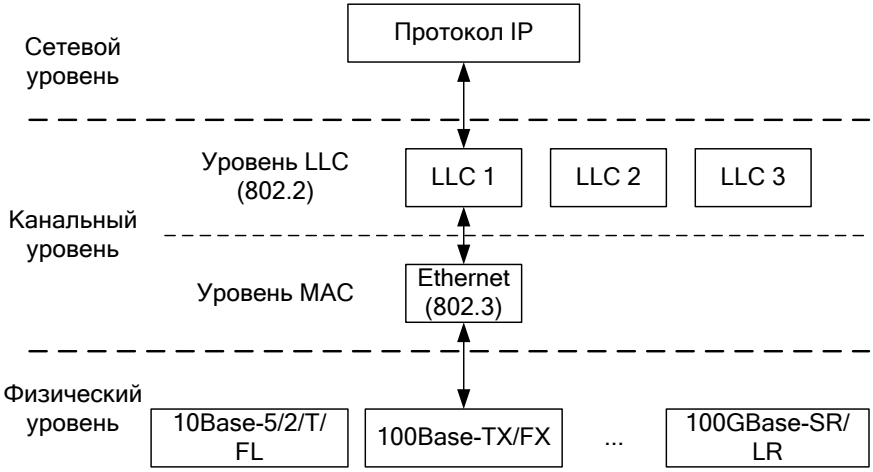

Рисунок 5.1 – Функциональные уровни технологии Ethernet

PDU, используемые в технологии Ethernet, называются **кадрами**. Формат кадра технологии Ethernet представлен на рисунке 5.2.

Название поля	Preamble	SFD	DA	SA	L/T	Data	FCS
Размер, байт	7	1	6	6	2	46 - 1500	4

Рисунок 5.2 – Формат кадра технологии Ethernet

Поля, представленные на рисунке 5.2, имеют следующее назначение:

– **Preamble** – преамбула используется в качестве синхронизирующей последовательности для интерфейсных цепей и способствует декодированию битов (семь раз повторяется комбинация 10101010);

– **SFD** (**Start-Frame Delimiter**) – разделитель начала кадра, состоящий из одного байта (10101011), который указывает на начало полезной информации после него;

– **DA** (**Destination Address**) – адрес узла назначения;

– **SA** (**Source Address**) – адрес узла отправителя (для доставки кадра достаточно адреса назначения, а адрес источника помещается в кадр для того, чтобы узел, получивший кадр, знал, от кого пришел кадр и кому нужно на него ответить в случае поступления с сетевого уровня соответствующего указания);

– **L** (**Length**) – длина поля данных в байтах;

– **T** (**Type**, **EtherType**) – условный код протокола верхнего уровня (используется в DIX Ethernet, встречается гораздо чаще), данные которого находятся в поле данных кадра (требуется для поддержки интерфейсных функций мультиплексирования и демультиплексирования кадров при взаимодействии с протоколами верхних уровней);

– **Data** может содержать от 46 до 1500 байт данных, поступивших от сетевого уровня (если длина данных меньше 46 байт, то это поле дополняется до минимального размера байтами заполнения);

– **FCS** (**Frame Check Sequence**) – поле контрольной последовательности кадра состоит из 4 байт контрольной суммы, которая вычисляется по алгоритму CRC-32.

В настоящее время существуют следующие разновидности технологии Ethernet:

– Ethernet (10 Мбит/с);

– Fast Ethernet (100 Мбит/с);

– Gigabit Ethernet (1 Гбит/с);

– 10G Ethernet (10 Гбит/с);

– 100G и 40G Ethernet (100 и 40 Гбит/с соответственно);

– 400G, 200G и 50G Ethernet (400, 200 и 50 Гбит/с соответственно).

5.2 Локальные адреса

Уровень MAC дал название адресам сети Ethernet (MAC-адреса). В технологии Ethernet используются уникальные 6-байтовые адреса. Обычно MAC-адрес записывают в виде шести пар шестнадцатеричных цифр, разделенных дефисами или двоеточиями, например, EC-8C-9A-42-87-20. Каждый сетевой адаптер имеет, по крайней мере, один MAC-адрес.

Помимо отдельных интерфейсов, MAC-адрес может определять группу интерфейсов и даже все интерфейсы сети. Первый (младший) бит старшего байта адреса назначения – это признак того, является адрес индивидуальным или групповым. Если он равен 0, то адрес является индивидуальным, то есть идентифицирует один сетевой интерфейс, а если 1, то групповым (рисунок 25), который связан только с интерфейсами, сконфигурированными как члены группы, номер которой указан в групповом адресе. Если сетевой интерфейс включен в группу, то, наряду с уникальным MAC-адресом, с

ним ассоциируется еще один адрес – групповой. В частном случае, если групповой адрес состоит из всех единиц (FF-FF-FF-FF-FF-FF), то он идентифицирует все узлы сети и называется широковещательным.

Второй бит старшего байта адреса определяет способ назначения адреса. Если этот бит равен 0 (что бывает почти всегда в стандартной аппаратуре Ethernet), то это говорит о том, что адрес назначен централизованно по правилам IEEE 802 (рисунок 5.3). Иначе адрес является локальным.

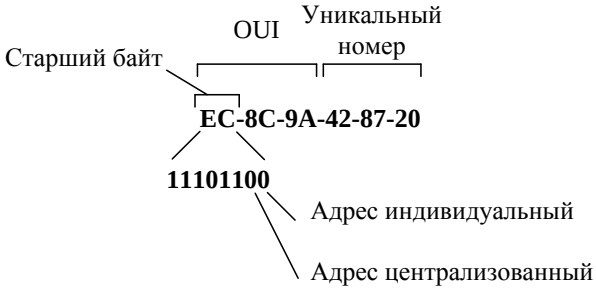

Рисунок 5.3 – Формат MAC-адреса

Уникальность централизованно распределяемых адресов распространяется на все основные технологии локальных сетей. Локальные адреса назначаются администратором сети, в обязанности которого входит обеспечение их уникальности.

Комитет IEEE распределяет между производителями оборудования так называемые организационно уникальные идентификаторы (**Organizationally Unique Identifier**, **OUI**). Каждый производитель помещает выделенный ему идентификатор в три старших байта адреса. За уникальность младших трех байтов адреса отвечает производитель оборудования.

5.3 Разделяемая среда передачи и борьба с коллизиями

Разделение среды передачи – это процесс распределения одного широковещательного канала между многочисленными пользователями, претендующими на него.

Канал может представлять собой часть беспроводного спектра, распространяемого на некоторой территории или один проводной канал, к которому присоединено несколько узлов. Такой канал соединяет каждого пользователя со всеми остальными пользователями, и любой из них, полностью нагружающий канал, мешает другим передавать данные. В таких условиях при передаче информации несколькими источниками одновременно часто происходят коллизии.

Коллизия – это одновременная передача двумя или более источниками кадров в общую распределяемую среду передачи. Коллизия – это нормальная ситуация в работе сетей Ethernet.

Существуют статические и динамические способы распределения общего канала. К статическим способам относятся:

– системы с частотным уплотнением (Frequency Division Multiplexing, FDM);

– системы с временным уплотнением (Time Division Multiplexing, TDM);

– системы со спектральным уплотнением (Wave Division Multiplexing, WDM).

К динамическим способам распределения общего канала относятся:

– система ALOHA (чистая и дискретная);

– системы с множественным доступом и контролем несущей (Carrier-Sense Multiple Access, CSMA);

– протоколы без столкновений (битовая карта, передача маркера и т. п.)

В сетях Ethernet на разделяемой проводной среде используется метод доступа **CSMA/CD** (**Carrier Sense Multiple Access with Collision Detection**) – прослушивание несущей частоты с множественным доступом и распознаванием коллизий. Алгоритм процесса передачи данных сетевым устройством по протоколу CSMA/CD представлен на рисунке 5.4.

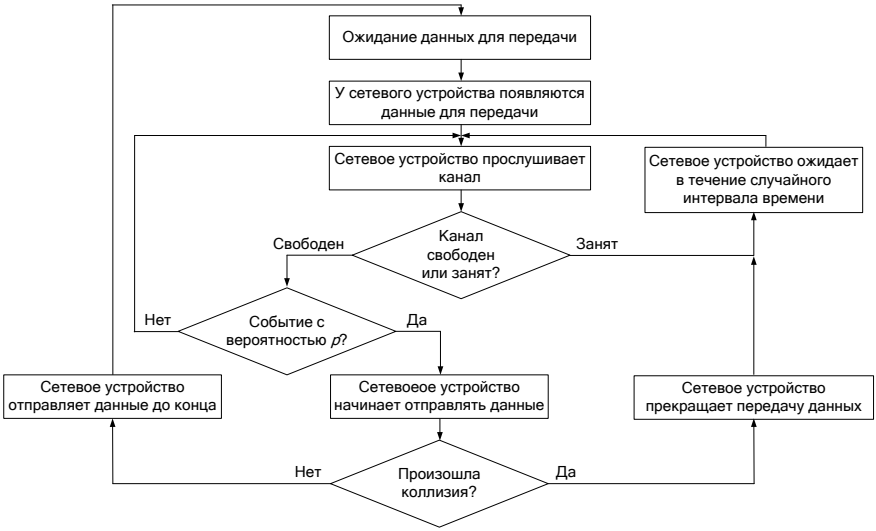

Рисунок 5.4 – Алгоритм процесса передачи данных сетевым устройством по протоколу CSMA/CD

Все сетевые устройства в сети на разделяемой среде имеют возможность немедленно получить данные, передаваемые любым из компьютеров в общую среду, которая работает в режиме коллективного доступа (**Multiply Access, MA**). Чтобы получить возможность передавать кадр, источник должен убедиться, что разделяемая среда свободна. Это достигается прослушиванием основной гармоники сигнала, которая еще называется несущей частотой (**Carrier Sense, CS**). Признаком «незанятости» среды является отсутствие на ней несущей частоты, которая при манчестерском способе кодирования и тактовой частоте 10 МГц равна 5-10 МГц в зависимости от последовательности единиц и нулей, передаваемых в данный момент.

После окончания передачи кадра все узлы сети обязаны выдержать технологическую паузу, равную межпакетному интервалу (**Inter Packet Gap, IPG**) в 9,6 мкс. Эта пауза нужна для приведения сетевых адаптеров в исходное состояние, а также для предотвращения монопольного захвата среды одним сетевым устройством. После окончания технологической паузы прочие сетевые устройства имеют право начать передачу своего кадра, так как среда свободна.

5.4 Беспроводные локальные и персональные сети

В **беспроводных локальных сетях** (**Wireless Local Area Network, WLAN**) сигнал распространяется с помощью электромагнитных волн высокой частоты. Современные беспроводные локальные сети позволяют передавать данные на скоростях до нескольких гигабит в секунду.

Преимущество беспроводных локальных сетей заключается в том, что их проще разворачивать и модифицировать, а также в том, что эти сети обеспечивают мобильность пользователей.

Недостатками беспроводных локальных сетей являются подверженность помехам от разнообразных бытовых приборов и других телекоммуникационных систем, кроме того помехи могут быть атмосферными.

Неравномерное распределение интенсивности сигнала приводит не только к битовым ошибкам передаваемой информации, но и к неопределенности зоны покрытия беспроводной локальной сети. Беспроводная локальная сеть не имеет точной области покрытия. В связи с этим в беспроводной локальной сети может возникнуть одна из двух проблем:

– скрытого сетевого устройства (рисунок 5.5);

– засвеченного сетевого устройства (рисунок 5.6).

Проблема скрытого сетевого устройства возникает, если два сетевых устройства находятся в зоне недосягаемости друг друга (*A* и *C* на рисунке 5.5), но существует третье сетевое устройство – *B*, которое принимает сигналы как от *A*, так и от *C*. При передаче информации от *A* к *B* сетевое устройство *C* «видит», что среда свободна, и начинает передавать свой кадр

сетевому устройству *B*. В результате сигналы в районе сетевого устройства В исказятся, то есть произойдет коллизия.

При проблеме засвеченного сетевого устройства *B* передает данные *A*, в это время сетевое устройство *C* решает связаться с *D*, но, проверив среду, решает, что она занята, хотя на самом деле сетевое устройство *D* доступно.

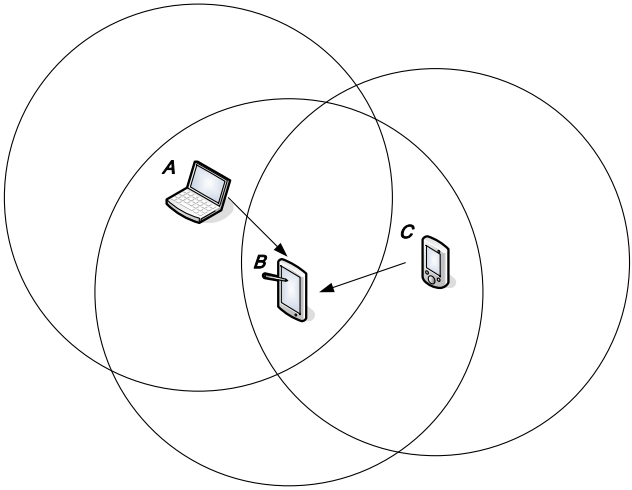

Рисунок 5.5 – Проблема скрытого сетевого устройства

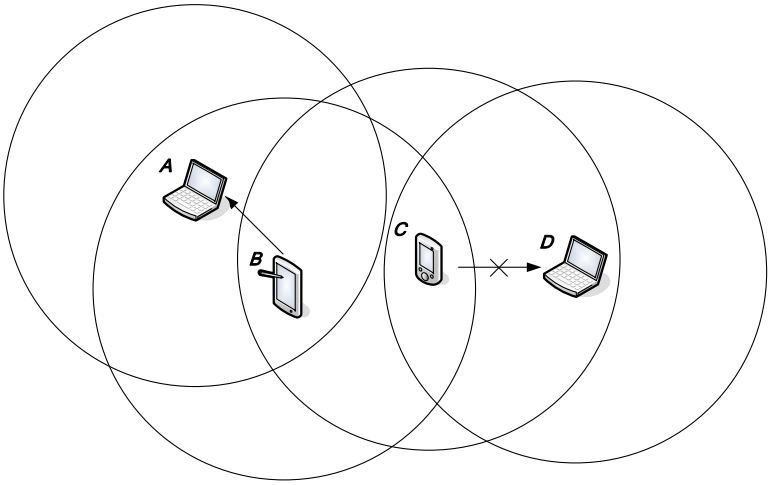

Рисунок 5.6 – Проблема засвеченного сетевого устройства

Если для проводной линии связи (протокол CSMA/CD) занятость на выходном интерфейсе передающего сетевого устройства действительно означает занятость сетевого устройства-получателя, то для беспроводной сети это не так.

Поэтому в беспроводных локальных сетях применяется другой алгоритм доступа, основанный на методе простоя источника: сетевое устройство, передавшее кадр, должно дождаться подтверждения о его получении от сетевого устройства-получателя и только после этого посылать следующий кадр. Если подтверждение не приходит в течение заданного интервала времени, то считается, что кадр был потерян в результате коллизии, и узел передает копию этого кадра. Такой метод доступа называется **CSMA/CA** (**Carrier Sense Multiple Access with Collision Avoidance**) – прослушивание несущей частоты с множественным доступом и предотвращением коллизий. Алгоритм процесса передачи данных сетевым устройством по протоколу CSMA/CA представлен на рисунке 5.7.

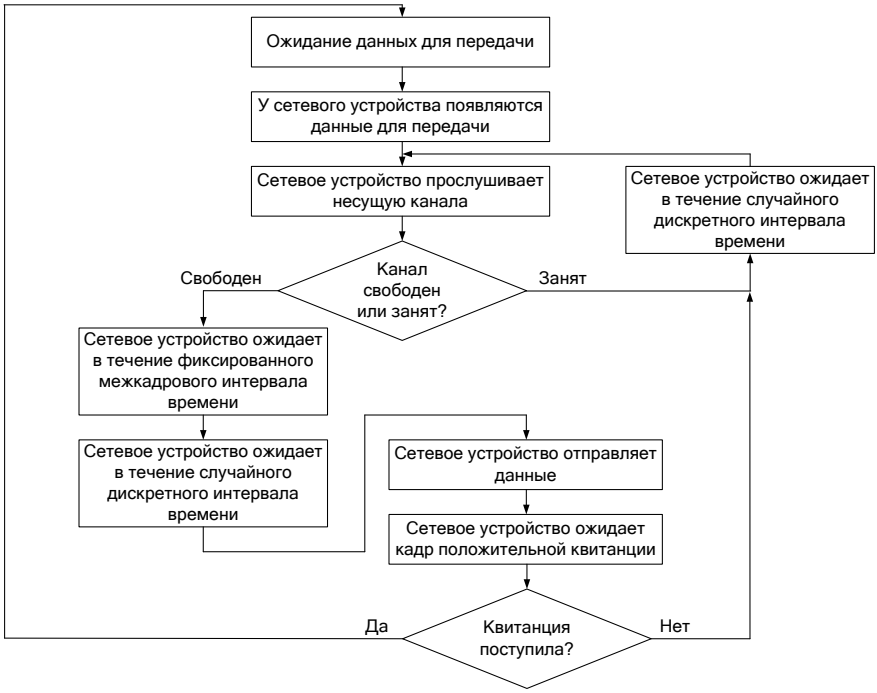

Рисунок 5.7 – Алгоритм процесса передачи данных сетевым устройством по протоколу CSMA/CA

Сети и оборудование стандарта IEEE 802.11, также известные под названием Wi-Fi (Wireless Fidelity) занимают лидирующие позиции в мире беспроводных локальных сетей. Стандарт 802.11 определяет в качестве основного структурного элемента WLAN **сеть с базовым набором услуг** (**Basic Service Set**, **BSS**). BSS представляет собой набор беспроводных сетевых устройств, разделяющих среду передачи и работающих с одинаковыми характеристиками доступа к среде: частота и схема модуляции сигналов.

Сети BSS могут быть объединены в группы, называемые **сетями с расширенным набором услуг** (**Extended Service Set**, **ESS**). ESS образуется путем соединения между собой нескольких сетей BSS, расположенных в одном и том же сегменте логической сети.

Стандарт 802.11 различает два типа топологий сетей BSS:

– произвольная сеть (Ad Hoc BSS) – набор сетевых устройств, которые связаны таким образом, чтобы они могли напрямую отправлять кадры друг другу;

– инфраструктурный режим (Infrastructure BSS) – подключение сетевых устройств к базовой станции, которая транзитом обеспечивает взаимодействие между отдельными пользователями.

Базовая станция обычно соединяется проводным сегментом Ethernet с проводной частью сети, обеспечивая доступ сетевым устройствам к устройствам других базовых станций или сетей, обычно к сети Интернет. Поэтому базовая станция также называется **точкой доступа** (**Access Point**, **AP**).

Стек протоколов стандарта IEEE 802.11 (рисунок 5.8) соответствует общей структуре стандартов комитета 802, то есть состоит из физического уровня и уровня MAC, поверх которых работает уровень LLC. Как и у всех технологий семейства 802, технология 802.11 определяется нижними двумя уровнями, а уровень LLC выполняет свои стандартные функции, общие для всех технологий LAN.

В сетях 802.11 уровень MAC поддерживает два режима доступа к разделяемой среде: **распределенный режим** (**Distributed Coordination Function**, **DCF**), являющийся основным, и опциональный – **централизованный режим** (**Point Coordination Function**, **PCF**).

В распределенном режиме реализуется метод CSMA/CA. Этот режим требует синхронизации станций. Точками синхронизации являются моменты окончания передачи очередного кадра. Никакие специальные синхронизирующие сигналы не используются.

Централизованный режим доступа используется в сетях Wi-Fi, когда требуется обеспечить приоритетное обслуживание чувствительного к задержкам трафика. Метод PCF может применяться только в инфраструктурных BSS, то есть сетях, имеющих точку доступа, которая играет роль арбитра среды. Арбитр среды передает специальный кадр, который «говорит»

всем станциям, что начинается контролируемый период. Получив этот кадр, станции, которые хотели бы воспользоваться алгоритмом DCF для захвата среды, уже не могут этого сделать, они должны дожидаться окончания контролируемого периода. Затем реализуется метод PCF и арбитр выполняет процедуру опроса, чтобы по очереди предоставить каждой станции право на использование среды, направляя ей специальный кадр, который разрешает станции передавать данные. Режим PCF в сетях 802.11 сосуществует с режимом DCF.

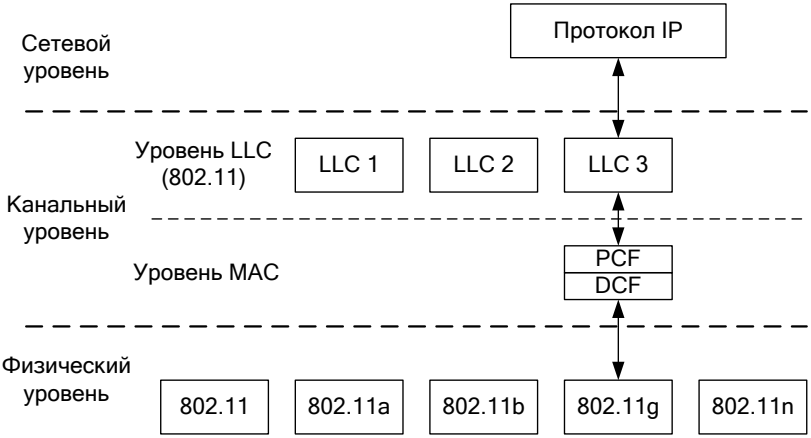

Рисунок 5.8 – Функциональные уровни технологии 802.11

Уровень MAC выполняет в беспроводных сетях больше функций, чем в проводных. Функции уровня MAC в стандарте 802.11 включают:

– доступ к разделяемой среде;

– обеспечение мобильности станций при наличии нескольких базовых станций;

– обеспечение безопасности, эквивалентной безопасности проводных локальных сетей.

Персональные сети (**Personal Area Network**, **PAN**) предназначены для взаимодействия устройств, принадлежащих одному владельцу, на небольшом расстоянии, обычно в радиусе 10 метров.

Типичным примером PAN является беспроводное соединение компьютера с периферийными устройствами. Персональные сети во многом похожи на локальные, но, помимо существенно меньшей области покрытия, персональные сети должны обеспечивать более высокие требования по информационной безопасности, энергосбережению и обеспечению безопасности здоровья пользователей.

В настоящее время самой популярной технологией PAN является Bluetooth, которая обеспечивает взаимодействие восьми устройств в разделяемой среде диапазона 2,4 МГц с битовой скоростью передачи данных до 3 Мбит/с.

Стандарт Bluetooth разработан группой Bluetooth SIG (Bluetooth Special Interest Group), организованной по инициативе компании Ericsson. Стандарт Bluetooth адаптирован рабочей группой IEEE 802.11 в соответствии с общей структурой стандартов IEEE 802.

В технологии Bluetooth используется термин **пикосеть**, который подчеркивает небольшую область ее покрытия. В пикосеть может входить до 255 устройств, но только восемь из них могут в каждый момент времени быть активными и обмениваться данными. Одно из устройств в пикосети является главным, а остальные – подчиненными.

Активное подчиненное устройство может обмениваться данными только с главным устройством. Все устройства пикосети, не являющиеся активными, должны находиться в режиме пониженного энергопотребления, в котором они только периодически прослушивают команду главного устройства для перехода в активное состояние.

Несколько пикосетей, которые обмениваются между собой данными, образуют рассредоточенную сеть. Взаимодействие в пределах рассредоточенной сети осуществляется за счет того, что один узел (называемый мостом) одновременно является членом нескольких пикосетей.

Bluetooth является законченной оригинальной технологией, рассчитанной на самостоятельное применение в электронных персональных устройствах и поддерживающей полный стек протоколов, включая собственные прикладные протоколы. В этом заключается ее отличие от технологий Ethernet и IEEE 802.11, которые выполняют функции только физического и канального уровней модели OSI. Для технологии Bluetooth был создан оригинальный стек протоколов, в дополнение к которому появилось большое количество профилей, определяющих конкретный набор протоколов для решения той или иной задачи.

5.5 Коммутируемые сети Ethernet

В сети Ethernet требование использовать единую разделяемую среду приводит к нескольким достаточно жестким ограничениям:

– общий диаметр сети не может быть больше 2500 м;

– количество узлов не может превышать 1024.

Для преодоления этих недостатков появилось средство построения более крупных локальных сетей на разделяемой среде – мосты локальных сетей. Такой мост связывал между собой два или больше сегментов сети, каждый из которых был построен на разделяемой среде. В задачу мостов входило

продвижение кадров из одного сегмента в другой исходя из их адресов назначения. Для этих целей был разработан алгоритм прозрачного моста IEEE 802.1D. Прозрачным этот алгоритм называется из-за того, что мост остается незамеченным для сетевых устройств сети. Каждый порт моста работает как конечный узел своего сегмента сети.

Для выполнения продвижения (фильтрации) кадров мост строит свою таблицу продвижения на основании пассивного наблюдения за трафиком, циркулирующим в подключенных к его портам сегментах. Мост «слушает» весь трафик, передаваемый в присоединенных к нему сегментах, и использует проходящие через него кадры для изучения топологии сети. По адресу источника кадра мост делает вывод о принадлежности узла-источника тому или иному сегменту сети и заносит в таблицу продвижения запись вида: MAC-адрес – номер порта.

Процесс обучения моста никогда не заканчивается и происходит одновременно с продвижением кадров. Мост постоянно следит за адресами источника кадров, поступающих на его интерфейсы, чтобы автоматически приспосабливаться к изменениям, происходящим в сети.

Такие динамические записи имеют срок жизни – при создании или обновлении записи в адресной таблице с ней связывается отметка времени. По истечении определенного тайм-аута запись помечается как недействительная, если за это время мост не принял ни одного кадра с данным адресом в поле адреса источника.

Кроме динамических записей в таблице продвижения могут быть статические записи, которые не имеют срока жизни, что дает администратору возможность влиять на работу моста, например, ограничивая передачу кадров с определенными адресами из одного сегмента в другой.

Серьезным ограничением функциональных возможностей мостов является отсутствие поддержки петлеобразных конфигураций сети. При таких конфигурациях в локальной сети будет наблюдаться бесконечная циркуляция кадров и постоянная перестройка таблиц продвижения. Для того чтобы избежать таких негативных последствий необходимо строить только древовидные структуры, гарантирующие наличие единственного пути между любыми двумя сегментами сети.

5.6 Коммутаторы и их архитектура

В процессе развития информационных технологий классические мосты перестали справляться со своей работой. Использование одного процессорного блока для обслуживания потоков кадров нескольких портов стало неэффективно. Лучшим оказалось решение, при котором для обслуживания потока, поступающего на каждый порт, в устройство ставился отдельный специализированный процессор, который реализовывал алгоритм прозрач-

ного моста. Такое устройство стали называть коммутатором. Помимо процессоров портов коммутатор имеет центральный процессор, который координирует работу портов, отвечая за построение общей таблицы продвижения, а также поддерживая функции конфигурирования и управления коммутатором. Со временем коммутаторы вытеснили из локальных сетей классические однопроцессорные мосты. Основной причиной повышения производительности сети при использовании коммутатора является параллельная обработка нескольких кадров.

Технология коммутации сама по себе не имеет непосредственного отношения к методу доступа к среде, который используется портами коммутатора. При подключении к порту коммутатора сегмента, представляющего собой разделяемую среду, данный порт, как и все остальные узлы такого сегмента, должен поддерживать полудуплексный режим. В случае, когда к каждому порту коммутатора подключен не сегмент, а только одно сетевое устройство и используется два физически раздельных канала можно использовать дуплексный режим.

В полудуплексном режиме работы порт коммутатора по-прежнему распознает коллизии. Доменом коллизий в этом случае является участок сети, включающий передатчик и приемник коммутатора, передатчик и приемник сетевого адаптера компьютера, а также две витые пары, соединяющие передатчики с приемниками. Коллизия возникает, когда передатчики порта коммутатора и сетевого адаптера одновременно или почти одновременно начинают передачу своих кадров.

В дуплексном режиме одновременная передача данных передатчиком порта коммутатора и сетевого адаптера коллизией не считается. При дуплексной связи порты Ethernet стандарта 10 Мбит/с могут передавать данные со скоростью 20 Мбит/с – по 10 Мбит/с в каждом направлении.

При разработке технологий Fast Ethernet и Gigabit Ethernet дуплексный режим стал одним из двух полноправных стандартных режимов работы узлов сети. Однако практика применения первых коммутаторов с портами Gigabit Ethernet показала, что они практически всегда применяются в дуплексном режиме для взаимодействия с другими коммутаторами или высокоскоростными сетевыми адаптерами. Поэтому при разработке версий стандартов 10G и 100G Ethernet его разработчики не стали создавать версию для работы в полудуплексном режиме, окончательно закрепив уход разделяемой среды из технологии Ethernet.

Коммутатор называют **неблокирующим**, если он может передавать кадры через свои порты с той же скоростью, с которой они на них поступают.

Под коммутатором, способным поддерживать устойчивый неблокирующий режим работы, подразумевается коммутатор, передающий кадры со скоростью их поступления в течение произвольного промежутка времени.

Для поддержания подобного режима нужно распределить потоки кадров по выходным портам таким образом, чтобы, во-первых, порты справлялись с нагрузкой и, во-вторых, коммутатор мог всегда в среднем передать на выходы столько кадров, сколько их поступило на входы. Если же входной поток кадров (просуммированный по всем портам) в среднем будет превышать выходной поток кадров (также просуммированный по всем портам), то кадры будут накапливаться в буферной памяти коммутатора и при переполнении – просто отбрасываться. Для того чтобы коммутатор был неблокирующим необходимо, чтобы достаточной производительностью обладали все элементы архитектуры коммутатора, включая центральный процессор, общую память, шины, соединяющие отдельные модули между собой, саму архитектуру коммутатора.

Для ускорения операций коммутации в настоящее время во всех коммутаторах используются специализированные БИС – ASIC (Application-Specific Integrated Circuit), которые оптимизированы для выполнения основных операций коммутации. Важную роль в построении коммутаторов играют и программируемые микросхемы FPGA (Field-Programmable Gate Array). Эти микросхемы могут выполнять все те же функции, что и микросхемы ASIC, но, в отличие от последних, могут программироваться и перепрограммироваться. В коммутаторах также применяются сетевые процессоры (NPU, Network Processor Unit). Этот тип процессоров имеет набор команд, ориентированных на обработку пакетов, обеспечивая еще большую гибкость, чем микросхемы FPGA.

Помимо процессорных микросхем для успешной неблокирующей работы коммутатору нужно иметь быстродействующий узел обмена, предназначенный для передачи кадров между процессорными микросхемами портов. В настоящее время в коммутаторах узел обмена строится на основе одной из трех схем:

1 **Коммутационная матрица**. Такая матрица состоит из двоичных переключателей, которые выполняют коммутацию канала между парой портов на время передачи данных пакета. Это наиболее простое решение, но работает оно только в случае фиксированного количества портов коммутатора: добавление портов требует изменения организации матрицы.

2 **Общая шина**. Это наиболее традиционный и гибкий метод объединения модулей вычислительного устройства, широко применяемый в компьютерах.

3 **Разделяемая многовходовая память**. В памяти для каждого порта организуется отдельная очередь пакетов. Любой порт может поместить пришедший пакет в эту очередь, а порт, для которого очередь предназначена, выбирает из нее пакеты и передает в сеть. Для поддержания нужной скорости работы коммутатора разделяемая память должна обладать высоким быстродействием.

5.7 Построение отказоустойчивых сетей с использованием протокола покрывающего дерева

В небольших сетях сравнительно легко гарантировать наличие одного и только одного пути между двумя сегментами сети. Но когда количество соединений возрастает, вероятность непреднамеренного образования петли оказывается высокой. Кроме того, для повышения надежности желательно иметь между мостами/коммутаторами резервные линии связи, которые присутствуют в топологии сети на физическом уровне, но не участвуют в работе сети на логическом уровне. Такие избыточные линии связи необходимо переводить в неактивное состояние. Для автоматического нахождения и конфигурирования активной древовидной топологии, мониторинга состояния ее связей и перехода к новой древовидной топологии при обнаружении отказа связи в коммутируемых локальных сетях используются **алгоритм покрывающего дерева** (**Spanning Tree Algorithm**, **STA**) и реализующий его **протокол покрывающего дерева** (**Spanning Tree Protocol**, **STP**).

Протокол STP формализует сеть в виде графа, вершинами которого являются коммутаторы и сегменты сети. Сегмент – это связная часть сети, не содержащая коммутаторов. Сегмент может быть разделяемой средой и включать устройства физического уровня – повторители/концентраторы или представлять собой двухточечный канал, что характерно для современных коммутируемых локальных сетей.

Протокол покрывающего дерева обеспечивает построение древовидной топологии связей с единственным путем минимальной длины от каждого коммутатора и от каждого сегмента до некоторого выделенного корневого коммутатора – корня дерева.

В качестве «расстояния» в STA используется метрика, учитывающая пропускную способность сегмента (величина, обратно пропорциональная пропускной способности сегмента). В текущей версии стандарта 802.1D-2004 используются значения метрик, представленные в таблице 5.1.

Протокольными единицами данных моста (**Bridge Protocol Data Unit**, **BPDU**) называются специальные пакеты, которыми периодически обмениваются коммутаторы для автоматического определения конфигурации дерева. Пакеты BPDU переносят данные об идентификаторах коммутаторов и портов, а также о расстоянии до корневого коммутатора. Существуют два типа сообщений, которые переносят пакеты BPDU:

– конфигурационные, называемые также сообщениями hello (с интервалом 2 с);

– сообщения с уведомлениями об изменении конфигурации.

Для доставки BPDU используется групповой адрес 01:80:C2:00:00:00, позволяющий организовать эффективный обмен данными.

Таблица 5.1 – **Значения метрик в соответствии с 802.D-2004**

Пропускная способность сегмента	Значение метрики
10 Тбит/с	2
1 Тбит/с	20
100 Гбит/с	200
10 Гбит/с	2000
1 Гбит/с	20000
100 Мбит/с	200000
10 Мбит/с	2000000

Работа STA происходит в три этапа:

1 **Определение корневого коммутатора**, от которого строится дерево. В качестве корневого выбирается коммутатор с наименьшим значением идентификатора. В исходном состоянии каждый коммутатор, считая себя корневым, генерирует и передает своим соседям сообщения hello, в которых помещает свой идентификатор в качестве идентификатора корневого коммутатора. Коммутатор, получив от соседа сообщение hello, содержащее идентификатор корневого коммутатора, меньший его собственного, перестает считать себя корневым коммутатором и генерировать свои сообщения hello, начиная ретранслировать сообщения hello, получаемые от соседа.

2 **Выбор корневого порта для каждого коммутатора**. Корневым портом коммутатора является тот порт, расстояние от которого до корневого коммутатора является минимальным. Сам корневой коммутатор корневых портов не имеет. Для определения корневого порта каждый коммутатор использует пакеты hello, ретранслируемые ему другими коммутаторами. На основании этих пакетов каждый коммутатор определяет минимальные расстояния от всех своих портов до корневого коммутатора и выбирает порт с наименьшим значением в качестве корневого. При равенстве расстояний выбирается порт с наименьшим значением идентификатора порта (это порядковый номер порта в коммутаторе).

3 **Выбор назначенных коммутаторов и портов для каждого сегмента сети**. Назначенным для сегмента является коммутатор, у которого расстояние от его корневого порта до корневого коммутатора минимально. Каждый коммутатор сегмента прежде всего исключает из рассмотрения свой корневой порт. Для каждого из оставшихся портов выполняется сравнение принятых по ним минимальных расстояний до корня с расстоянием до корня корневого порта данного коммутатора. Если все принятые на этом порту расстояния оказываются больше, чем расстояние от собственного корневого порта, то это значит, что для сегмента, к которому подключен порт, кратчайший путь к корневому коммутатору проходит через него, и он становится назначенным. Коммутатор делает все свои порты, для которых такое условие выполняется, назначенными. Когда имеется несколько портов с

одинаковым кратчайшим расстоянием до корневого коммутатора, выбирается порт с наименьшим идентификатором. Все остальные порты, кроме корневых и назначенных, каждым коммутатором блокируются и не могут передавать пользовательские кадры.

На выполнение всех трех этапов коммутаторам сети отводится по умолчанию 15 секунд. Эта стадия работы портов называется стадией прослушивания (Listening) – порты слушают только сообщения BPDU и не передают пользовательских кадров. Считается, что порты находятся в заблокированном состоянии, которое относится только к пользовательским кадрам, в то время как кадры BPDU обрабатываются.

После построения покрывающего дерева коммутатор начинает принимать пакеты данных и на основе их адресов источника строить таблицу продвижения.

В процессе нормальной работы корневой коммутатор продолжает генерировать пакеты hello, а остальные коммутаторы получают их через свои корневые порты и ретранслируют через назначенные порты. Если по истечении максимального времени жизни сообщения (по умолчанию – 10 интервалов hello – 20 секунд) корневой порт любого коммутатора сети не получает служебный пакет hello, он инициализирует новую процедуру построения покрывающего дерева – так обеспечивается отказоустойчивость локальной сети на коммутаторах. При этом на все порты генерируется и передается пакет hello, в котором коммутатор указывает себя в качестве корневого. Аналогично ведут себя и другие коммутаторы сети, у которых сработал таймер истечения максимального времени жизни сообщения, в результате чего выбирается новая активная конфигурация.

5.8 Виртуальные локальные сети и их конфигурирование

Виртуальной локальной сетью (**Virtual Local Area Network**, **VLAN**) называется группа сетевых устройств сети, трафик между которыми на канальном уровне полностью изолирован от трафика других устройств этой сети. Базовые правила построения виртуальных локальных сетей, не зависящие от протокола канального уровня, который поддерживается коммутатором, определены стандартом IEEE 802.1Q.

Передача кадров между разными виртуальными сетями на основании адреса канального уровня невозможна. Каждая виртуальная сеть образует свой домен широковещательного трафика. Достоинством технологии виртуальных сетей является то, что она позволяет создавать полностью изолированные сегменты сети путем логического конфигурирования коммутаторов, не прибегая к изменению физической структуры сети.

Виртуальные локальные сети могут перекрываться, если одно или более сетевых устройств входят в состав более чем одной виртуальной сети.

Для связывания виртуальных сетей в общую сеть требуется привлечение средств сетевого уровня (маршрутизатора или коммутатора 3-го уровня).

При создании виртуальных сетей на основе одного коммутатора обычно используется механизм группирования портов коммутатора, при котором каждый порт приписывается конкретной виртуальной сети (рисунок 5.9).

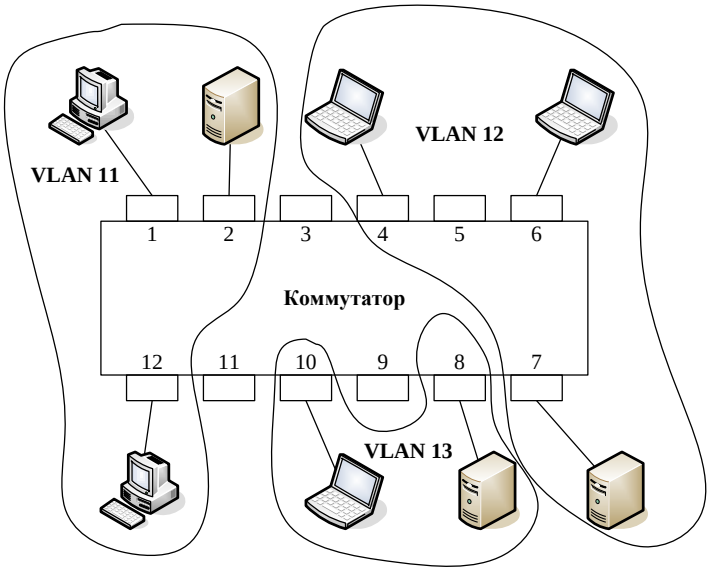

Рисунок 5.9 – VLAN на основе одного коммутатора

Создание виртуальных сетей путем группирования портов не требует от администратора большого объема ручной работы – достаточно каждый порт приписать к одной из нескольких заранее поименованных виртуальных сетей. Обычно такая операция выполняется с помощью специальной программы, прилагаемой к коммутатору.

При создании виртуальных сетей с несколькими коммутаторами используется метод, при котором в кадр вводится дополнительное поле, которое хранит информацию о принадлежности кадра той или иной виртуальной локальной сети. Такое поле используется только тогда, когда кадр передается от коммутатора к коммутатору, а при передаче кадра сетевому устройству оно удаляется.

Стандарт IEEE 802.1Q вводит в кадре Ethernet дополнительный заголовок – тег виртуальной локальной сети, который состоит из поля **TCI** (**Tag Control Information** – управляющая информация тега) размером в 2 байта и

предшествующего ему поля EtherType, которое является стандартным для кадров Ethernet и также состоит из 2 байтов (рисунок 5.10).

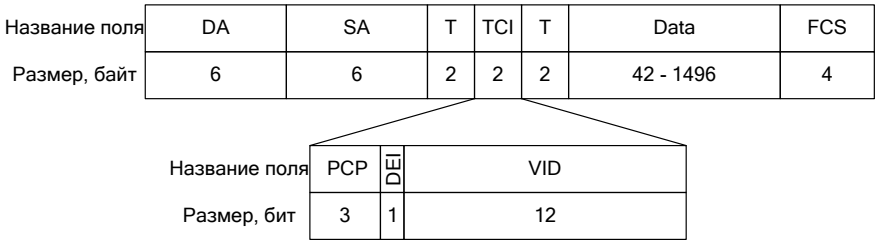

Рисунок 5.10 – Формат кадра технологии Ethernet с пометкой VLAN

Кадр, у которого в заголовке имеется тег VLAN, называют помеченным. Коммутаторы могут одновременно работать как с помеченными, так и с непомеченными кадрами. Из-за добавления тега VLAN максимальная длина поля данных уменьшилась на 4 байта.

Чтобы оборудование локальных сетей могло отличать и понимать помеченные кадры, для них введено специальное значение поля T, равное 0x8100. Это значение говорит о том, что за ним следует поле TCI, а не стандартное поле данных. В помеченном кадре за полями тега VLAN следует другое поле T, указывающее тип протокола, данные которого переносятся полем данных кадра.

Поле TCI состоит из следующих полей:

– **PCP (Priority Code Point)** – поле приоритета кадра;

– **DEI (Drop Eligible Indicator)** – индикатор допустимости удаления, который используется для указания кадров, которые могут быть отброшены при наличии перегрузки (ранее вместо DEI использовался бит **CFI (Canonical Format Indicator)**, который использовался для поддержания специального формата кадра Token Ring, а для Ethernet он должен был содержать значение 0);

– **VID (VLAN Identifier)** – 12-битное поле номера (идентификатора) VLAN, разрядность которого позволяет коммутаторам создавать до 4096 виртуальных сетей.

Наиболее распространенным подходом к конфигурированию виртуальных локальных сетей, построенных на нескольких коммутаторах, является подход, основанный на понятиях линии доступа и транка.

Линия доступа связывает порт коммутатора (называемый в этом случае портом доступа) с сетевым устройством, принадлежащим конкретной виртуальной локальной сети. **Транк** – это линия связи, которая соединяет между собой порты двух коммутаторов и может передавать трафик нескольких виртуальных сетей.

Чтобы образовать в исходной сети виртуальную локальную сеть, нужно в первую очередь выбрать для нее значение идентификатора VID, отличное от 1, а затем, используя команды конфигурирования коммутатора, приписать к этой сети те порты, к которым присоединены включаемые в нее сетевые устройства. Порты доступа получают от сетевых устройств сети непомеченные кадры, маркируя их тегом VLAN, содержащим то значение VID, которое назначено этому порту. При обратной передаче (от порта доступа к сетевому устройству) порт доступа удаляет тег виртуальной локальной сети.

Коммутаторы, поддерживающие технологию VLAN, осуществляют дополнительную фильтрацию трафика. Коммутатор проверяет, соответствует ли значение VID в теге VLAN кадра той виртуальной локальной сети, которая приписана к порту, в которой его необходимо передать. В случае соответствия кадр передается, несоответствия – отбрасывается. Изучение MAC-адресов коммутаторами сети производится отдельно по каждой виртуальной локальной сети.

Существует схема с гибким конфигурированием портов, в которой порты не делятся на транки и порты доступа. Каждый порт может быть гибко сконфигурирован для специфической поддержки кадров VLAN в зависимости от потребностей сети. Порт может работать в следующих режимах:

– Принимать только непомеченные кадры. В этом случае режим соответствует режиму порта доступа.

– Принимать только помеченные кадры. При этом порту могут быть приписаны один или несколько номеров VLAN. Этот режим соответствует избирательному режиму работы транка. Помеченные кадры передаются без отбрасывания/добавления тега VLAN.

– Принимать как помеченные, так и непомеченные кадры. Непомеченные кадры всегда принадлежат виртуальной локальной сети по умолчанию (VLAN1 или другой, назначенной администратором). Порту может быть приписан один или несколько номеров VLAN.

В схеме с гибким конфигурированием портов администратору проще производить изменения в конфигурации виртуальных локальных сетей, так как ему не требуется изменять роли портов в сети (например, изменять роль порта доступа на роль транка), но при этом увеличивается объем конфигурационных операций.

5.9 Методы защиты информации на канальном уровне

Протоколы и стандарты канального уровня описывают процедуры проверки доступности среды передачи, которые предполагают постоянное прослушивание среды передачи всеми подключенными к ней сетевыми устройствами, что может использоваться злоумышленниками для организации различных видов атак. Потенциально злоумышленник может осуществить

прослушивание трафика между произвольно выбранной парой сетевых устройств в сети.

Процесс передачи информации от одного сетевого устройства к другому через простой коммутатор происходит поэтапно и данные передаются кадрами, размер которых определен стандартом канального уровня. В процессе работы локальной сети сетевое устройство злоумышленника постоянно будет получать кадры широковещательной рассылки. Накапливая сведения из широковещательных запросов, злоумышленник будет иметь представление о сетевой активности всех узлов: кто, в какое время и с кем осуществляет информационный обмен. Таким образом, не проявляя сетевой активности, злоумышленник может определить аппаратные и сетевые адреса узлов являющихся серверами или маршрутизаторами.

Кроме того, злоумышленник может перехватывать информацию, передаваемую между двумя сетевыми устройствами в сети. Такая атака называется ARP-spoofing (рисунок 5.11). Для этого в процессе работы протокола ARP (подробнее будет рассмотрен в следующем разделе) злоумышленник может передать ответный кадры этого протокола одному из атакуемых сетевых устройств, подставляя в заголовок в качестве источника свой MAC-адрес и IP-адрес второго атакуемого сетевого устройства Проблема заключается в том, что сетевое устройство доверяет содержимому кадра с ответом протокола ARP. Получив такой ложный ответ первое сетевое устройство перестраивает свою таблицу продвижения кадров и с этого момента все кадры, отправляемые им в адрес второго сетевого устройства, будут иметь в заголовке MAC-адрес сетевого устройства злоумышленника. Организовав ложную рассылку ответов протокола ARP в адрес обоих атакуемых сетевых устройств, злоумышленник может прослушивать весь трафик между этими устройствами в локальной сети.

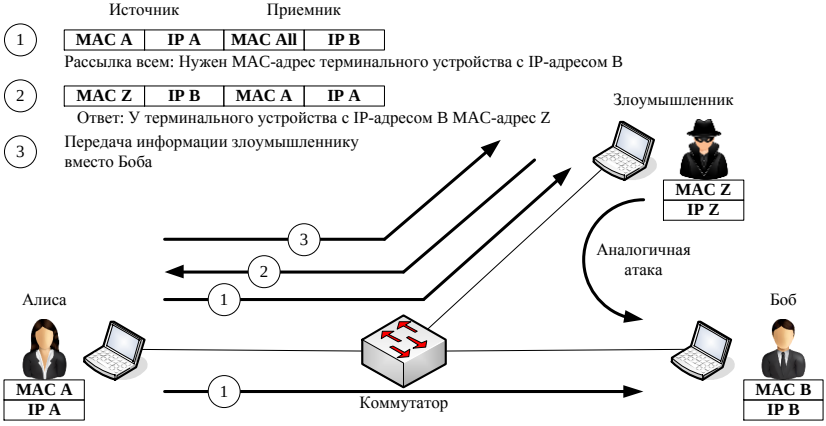

Рисунок 5.11 – ARP-spoofing

Имена «Алиса» и «Боб» (рисунок 5.11) традиционно используются для обозначения субъектов практически во всех материалах, касающихся криптографии, с тех пор как Рон Ривест использовал их в 1978.

Техника атаки ARP-spoofing реализована в виде программного обеспечения и доступна пользователям сети Интернет. Компьютерные сети, оснащенные многофункциональными управляемыми коммутаторами, зачастую также остаются уязвимыми к подобного рода атакам. Во многих случаях функции защиты и разграничения доступа к среде передачи, реализованные в этих изделиях, остаются невостребованными в связи с недостатком квалификации или небрежностью системных администраторов.

Для защиты информации на канальном уровне необходимо вести мониторинг соответствия аппаратных и сетевых адресов всех узлов сети, должны быть определены допустимые маршруты передачи кадров канального уровня и рабочие места, с которых разрешено конфигурирование коммутаторов. Должен быть обеспечен строгий контроль доступа в помещения, в которых расположены коммутаторы и прочие сетевые устройства, с которых разрешено управление коммутаторами. Кроме того, коммутаторы должны обеспечивать разграничение доступа между узлами сети с применением технологии VLAN, отключением VLAN1 и неиспользуемых портов коммутатора. Необходимо проводить мониторинг сетевой активности пользователей с целью выявления источников аномально высокого количества широковещательных запросов.

Контрольные вопросы

1 Что такое технология Ethernet?

2 Какие поля входят в состав кадра Ethernet?

3 Какова структура MAC-адреса?

4 Что такое разделяемая среда передачи?

5 Опишите алгоритм процесса передачи данных сетевым устройством по протоколу CSMA/CD.

6 Назовите основные проблемы беспроводных локальных сетей.

7 Опишите алгоритм процесса передачи данных сетевым устройством по протоколу CSMA/CA.

8 Что такое персональная сеть?

9 Что такое коммутатор?

10 Какие коммутаторы называются неблокирующими?

11 Перечислите разновидности архитектуры коммутаторов.

12 Опишите работу протокола покрывающего дерева.

13 Что такое виртуальная локальная сеть?

14 Какие дополнительные поля входят в состав кадра Ethernet с пометкой VLAN?

15 Какие методы защиты информации применяются на канальном уровне модели OSI?

6 СТЕК ПРОТОКОЛОВ TCP/IP

В настоящее время стек протоколов TCP/IP широко используется как в глобальных, так и в локальных сетях и имеет иерархическую, четырехуровневую структуру, представленную на рисунке 6.1.

Прикладной уровень	HTTP, HTTPs, SMTP, POP3, IMAP, FTP, Telnet, SSH
Транспортный уровень	TCP, UDP
Сетевой уровень	IP, RIP, OSPF, EIGRP, BGP, ICMP, IGMP
Уровень сетевых интерфейсов	Не регламентируется

Рисунок 6.1 – Стек протоколов TCP/IP

Прикладной уровень стека протоколов TCP/IP соответствует трем верхним уровням модели OSI: прикладному, уровню представления и сеансовому. Он объединяет сервисы, предоставляемые стеком TCP/IP пользовательским приложениям. Подробнее протоколы этого уровня стека протоколов TCP/IP будут рассмотрены в следующем разделе.

Нижние уровни модели OSI (канальный и физический) реализуют разнообразный набор функций: доступ к среде передачи, формирование кадров, согласование величин электрических сигналов, кодирование, синхронизация, усиление. Конкретные реализации этих функций составляют суть протоколов физического и канального уровней, таких, например, как Ethernet и 802.11. У нижнего уровня стека TCP/IP задача существенно проще – он отвечает только за организацию взаимодействия с подсетями нижележащих технологий, которые входят в составную сеть.

Задачу организации интерфейса между технологией TCP/IP и любой другой технологией промежуточной сети упрощенно можно свести к двум задачам:

– инкапсуляция (упаковка) IP-пакета в единицу передаваемых данных локальной сети;

– преобразование сетевых IP-адресов в адреса технологии локальной сети.

Технологии локальных сетей были подробно рассмотрены в предыдущем разделе. Предметом данного раздела являются два уровня модели OSI: сетевой и транспортный.

6.1 Межсетевой протокол

Сетевой уровень, называемый также уровнем Интернета, является ключевым уровнем всей архитектуры TCP/IP. Протоколы сетевого уровня поддерживают интерфейс с вышележащим транспортным уровнем, получая от него запросы на передачу данных по составной сети, а также с нижележащим уровнем сетевых интерфейсов.

Основным протоколом сетевого уровня является **межсетевой протокол** (**Internet Protocol**, **IP**). В его задачу входит продвижение **пакета** (PDU сетевого уровня) между сетями – от одного маршрутизатора к другому до тех пор, пока пакет не попадет в сеть назначения. Этот протокол развертывается не только на хостах, но и на всех маршрутизаторах. Протокол IP – это дейтаграммный протокол, работающий без установления соединений по принципу доставки с максимальными усилиями.

К сетевому уровню TCP/IP также относятся протоколы маршрутизации (RIP, OSPF, EIGRP, BDP и т. п.), предназначенные для изучения топологии сети, определения маршрутов и составления таблиц маршрутизации, на основании которых протокол IP перемещает пакеты в нужном направлении. Кроме того, к сетевому уровню могут быть отнесены вспомогательные протоколы, например, **протокол межсетевых управляющих сообщений** (**Internet Control Message Protocol**, **ICMP**), предназначенный для передачи маршрутизатором источнику сведений об ошибках, возникших при передаче пакета, и пр.

Важную часть технологии TCP/IP составляют задачи адресации, к числу которых относятся:

– согласованное использование адресов различного типа – эта задача включает в себя отображение адресов разных типов друг на друга;

– обеспечение уникальности адресов – в зависимости от типа адреса требуется обеспечивать однозначность адресации в пределах компьютера, подсети, корпоративной сети или Интернета;

– конфигурирование сетевых интерфейсов и сетевых приложений.

Процедуры, предлагаемые TCP/IP для назначения, отображения и конфигурирования адресов, одинаково хорошо работают в сетях разного масштаба. Система IP-адресации позволяет универсальным и однозначным способом идентифицировать любой интерфейс составной сети. Для этого

используется «пара», состоящая из номера сети и номера узла, которая является сетевым адресом, или в терминологии TCP/ IP – **IP-адресом**.

IP-адрес идентифицирует не отдельный узел сети (компьютер или маршрутизатор), а одно сетевое соединение или один сетевой интерфейс.

Каждый раз, когда пакет направляется адресату через составную сеть, в его заголовке указывается IP-адрес узла назначения. По номеру сети назначения каждый очередной маршрутизатор находит IP-адрес следующего маршрутизатора и на основании этого IP-адреса его локальный адрес.

IP-адрес имеет фиксированную длину 4 байта (32 бита). Наиболее распространенной формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 185.179.82.239. Такая запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла. Для выделения из IP-адреса IP-адрес сети используют следующие варианты:

– фиксированные границы – все 32-битное поле адреса заранее делится на две части (номер сети и номер узла) не обязательно равной, но фиксированной длины;

– применение маски, которая позволяет максимально гибко устанавливать границу между номером сети и номером узла – при таком подходе адресное пространство можно использовать для создания множества сетей разного размера (**маска** – это число, применяемое в паре с IP-адресом, причем двоичная запись маски содержит непрерывную последовательность единиц в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети);

– классификация адресов – компромисс по отношению к двум предыдущим вариантам: размеры сетей хотя и не могут быть произвольными, как при использовании масок, но и не должны быть одинаковыми, как при установлении фиксированных границ. По значениям первых битов адреса можно определить к какому классу он относится (рисунок 6.2).

Адреса классов A, B и C являются индивидуальными адресами. Групповые адреса, принадлежащие классу D, не делятся на номер сети и номер узла и обрабатываются маршрутизатором особым образом. Их основное назначение – распространение информации по схеме «один-ко-многим».

Существуют следующие ограничения при назначении IP-адресов:

– номера сетей и номера узлов не могут состоять из одних двоичных нулей или единиц (такие значения используются в IP для особых целей);

– запрещается присваивать сетевым интерфейсам IP-адреса, начинающиеся со значения 127 (адрес, первый октет которого равен 127, является внутренним адресом стека протоколов компьютера (или маршрутизатора) и используется для тестирования программ, или для работы клиентской и серверной частей приложения, установленных на одном компьютере).

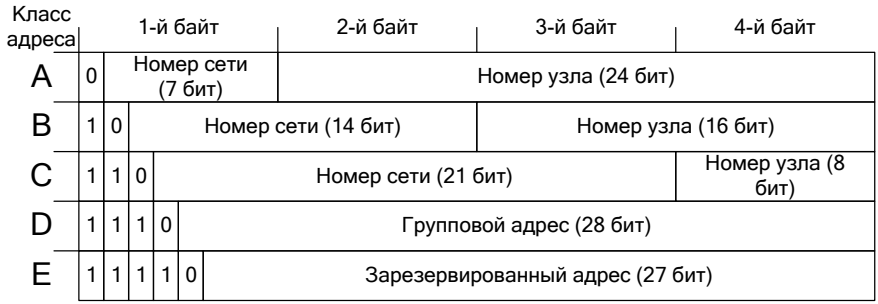

Рисунок 6.2 – Классы IP-адресов

IP-адреса могут быть:

– публичными (глобальными), когда уникальность нумерации в сети может быть обеспечена только усилиями специально созданных для этого центральных органов;

– частными, определенными для автономных сетей без подключения к сети Интернет.

Выделено несколько диапазонов частных адресов, рекомендуемых для автономного использования:

– в классе A – сеть 10.0.0.0;

– классе B – диапазон из 16 сетей (172.16.0.0 – 172.31.0.0);

– классе C – диапазон из 255 сетей (192.168.0.0 – 192.168.255.0).

Эти адреса, исключенные из множества централизованно распределяемых, составляют достаточно большое адресное пространство.

Проблемой централизованного распределения адресов является их дефицит, который обусловлен не только ростом количества узлов и сетей, но и тем, что имеющееся адресное пространство используется нерационально.

Для смягчения проблемы дефицита адресов разработчики стека протоколов TCP/IP предлагают следующие подходы:

– переход на новую версию протокола IP – протокол IPv6, в котором проблемы дефицита адресов не существует;

– использование технологии трансляции сетевых адресов (Network Address Translation, NAT);

– использование технологии бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR).

Заголовок IP-пакета предназначен для передачи служебной информации, необходимой для продвижения пакета по сети от маршрутизатора к маршрутизатору. Состав заголовка IP-пакета IPv4 представлен на рисунке 36 и включает следующие поля:

– **VERS (Version)** – номер версии – идентифицирует версию протокола IP (для четвертой версии протокола IP равно 0100);

– **HLEN** (**Head Length**) – длина заголовка – количество 32-битных строк в заголовке (для стандартного заголовка IPv4 без дополнительных параметров, как это представлено на рисунке 6.3, равно 0101);

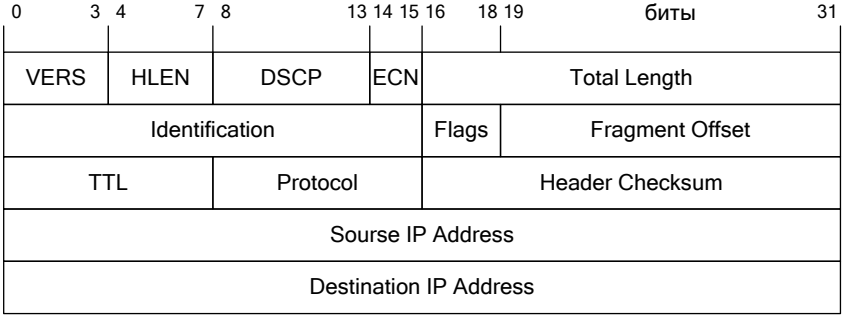

Рисунок 6.3 – Структура заголовка IPv4

– **DSCP** (**Differentiated Services Code Point**) – точка кода дифференцированных услуг – используется для разделения трафика на классы обслуживания, изначально это поле называлось «Тип обслуживания» (Type of Service, ToS);

– **ECN** (**Explicit Congestion Notification**) – указатель перегрузки – предупреждает о перегрузке сети без потери пакетов (не является обязательной функцией);

– **Total Length** – общая длина – характеризует общую длину пакета с учетом заголовка и поля данных (максимальная длина пакета ограничена разрядностью поля и составляет 65 535 байт);

– **Identification** – идентификатор пакета – используется для распознавания пакетов, образовавшихся путем фрагментации (деления на части) исходного пакета (все фрагменты одного пакета имеют одинаковое значение этого поля);

– **Flags** – флаги DF и MF – содержат признаки, связанные с фрагментацией (1 в бите **DF** (**Do not Fragment**) запрещает маршрутизатору фрагментировать данный пакет; 1 в бите **MF** (**More Fragments**) говорит о том, что данный пакет не является последним в серии фрагментов; еще один бит зарезервирован);

– **Fragment Offset** – смещение фрагмента – задает смещение в байтах поля данных текущего фрагмента относительно начала поля данных исходного пакета;

– **TTL** (**Time To Live**) – время жизни – содержит предельный срок, в течение которого пакет может перемещаться по сети (измеряется в секундах пребывания в маршрутизаторах, при современных скоростях фактически характеризует количество маршрутизаторов, которое может пройти пакет);

– **Protocol** – протокол верхнего уровня – содержит идентификатор, указывающий, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета;

– **Header Checksum** – контрольная сумма заголовка, которая рассчитывается и проверяется на каждом из устройств и только по заголовку пакета;

– **Sourse IP Address** – 32-битный IP-адрес источника пакета;

– **Destination IP Address** – 32-битный IP-адрес приемника пакета.

Помимо основного заголовка допускается использование дополнительных параметров, значения которых по размеру должны быть выравнены до 4-х байт (32 бита). В этом случае поле HLEN должно учитывать наличие этих параметров.

Уже в 1980-е годы стало очевидно, что распределение адресного пространства происходит значительно более быстрыми темпами, чем было заложено в архитектуру IPv4, что привело к разработке нового протокола IPv6. 25 ноября 2019 года были распределены последние свободные IPv4 адреса в Европе, странах бывшего СССР и на Ближнем Востоке. Теперь получить IPv4 адрес можно будет, только если его освободит текущий владелец (закроется компания или какая-либо сеть освободит ненужный ей адресный ресурс).

Структура основного заголовка IPv6 представлена на рисунке 6.4.

Заголовок IPv6 имеет следующие поля:

– **Version** – номер версии – идентифицирует версию протокола IP (для шестой версии протокола IP равно 0110);

– **Traffic Class** – вид нагрузки – аналогично полю DSCP в заголовке IPv4;

– **Flow Label** – метка потока – указывает на принадлежность пакета к тому или иному потоку;

– **Payload Length** – длина поля данных – характеризует длину пакета без основного заголовка, т. е. с учетом дополнительных заголовков и поля данных (максимальное значение составляет 65 535 байт, но IPv6 допускает существование пакетов с более длинным полем данных, так называемых сверхбольших дейтаграмм или джамбограмм (jumbograms), для которых длина задается 32-разрядным полем одной из опций дополнительного заголовка транзитных опций hop-by-hop);

– **Next Header –** следующий заголовок – при наличии дополнительных заголовков содержит ссылку на первый из них (определяет его тип), который в таком же поле содержит ссылку на следующий дополнительный заголовок и т. д.; в последнем дополнительном заголовке значение, аналогичное полю «Protocol» заголовка IPv4; при отсутствии дополнительных заголовков – соответствует полю «Protocol» заголовка IPv4;

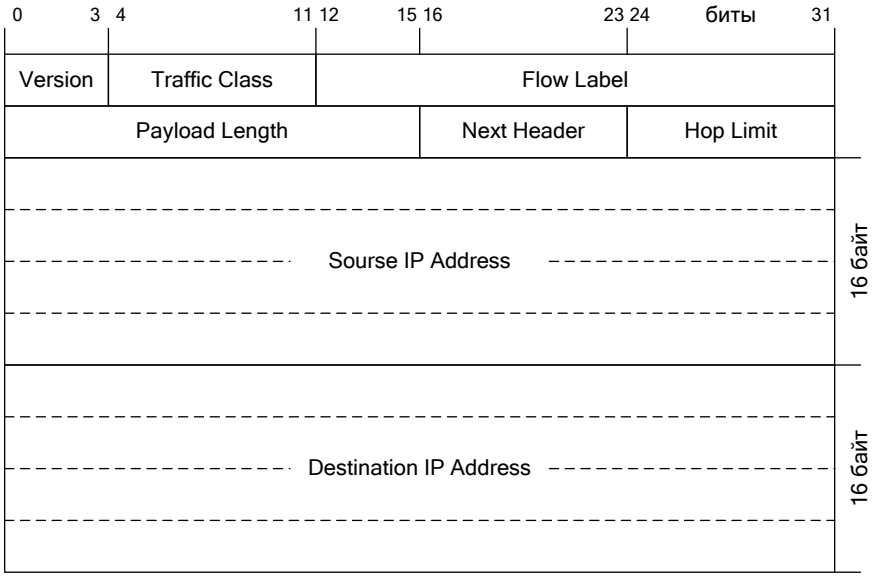

Рисунок 6.4 – Структура основного заголовка IPv6

– **Hop Limit –** лимит переходов – данное поле аналогично полю TTL протокола IPv4 и при прохождении каждого маршрутизатора из значения этого поля вычитается единица (при значении поля равным 0 маршрутизатор отбрасывает пакет);

– **Sourse IP Address** – 128-битный IP-адрес источника пакета;

– **Destination IP Address** – 128-битный IP-адрес приемника пакета.

В IPv6 вместо десятичной используется шестнадцатеричная форма записи IP-адреса. Каждые четыре шестнадцатеричные цифры отделяются друг от друга двоеточием, например: FE80:0000:0000:0000:19A4:07D5:0000:A417. Старшие нули в группе четырех шестнадцатеричных цифр могут быть опущены (можно записать 7D5 вместо 07D5). Несколько нулевых групп могут быть заменены парой двоеточий: FE80::19A4:7D5:0:A417. В IP-адресе допускается только одна такая замена.

Общий формат адреса IPv6 представлен на рисунке 6.5.

На этом рисунке введены следующие обозначения полей:

– **FP** (**Format Prefix**) – префикс формата – определяет тип адреса;

– **TLA** (**Top-Level Aggregation**) – предназначено для идентификации сетей самых крупных поставщиков услуг;

– **NLA** (**Next-Level Aggregation**) – предназначено для нумерации сетей средних и мелких поставщиков услуг;

Название поля	FP	TLA	Резерв	NLA	SLA	Идентификатор интерфейса
Размер, бит	3	13	8	24	16	64

Рисунок 6.5 – Формат адреса IPv6

– **SLA** (**Site-Level Aggregation**) предназначено для адресации подсетей отдельного абонента (одной корпоративной сети);

– **идентификатор интерфейса** является аналогом номера узла в IPv4.

Для нормальной работы сети каждому сетевому интерфейсу сетевого устройства должен быть назначен IP-адрес. Процедура присвоения адресов происходит в ходе их конфигурирования вручную или динамически.

При конфигурировании указывается не только IP-адрес сетевого интерфейса и его маска, но также ряд других конфигурационных параметров, необходимых для его эффективной работы: IP-адрес маршрутизатора, IP-адрес DNS-сервера, доменное имя сетевого устройства и т. п. При ручном конфигурировании эта работа является достаточно сложной.

Протокол динамического конфигурирования хостов (**Dynamic Host Configuration Protocol**, **DHCP**) автоматизирует процесс конфигурирования сетевых интерфейсов, защищая от дублирования адресов за счет централизованного управления их распределением. Этот протокол работает в соответствии с моделью клиент-сервер. Во время запуска операционной системы сетевого устройства DHCP-клиент посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес и ряд других конфигурационных параметров. DHCP-сервер должен находиться в одной подсети с клиентами, при его отсутствии в сети может располагаться связной DHCP-агент, который переправляет запросы клиентов к серверу, расположенному в другой сети.

DHCP-сервер может работать как в ручном режиме (строгое соответствие IP-адресов MAC-адресам), так и в автоматическом. При автоматическом режиме возможно статическое и динамическое распределение адресов.

При статическом распределении адресов DHCP-сервер без вмешательства администратора произвольным образом выбирает для клиента в постоянное пользование IP-адрес из пула наличных IP-адресов. При динамическом распределении адрес DHCP-клиенту выдается на определенное время, называемое сроком аренды. При таком подходе администратор управляет процессом конфигурирования сети, определяя два основных конфигурационных параметра DHCP-сервера: пул адресов, доступных распределению, и срок аренды. Срок аренды диктует, как долго сетевое устройство может использовать назначенный IP-адрес, перед тем как снова запросить его у DHCP-сервера.

Не рекомендуется использовать динамическое назначение адресов для интерфейсов, которые участвуют в системах мониторинга и безопасности.

В сети вполне вероятны ситуации, когда протокол IP не может доставить пакет адресату в силу ряда объективных причин. Для компенсации ненадежности протокола IP используется протокол ICMP, который является вспомогательным протоколом, использующимся для диагностики и мониторинга сети. Он не предназначен для исправления возникших при передаче пакета проблем, как протоколы более высоких уровней модели OSI, он является средством оповещения отправителя о проблемах, произошедших с его пакетами.

Несмотря на многообразие решаемых задач, все типы сообщений ICMP имеют один и тот же формат, представленный на рисунке 6.6.

Название поля	Type	Code	Checksum	Message Body
Размер, байт	1	1	2	Зависит от типа сообщения

Рисунок 6.6 – Формат ICMP-сообщения

Здесь введены следующие обозначения полей:

– **Type** – числовой идентификатор типа сообщения;

– **Code** – числовой идентификатор, более тонко дифференцирующий тип ошибки;

– **Checksum** – контрольная сумма, которая подсчитывается для всего ICMP-сообщения;

– **Message Body** – поле данных.

Все ICMP-сообщения можно разделить на сообщения об ошибках и сообщения запрос-ответ. Сообщения об ошибках конкретизируются уточняющим кодом. Сообщения запрос-ответ связаны в пары. Наиболее распространенными утилитами, использующими ICMP, являются утилиты **ping** и **tracert** (**traceroute**).

Утилита ping представляет собой очень простое средство мониторинга сети. Сетевое устройство посылает по составной сети ICMP-сообщение эхо-запроса, указывая в нем IP-адрес узла, достижимость которого нужно проверить, а узел, получивший эхо-запрос, формирует и отправляет эхо-ответ отправителю запроса. Успешная доставка означает нормальное функционирование всей транспортной системы составной сети.

Утилита tracert позволяет проследить маршрут до удаленного хоста, определить среднее время оборота, IP-адрес и в некоторых случаях доменное имя каждого промежуточного маршрутизатора. Такая информация помогает найти маршрутизатор, на котором оборвался путь пакета к удаленному хосту.

6.2 Протоколы разрешения адресов

При организации сети связи обычно применяют сразу несколько схем адресации. Сетевой интерфейс сетевого устройства может одновременно иметь несколько адресов, каждый из которых используется определенными протоколами своего уровня модели OSI. При такой организации необходимо обеспечить преобразование адресов из одного вида в другой. Для этого используются специальные вспомогательные протоколы, которые называют **протоколами разрешения адресов**.

Процесс установления соответствия между адресами различных типов может решаться как централизованными, так и распределенными средствами. При централизованном подходе в сети выделяется один или несколько серверов адресов (имен), в которых хранится таблица соответствия адресов различных типов. Все сетевые устройства обращаются к серверу с запросами, чтобы по адресу одного типа найти адрес другого. Примером централизованного подхода является справочная служба – **система доменных имен** (**Domain Name System**, **DNS**), которая отображает символьные имена узлов сети на их IP-адреса.

Доменная служба имен является важной частью Интернета, но может также работать и в любой автономной IP-сети. В стеке TCP/IP применяется доменная система имен, имеющая иерархическую древовидную структуру, допускающую наличие в имени произвольного количества составных частей. Дерево имен начинается с корня (рисунок 6.7), обозначаемого точкой. Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует конечному узлу сети. Составные части доменного имени отделяются друг от друга точкой. Разделение имени на части позволяет распределить административную ответственность за назначение уникальных имен между различными людьми или организациями в пределах своего уровня иерархии.

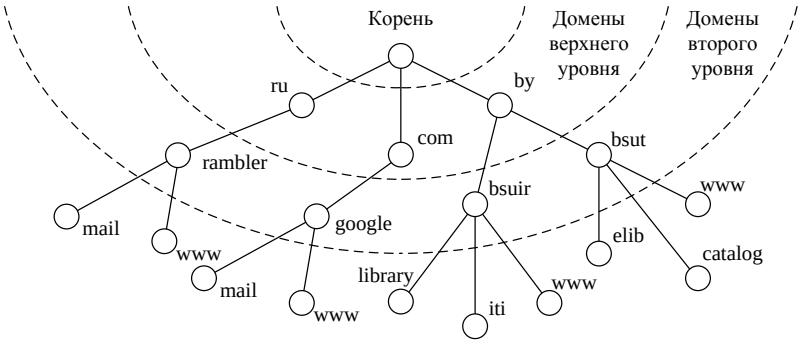

Рисунок 6.7 – Дерево доменных имен

Совокупность имен, у которых несколько старших составных частей совпадают, образуют **домен имен**. Администратор домена несет ответственность за уникальность имен следующего уровня, входящих в домен.

Корневой домен имен регулируется **корпорацией по управлению доменными именами и IP-адресами (Internet Corporation for Assigned Names and Numbers, ICANN)**. Домены верхнего уровня назначаются для каждой страны, а также для различных типов организаций. Каждый домен администрирует отдельная организация, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям.

Система DNS состоит из серверов и клиентов. DNS-серверы поддерживают распределенную базу разрешений имен, а DNS-клиенты, которыми являются практически все сетевые устройства, обращаются к серверам с запросами об разрешении доменного имени на IP-адрес. Программа, реализующая функции клиента DNS, называется резольвером и входит в состав операционной системы. Любое приложение, у которого возникает необходимость в отображении доменного имени, обращается к резольверу своей операционной системы, который взаимодействует с DNS-сервером.

DNS-серверы образуют иерархию, на самой вершине которой располагаются корневые серверы. Эти серверы хранят текстовые файлы имен и IP-адресов DNS-серверов следующего (верхнего) уровня, которые, в свою очередь, хранят данные об именах и адресах имен, входящих в домены верхнего уровня, а также об именах DNS- серверов, которые обслуживают домены второго уровня иерархии и т. д. Пространство доменных имен разделено между серверами так, чтобы каждый сервер хранил записи только в пределах одного уровня, а для имен своих поддоменов хранил только ссылки на серверы DNS, которые отвечают за эти поддомены.

Корневые серверы – это наиболее уязвимое звено DNS. Корневые серверы распределены географически, а каждый кластер, соответствующий одному имени, администрируется отдельной организацией. В настоящее время установлено 13 кластеров корневых серверов, а общее количество корневых серверов превышает 1300 штук.

Часть пространства доменных имен, для которых некоторый DNS-сервер имеет информацию об их разрешениях на основе соответствующего текстового файла (файла зоны), называется **зоной DNS** данного сервера. Для обеспечения надежности и высокой производительности для каждой зоны существует один первичный (primary) DNS-сервер и несколько вторичных (secondary) серверов. На первичном сервере находится исходный файл зоны; вторичные серверы периодически копируют файл зоны с первичного сервера.

Существуют две основные схемы разрешения DNS-имен: итеративная, в которой работу по поиску IP-адреса координирует DNS-клиент (итеративно выполняет последовательность запросов к разным серверам имен), и рекурсивная, в которой разрешение адресов выполняет цепочка DNS-серверов. Существует смешанная схема, включающая в себя рекурсивную и итеративную фазы разрешения адресов.

При распределенном подходе к разрешению адресов каждое сетевое устройство само хранит все назначенные ему адреса разных типов. В этом случае сетевое устройство, которому необходимо определить по известному адресу некоторого сетевого устройства его адрес другого типа, посылает в сеть широковещательный запрос. Все сетевые устройства сети сравнивают содержащийся в запросе адрес с собственным, и то сетевое устройство, у которого обнаружилось совпадение, посылает ответ, содержащий искомый адрес. Такая схема использована в **протоколе разрешения адресов** (**Address Resolution Protocol**, **ARP**) стека TCP/IP.

При работе протокола ARP в локальных сетях с возможностью широковещательной рассылки процесс разрешения адресов происходит следующим образом. Каждый сетевой интерфейс локальной сети имеет IP-адрес и MAC-адрес. Межсетевой протокол сетевого устройства, который организует передачу IP-пакета, определил IP-адрес интерфейса следующего маршрутизатора. Прежде чем упаковать пакет в кадр Ethernet и направить его маршрутизатору, необходимо определить его MAC-адрес. Для решения этой задачи протокол IP обращается к протоколу ARP.

Протокол ARP поддерживает на каждом интерфейсе сетевого адаптера или маршрутизатора отдельную ARP-таблицу, в которой в ходе функционирования сети накапливается информация о IP-адресах и соответствующих им MAC-адресах интерфейсов сети. Первоначально, при подключении компьютера или маршрутизатора к сети, ARP-таблица его интерфейса пуста. В таком случае происходит опрос интерфейсов сети широковещательным ARP-запросом, размещенном в кадре технологии локальной сети, например, Ethernet. Каждый интерфейс сети получает этот запрос и направляет его протоколу ARP. ARP сравнивает указанный в запросе адрес IP с IP-адресом собственного интерфейса. Протокол ARP, который обнаружил совпадение, формирует ARP-ответ, в котором указывает искомый MAC-адрес, и отправляет его запрашивающему сетевому устройству. Чтобы уменьшить число ARP-обращений, запись о найденном соответствии между IP-адресом и MAC-адресом сохраняется в ARP-таблице соответствующего интерфейса. Эта таблица пополняется также в результате извлечения полезной информации из широковещательных ARP-запросов других интерфейсов сети.

В глобальных сетях, в которых не поддерживается широковещательная рассылка, используется централизованный подход. Для этого организуется

ARP-сервер, на котором регистрируются адреса сетевых устройств, подключаемых к сети.

Достоинство распределенного подхода состоит в том, что он позволяет отказаться от выделения сервера. Недостатком его является необходимость широковещательных сообщений, перегружающих сеть. Именно поэтому распределенный подход используется в небольших сетях, а централизованный – в больших.

6.3 Маршрутизация

Протоколы маршрутизации обеспечивают поиск и фиксацию маршрутов продвижения данных через составную сеть TCP/IP. Задачей протоколов маршрутизации является создание на всех маршрутизаторах согласованных друг с другом таблиц маршрутизации, по которым осуществляется выбор рационального маршрута.

Различают протоколы, выполняющие статическую и динамическую маршрутизацию. При статической маршрутизации все записи в таблице имеют неизменяемый статус и заполняются вручную администратором сети. При динамической маршрутизации все изменения конфигурации сети автоматически отражаются в таблицах маршрутизации благодаря протоколам маршрутизации. Эти протоколы собирают информацию о топологии связей в сети и оперативно отражают все текущие изменения. При динамической маршрутизации в таблицах для каждой записи, полученной от динамического протокола маршрутизации, имеется информация об интервале времени, в течение которого эта запись будет оставаться действительной. Если по истечении этого времени существование маршрута не подтверждается динамическим протоколом маршрутизации, то он считается нерабочим, и пакеты по нему больше не посылаются.

Протоколы динамической маршрутизации бывают распределенными и централизованными. При распределенном подходе все маршрутизаторы сети находятся в равных условиях. Каждый из них самостоятельно находит маршруты и строит собственную таблицу маршрутизации. Для эффективного взаимодействия они постоянно обмениваются информацией о конфигурации сети. При централизованном подходе в сети существует один выделенный маршрутизатор, собирающий всю информацию о топологии и состоянии сети. На основании этих данных такой маршрутизатор строит таблицы маршрутизации и рассылает их всем остальным маршрутизаторам сети. Централизованный подход составляет более рациональные маршруты, но плохо масштабируется при развитии сети. Распределенная маршрутизация может привести к временной несогласованности таблиц разных маршрутизаторов. Это связано с тем, что при изменениях в сети протоколам необходимо некоторое время, чтобы все маршрутизаторы сети внесли изменения в свои таблицы и сделали их согласованными.

Протоколы маршрутизации по области применения подразделяются:

– на протоколы межсистемной (междоменной) маршрутизации – **внешние шлюзовые протоколы** (**Exterior Gateway Protocol**, **EGP**);

– протоколы внутрисистемной (внутридоменной) маршрутизации – **внутренние шлюзовые протоколы** (**Interior Gateway Protocol**, **IGP**).

В зависимости от алгоритма маршрутизации выделяют **дистанционно-векторные** (**Distance Vector Algorithm**, **DVA**) и **алгоритмы состояния каналов связи** (**Link State Algorithm**, **LSA**).

В дистанционно-векторных алгоритмах каждый маршрутизатор с определенной периодичностью широковещательно рассылает по сети вектор с метрикой расстояний от данного маршрутизатора до всех известных ему сетей. Каждый маршрутизатор, получив такой вектор, наращивает его компоненты на величину расстояния от себя до данного соседа и дополняет информацией об известных ему самому сетях. Обновленное значение вектора маршрутизатор рассылает своим соседям. Такие алгоритмы хорошо работают только в небольших сетях. В больших сетях они создают излишнюю нагрузку на линии связи.

Алгоритмы состояния каналов связей обеспечивают каждый маршрутизатор информацией, которой достаточно для построения графа связей сети. В таких условиях все маршрутизаторы работают на основании одного и того же графа, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. Каждый маршрутизатор использует граф сети для нахождения оптимальных по некоторому критерию маршрутов до каждой из сетей, входящих в составную сеть.

В результате служебный трафик, создаваемый протоколами, которые построены на основании алгоритмов состояния каналов связи, гораздо менее интенсивный, чем у протоколов, построенных на дистанционно-векторных алгоритмах.

Процесс определения направления продвижения пакета по таблице маршрутизации включает в себя следующие этапы:

1 Первый этап – **поиск конкретного маршрута к узлу**. Полный IP-адрес назначения, извлеченный из продвигаемого пакета, последовательно, строка за строкой сравнивается с содержимым поля адреса назначения таблицы маршрутизации. Если произошло совпадение, то из соответствующей строки извлекаются адрес следующего маршрутизатора и идентификатор выходного интерфейса. На этом просмотр таблицы заканчивается.

2 Если в таблице нет строки с полным адресом назначения, то протокол IP переходит ко второму этапу просмотра – **поиску маршрута к сети назначения**. Из IP-адреса выделяется номер сети, и таблица снова просматривается на предмет совпадения номера сети в какой-либо строке с номером сети из пакета. При совпадении из соответствующей строки таблицы извле-

каются адрес следующего маршрутизатора и идентификатор выходного интерфейса. Просмотр таблицы на этом завершается.

3 Если совпадение не обнаружено в процессе выполнения первых двух этапов, то на третьем этапе средствами протокола IP **выбирается маршрут по умолчанию**. При отсутствии маршрута по умолчанию пакет отбрасывается.

Для большинства маршрутизаторов существуют три основных источника записей в таблице:

– программное обеспечение стека TCP/IP, которое при инициализации маршрутизатора автоматически заносит в таблицу несколько записей, в результате чего формируется минимальная таблица маршрутизации;

– администратор, непосредственно формирующий статические записи;

– протоколы маршрутизации, формирующие динамические записи.

Многообразие источников записей в таблице маршрутизации, а также работа нескольких протоколов динамической маршрутизации на одном маршрутизаторе приводит к тому, что в таблице могут появиться альтернативные маршруты. Для выбора наиболее оптимального из них нельзя использовать метрики – они различны для разных протоколов и не пригодны для сравнения. Поэтому используется **административное расстояние** – это степень надежности источника маршрутной информации (таблица 6.1). Чем меньше значение административного расстояния, тем более надежным считается источник маршрута.

Таблица 6.1 – **Значения административных расстояний некоторых протоколов**

Источник маршрута	Административное расстояние
Подключенный интерфейс	0
Статический маршрут	1
Объединенный маршрут по протоколу EIGRP	5
Внешний протокол BGP	20
Внутренний протокол EIGRP	90
Протокол IGRP	100
Протокол OSPF	110
Протокол RIP	120
Внешний протокол EIGRP	170
Внутренний протокол BGP	200

Протокол маршрутной информации (**Routing Information Protocol**, **RIP**) – это дистанционно-векторный протокол маршрутизации, который предназначен для использования в небольших сетях. Данный протокол предполагает использование в качестве метрик следующие параметры: хопы, значения пропускной способности, вносимые задержки, надежность сетей, а также любые их комбинации.

Процесс построения таблицы маршрутизации при использовании протокола RIP происходит в несколько этапов:

1) каждый маршрутизатор создает собственную минимальную таблицу;

2) рассылка существующей таблицы от каждого маршрутизатора соседям;

3) получение RIP-сообщений от соседей и обработка полученной информации.

Последние два этапа периодически повторяются, пока в сети не установится корректный режим маршрутизации, который означает, что все сети достижимы из любой сети с помощью оптимального маршрута.

При появлении новых сетей маршрутизаторы RIP передают новую информацию в очередном сообщении своим соседям, и постепенно эта информация становится известна всем маршрутизаторам сети. При отключении какой-либо сети протоколом RIP используются следующие механизмы для оповещения маршрутизаторов сети:

– истечение времени жизни маршрута – метод основанный на том, что каждая запись таблицы маршрутизации, полученная по протоколу RIP, имеет время жизни и по истечении времени тайм-аута (180 секунд) будет помечена недействительной;

– указание бесконечного расстояния до отключенной сети, при котором маршрутизатор должен проверить, соответствует ли источник данной информации источнику, от которого ранее поступала информация о данной сети, и если это так, то сеть помечается как недоступная.

Выбор в качестве «бесконечного» расстояния числа 16 обусловлен опасностью зацикливания пакетов в петлях сети в моменты неопределенности. Проблема с петлей, образующейся между соседними маршрутизаторами, решается с помощью **метода расщепления горизонта**, заключающегося в том, что маршрутная информация о некоторой сети, хранящаяся в таблице маршрутизации, никогда не передается тому маршрутизатору, от которого она получена. Однако расщепление горизонта не помогает, если петли образуются не двумя, а большим числом маршрутизаторов. В таких случаях для предотвращения зацикливания пакетов применяются следующие два метода:

– триггерные обновления – метод, который заключается в том, что маршрутизатор, получив данные об изменении метрики до какой-либо сети, не ждет истечения периода передачи таблицы маршрутизации, а передает данные об изменившемся маршруте немедленно, что во многих случаях предотвращает передачу устаревших сведений;

– замораживание изменений – метод, который связан с введением тайм-аута на принятие новых данных о сети, которая только что стала недоступной.

Протокол **выбора кратчайшего пути первым** (**Open Shortest Path First**, **OSPF**) основан на алгоритме состояния связей и обладает многими

свойствами. Это протокол разбивает процедуру построения таблицы маршрутизации на два этапа:

1 Построение и поддержание базы данных состояний связей сети, которые представлены в виде графа (вершины графа – маршрутизаторы и подсети, ребра – связи между ними) за счет обмена между маршрутизаторами той информацией о графе сети, которой каждый из них располагает. При транзитной передаче такой информации маршрутизаторы ее не модифицируют. В результате все маршрутизаторы сети сохраняют в своей памяти идентичные сведения о текущей конфигурации графа связей сети. Для контроля маршрутизаторы OSPF передают друг другу особые сообщения hello каждые 10 секунд. Если сообщения hello перестают поступать от какого-либо маршрутизатора, то его соседи делают вывод о его неработоспособности, вносят коррективы в топологию сети и информируют об этом другие маршрутизаторы.

2 Нахождение оптимальных маршрутов и генерация таблицы маршрутизации производится с помощью итеративного алгоритма Дейкстры. При этом каждый маршрутизатор сети ищет оптимальные маршруты от своих интерфейсов до всех известных ему подсетей и для каждого маршрута запоминает только один шаг, который и заносится в таблицу маршрутизации.

При поиске оптимальных маршрутов протокол OSPF по умолчанию использует метрику, учитывающую пропускную способность каналов связи, но также может учитывать задержки и надежность передачи пакетов каналами связи. Для каждой из метрик протокол OSPF строит отдельную таблицу маршрутизации.

Вычислительная сложность алгоритма Дейкстры предъявляет высокие требования к мощности процессоров маршрутизаторов. И она быстро растет с увеличением размера сети. Для преодоления этого недостатка в протоколе OSPF вводится понятие **области сети** – часть сети, в которой маршрутизаторы строят граф связей только для этой области. Между областями информация о связях не передается, а пограничные для областей маршрутизаторы обмениваются только информацией об адресах сетей, имеющихся в каждой из областей, и расстоянием от пограничного маршрутизатора до каждой сети. При передаче пакетов между областями выбирается один из пограничных маршрутизаторов области, а именно тот, у которого расстояние до нужной сети меньше.

Усовершенствованный внутренний протокол маршрутизации шлюзов (Enhanced Interior Gateway Routing Protocol, EIGRP) – это протокол маршрутизации, объединяющий свойства дистанционно-векторных протоколов и протоколов по состоянию канала связи. Он появился после OSPF и благодаря специальному алгоритму распространения информации об изменениях в топологии сети защищен от зацикливания маршрутов. При этом

EIGRP более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем OSPF.

EIGRP имеет более сложный алгоритм вычисления метрики **DUAL** (**Diffusing Update ALgorithm**), который использует следующие компоненты:

– пропускная способность – минимальная пропускная способность участка сети маршрута (*B*);

– задержка – суммарная задержка на всём пути маршрута (*D*);

– надежность – наихудший показатель надёжности на всём пути маршрута (*R*);

– загруженность – наихудший показатель загруженности интерфейса на всём пути маршрута (*L*);

– минимальный размер **максимальной единицы передачи** (**Maximum Transmission Unit**, **MTU**) на всём пути маршрута – это максимальный размер пакета, который может быть передан через сеть без фрагментации (в расчете метрики не участвует).

Согласно DUAL расчет метрики производится по следующей формуле:

$$M = (K_1 BW + K_2 \frac{BW}{256 - L} + 256 K_3 \cdot D)\left(\frac{K_4}{K_5 + R}\right), \qquad (6.1)$$

где K_i – коэффициенты, используемые для расчета метрики (по умолчанию коэффициенты EIGRP имеют следующие значения: $K_1 = 1$; $K_2 = 0$; $K_3 = 1$; $K_4 = 0$; $K_5 = 0$);

BW – промежуточный параметр, зависящий от пропускной способности и вычисляемый по следующей формуле

$$BW = \frac{256 \cdot 10^7}{B}. \qquad (6.2)$$

Каждый маршрутизатор сети на основании рассчитанных метрик для каждой известной ему сети назначения определяет следующие два параметра:

– **Advertised distance** (***AD***) – величина метрики между соседним маршрутизатором, который предлагает маршрут к сети назначения, и сетью назначения.

– **Feasible distance** (***FD***) – величина метрики от данного маршрутизатора до сети назначения (равна сумме *AD* и величине метрики до маршрутизатора, который использовался при получении величины *AD*).

На основании *AD* и *FD* маршрутизатор для каждой сети назначения определяет первый маршрутизатор основного маршрута – **successor** (маршрутизатор с самым минимальным значением *FD* до сети назначения), а также первый маршрутизатор резервного маршрута – **feasible successor** (маршрутизатор с значением *AD* меньшим, чем *FD* основного маршрута).

Для своей работы EIGRP использует пять типов сообщений:

– hello – маршрутизаторы используют широковещательные hello-пакеты без подтверждения для обнаружения соседей;

– update – сообщения, в которых содержится информация об изменении маршрутов, отправляются только маршрутизаторам, которых касается обновление;

– query – когда маршрутизатор выполняет подсчет маршрута и у него нет feasible successor, он отправляет query-пакет своим соседям для того, чтобы определить, нет ли feasible successor для этого пункта назначения у них;

– reply – маршрутизатор отправляет reply-пакет в ответ на query-пакет;

– ACK – пакет, который подтверждает получение пакетов update, query и reply.

При маршрутизации в крупных составных сетях необходимо использовать другие подходы, которые базируются на разбиении сети на **автономные системы** (**Autonomous System**, **AS**) – это совокупности сетей под единым административным управлением, обеспечивающим общую для всех входящих в автономную систему маршрутизаторов политику маршрутизации. Номер автономной системы состоит из 16 разрядов и никак не связан с префиксами IP-адресов входящих в нее сетей. Выбор маршрута между автономными системами осуществляют внешние шлюзы, которые соединяют автономные системы между собой. Для этого они используют внешние шлюзовые протоколы.

Пограничный (**внешний**) **шлюзовой протокол** (**Border Gateway Protocol**, **BGP**) в версии 4 является в настоящее время основным протоколом обмена маршрутной информацией между автономными системами Интернета.

Внутри каждой автономной системы может применяться любой из существующих протоколов маршрутизации, в то время как между автономными системами всегда применяется один и тот же протокол.

Маршрутизатор взаимодействует с другими маршрутизаторами по протоколу BGP только в том случае, если администратор явно указывает при конфигурировании, что эти маршрутизаторы являются его соседями – такой способ взаимодействия удобен в ситуации, когда маршрутизаторы, обменивающиеся маршрутной информацией, принадлежат разным поставщикам услуг.

Основным сообщением протокола BGP является сообщение update, с помощью которого маршрутизатор сообщает маршрутизатору соседней автономной системы о достижимости сетей, относящихся к его собственной автономной системе. Такое сообщение является триггерным – оно посылается только тогда, когда в автономной системе появляются новые сети или новые пути к ним, а также если исчезают существовавшие сети или пути.

6.4 Протоколы транспортного уровня

Транспортный уровень стека TCP/IP может предоставлять вышележащему уровню два типа сервиса:

– доставку по возможности или с максимальными усилиями обеспечивает **протокол пользовательских дейтаграмм (User Datagram Protocol, UDP)**;

– гарантированную доставку обеспечивает **протокол управления передачей (Transmission Control Protocol, TCP)**.

Оба эти протокола ведут для каждого приложения две системные очереди: очередь поступающих к приложению данных из сети и отправляемых этим приложением данных в сеть. Такие системные очереди называются **портами**, которым для идентификации присваиваются номера. За популярными системными службами закрепляются стандартные назначенные «хорошо известные» номера, которые закрепляются и публикуются в стандартах Интернета (номера от 0 до 1023 являются уникальными в пределах Интернета и закрепляются за приложениями централизованно). Для остальных приложений номера портов (от 1024 до 65535) либо назначаются локально разработчиками этих приложений, либо выделяются динамически из пула свободных номеров операционной системой. Приложения, передающие данные на уровень IP по протоколу UDP, получают номера, называемые UDP-портами, а по протоколу TCP – TCP-порты. Никакой связи между назначенными номерами TCP- и UDP-портов нет.

Стандартные назначенные номера портов уникально идентифицируют тип «хорошо известного» приложения, но они не могут использоваться для однозначной идентификации прикладных процессов, связанных с каждым из этих типов приложений. Это связано с тем, что на одном сетевом устройстве могут быть запущены несколько одинаковых приложений, каждому из которых будут соответствовать одинаковые номера портов. Для возможности совместной работы эти приложения связываются с разными IP-адресами. Поэтому прикладной процесс однозначно определяется в пределах сети и в пределах отдельного сетевого устройства парой «IP-адрес – номер порта», которая называется **сокетом**. Сокет, определенный IP-адресом и номером UDP-порта, называется **UDP-сокетом**, а IP-адресом и номером TCP-порта – **TCP-сокетом.**

Протокол UDP является простейшим дейтаграммным протоколом, используемым, если задача надежного обмена данными либо вообще не ставится, либо решается средствами более высокого уровня – прикладным уровнем или пользовательскими приложениями.

Протокол UDP добавляет к каждому отдельному сообщению, поступающему от прикладного уровня, свой 8-байтный заголовок, формируя из этих сообщений собственные протокольные единицы, называемые UDP-

дейтаграммами. После этого протокол UDP передает их нижележащему протоколу IP. Структура заголовка UDP-дейтаграммы представлена на рисунке 6.8.

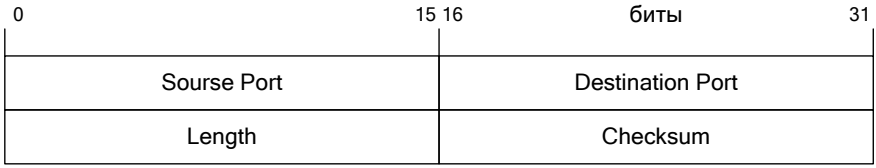

Рисунок 6.8 – Структура заголовка UDP-дейтаграммы

Заголовок UDP состоит из четырех 2-байтных полей:

– **Sourse Port** – номер UDP-порта отправителя;

– **Destination Port** – номер UDP-порта получателя;

– **Length** – длина дейтаграммы;

– **Checksum** – контрольная сумма.

Функции протокола UDP сводятся к простой передаче данных между прикладным и сетевым уровнями, а также примитивному контролю искажений в передаваемых данных, при котором протокол UDP только диагностирует, но не исправляет ошибку. Если контрольная сумма показывает, что в поле данных UDP-дейтаграммы произошла ошибка, то протокол UDP просто отбрасывает поврежденную дейтаграмму.

Протокол TCP основан на логическом соединении, что позволяет ему обеспечивать гарантированную доставку данных, используя в качестве инструмента ненадежный дейтаграммный сервис протокола IP. Установление логического соединения позволяет нумеровать пакеты, подтверждать их прием квитанциями, организовывать в случае потери повторные передачи, распознавать и уничтожать дубликаты, доставлять прикладному уровню пакеты в том порядке, в котором они были отправлены. Благодаря этому протоколу прикладные процессы двух сетевых устройств могут поддерживать обмен данными в дуплексном режиме. TCP дает возможность без ошибок доставить сформированный на одном из сетевых устройств поток байтов на любое другое сетевое устройство, входящее в составную сеть.

Логическое TCP-соединение однозначно идентифицируется парой сокетов, определенных для этого соединения двумя взаимодействующими процессами.

Протокол TCP рассматривает информацию, поступающую к нему от прикладных процессов, как неструктурированный поток байтов, данные которого буферизуются средствами TCP. Для передачи на сетевой уровень из буфера выбирается определенная непрерывная часть данных, которая

называется **TCP-сегментом** и снабжается заголовком. Структура заголовка TCP-сегмента представлена на рисунке 6.9.

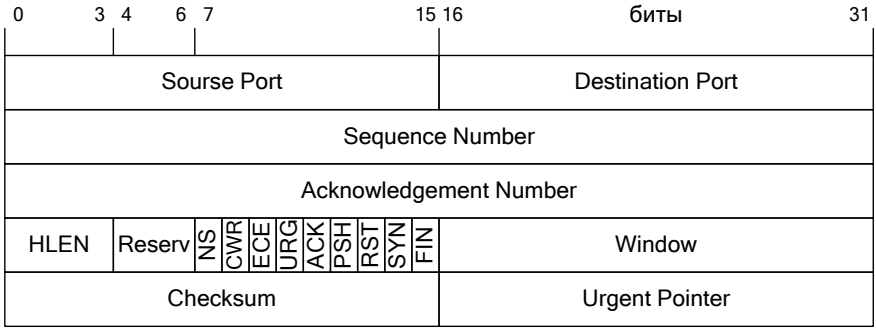

Рисунок 6.9 – Структура заголовка TCP-сегмента

В состав заголовка TCP-сегмента входят следующие поля:

– **Sourse Port** – номер TCP-порта отправителя;

– **Destination Port** – номер TCP-порта получателя;

– **Sequence Number** – последовательный номер – номер первого байта данных в передаваемом сегменте, который определяет положение данных сегмента относительно всего объема передаваемых данных;

– **Acknowledgement Number** – подтвержденный номер – увеличенный на единицу максимальный номер полученного приемником байта (номер ожидаемого байта);

– **HLEN** (**Head Length**) – длина заголовка – количество 32-битных строк в заголовке (для стандартного заголовка TCP без дополнительных параметров, как это представлено на рисунке 42, равно 0101);

– **Reserv** – три зарезервированных бита, имеющих значение 000;

– **NS** (**Nonce Sum**) – бит используется для улучшения работы механизма явного уведомления о перегрузке (ECN);

– **CWR** (**Congestion Window Reduced**) – флаг устанавливается отправителем, чтобы показать, что TCP-фрагмент был получен с установленным полем ECE;

– **ECE** (**ECN-Echo**) – при установленном флаге SYN указывает на то, что отправитель пакета поддерживает ECN, при сброшенном флаге SYN – на то, что IP-пакет с подтверждением перегрузки (Congestion Experienced, CE) в поле ECN заголовка был получен во время обычной передачи, что означает перегрузку сети для TCP-отправителя;

– **URG** (**Urgent pointer**) **–** флаг срочного сообщения;

– **ACK** (**Acknowledgement**) **–** признак квитанции на принятый сегмент;

– **PSH (Push) –** признак запроса на отправку сообщения без ожидания заполнения буфера;

– **RST (Reset the connection) –** признак запроса на сброс соединения;

– **SYN (Synchronize sequence numbers) –** признак сообщения, используемого для синхронизации счетчиков переданных данных при установлении соединения;

– **FIN (Final) –** признак достижения передающей стороной последнего байта в потоке передаваемых данных;

– **Window** – окно – количество байт данных, которые ожидает отправитель данного сегмента, начиная с байта, номер которого указан в поле Acknowledgement Number.

– **Checksum** – контрольная сумма;

– **Urgent Pointer –** если установлен флаг URG, то данное поле содержит численное значение положительного смещения, указывающее на последний байт срочных данных, которые необходимо принять в первую очередь.

При установлении TCP соединения в первую очередь необходимо определить параметры предстоящего обмена данными, для этого каждая сторона соединения посылает противоположной стороне следующие параметры:

– максимальный размер сегмента, который она готова принимать;

– начальный размер окна – максимальный объем данных, который она разрешает другой стороне передавать в свою сторону без подтверждения квитанциями;

– начальный порядковый номер байта пересылаемых данных.

Соединение устанавливается по инициативе клиентской части приложения, TCP которого посылает сегмент-запрос на установление соединения протоколу TCP, работающему на стороне сервера. В этом запросе содержится флаг SYN, установленный в 1. Серверная сторона, получив запрос, выделяет ресурсы для обслуживания клиента и посылает клиенту сегмент с флагами ACK и SYN. В ответ клиент посылает сегмент с флагом ACK и переходит в состояние установленного логического соединения. Получив флаг ACK, сервер также переходит в состояние установленного логического соединения.

Соединение может быть разорвано в любой момент по инициативе любой стороны. Для этого клиент или сервер посылают сегмент с флагом FIN и получают в ответ сегмент с флагом ACK. Точно такой же обмен сегментами должен быть произведен в противоположном направлении. Соединение считается закрытым по прошествии некоторого времени, в течение которого сторона-инициатор убеждается, что ее завершающий сигнал ACK дошел нормально и не вызвал никаких «аварийных» сообщений с противоположной стороны.

Для организации надежного обмена данными необходимо подтверждать правильный прием сегментов. Для этого используется **передача с квитированием,** при которой источник отсылает данные, а приемник подтверждает их получение квитанциями. Если источник вовремя не получает квитанции на переданные данные, то он передает их повторно. Все методы с квитированием можно разделить на два класса:

– **методы простоя источника**, при которых источник передает сегмент, дожидается квитанции от приемника и только после этого посылал следующий сегмент;

– **методы скользящего окна**, при которых для повышения скорости передачи данных источнику разрешается передать некоторое количество сегментов, не дожидаясь прихода на эти сегменты квитанций.

В протоколе TCP используется метод скользящего окна. Когда источник посылает TCP-сегмент, он помещает в поле Sequence Number номер первого байта данного сегмента, который служит идентификатором сегмента. На основании этих номеров приемник TCP-сегмента отличает данный сегмент от других и позиционирует полученный фрагмент относительно общего потока байтов.

В качестве квитанции приемник сегмента отсылает ответный сегмент, в поле Acknowledgement Number которого он помещает число, на единицу превышающее максимальный номер байта в полученном сегменте. Этот номер также указывает на следующий ожидаемый байт данных. Один и тот же TCP-сегмент может нести в себе пользовательские данные и квитанцию, которой подтверждается получение данных от противоположной стороны. Квитанция в протоколе TCP посылается только в случае правильного приема данных. Отсутствие квитанции говорит о потере сегмента, его искажении или потере квитанции.

В связи с тем, что протокол TCP является дуплексным, каждая сторона одновременно выступает как источник, так и приемник. У каждой стороны есть три буфера: первый – для хранения принятых сегментов, второй – для сегментов, которые предстоит отправить, третий – для хранения копий отправленных сегментов, но квитанции о получении которых еще не поступили. Когда протокол TCP передает в сеть сегмент, он помещает его копию в буфер и запускает таймер. Когда приходит квитанция на этот сегмент, соответствующая копия удаляется из очереди. Если же квитанция не приходит до истечения срока, то сегмент посылается повторно из буфера.

6.7 Аутентификация в компьютерных сетях

Для организации безопасной передачи информации между сетевыми устройствами, взаимодействующими через небезопасную открытую сеть, необходимо организовать защищенный канал, который подразумевает выполнение трех основных функций:

– взаимная аутентификация субъектов при установлении соединения;

– защита передаваемых по каналу сообщений от несанкционированного доступа – шифрование;

– подтверждение целостности поступающих по каналу сообщений.

Вторая и третья функции были рассмотрены в разделе, посвященном методам защиты информации на физическом уровне. Рассмотрим оставшуюся функцию.

Идентификация – это процесс распознавания субъектов с помощью заранее присвоенных им идентификаторов. **Аутентификация** – это процесс, заключающийся в проверке подлинности субъекта. Таким образом, **средство аутентификации** – это программный модуль или аппаратно-программное устройство, которое обеспечивает проверку подлинности субъекта, т. е. устанавливает, является ли он тем, за кого себя выдает. В качестве субъектов могут выступать пользователи информационной системы, прикладные или системные процессы. Объекты, к которым субъекты получают доступ – это информационные ресурсы.

В общем случае существуют три класса опознания, на основании которых строятся все средства аутентификации. Эти классы базируются на:

– условных, заранее присваиваемых признаках (сведениях), известных субъекту;

– физических средствах, действующих аналогично физическому ключу;

– индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц.

Парольные методы проверки подлинности субъектов при входе в систему могут применяться на основе простых и динамически изменяющихся паролей.

При использовании метода **простого пароля** его значение не изменяется в течение установленного администратором службы безопасности времени действия. Такой метод заключается в том, что субъект набирает только ему известную комбинацию символов. Данный пароль сравнивается с эталонным, хранящимся в системе, и при положительном результате проверки субъект получает к ней доступ. Данная схема опознания является простой с точки зрения реализации, но имеет два недостатка:

– сложность запоминания для большинства субъектов произвольного набора символов, используемого в качестве пароля;

– уязвимость пароля при наборе.

Модернизацией схемы простого пароля является **схема паролей однократного использования**, в которой субъекту выдается список из N паролей. При каждом обращении к системе синхронно используется пароль с текущим номером, а все пароли с предыдущими номерами вычеркиваются.

Данная схема обеспечивает большую степень безопасности, является более сложной и также имеет следующие недостатки:

– субъект должен помнить или иметь при себе весь список паролей и следить за текущим паролем;

– в случае, если встречается ошибка в процессе передачи, трудно определить, следует ли передавать тот же самый пароль или послать следующий;

– необходимо иметь разные таблицы паролей для каждого субъекта, так как может произойти рассинхронизация работы.

При использовании **динамически изменяющегося пароля** его значение для каждого нового сеанса работы изменяется по определённым правилам. Методы проверки подлинности на основе динамически изменяющегося пароля обеспечивают большую безопасность, так как частота смены паролей в них максимальна. При этом каждый следующий пароль по отношению к предыдущему изменяется по правилам, зависящим от используемого метода проверки подлинности.

К следующему классу средств аутентификации относятся методы, **основывающиеся на физических средствах**, которые имеет при себе субъект, обращающийся к системе. К ним относятся идентификационные карты с перфорированным или магнитным кодом, а также ряд активных устройств, называемых электронными ключами, включающих в себя: смарт-карты с процессорами, USB-брелоки, устройства Touch Memory и т. п.

В магнитных картах информация записывается на нескольких дорожках магнитного слоя и представляет собой данные, используемые для идентификации. К этим данным относятся: номер субъекта или его имя, пароль, количество допустимых использований карты и т. д. Наряду с очевидной простотой использования магнитные карты обладают низкой защищенностью от копирования содержимого. Для защиты от подделки или копирования карточки требуют сложной технологии их изготовления и, соответственно, сложной аппаратуры для считывания записанной на них информации. При любых способах достичь абсолютной защиты от копирования магнитных карт практически невозможно, так как носитель всегда открыт для доступа посторонних лиц.

Электронный ключ в самом общем смысле представляет собой физический носитель идентификатора субъекта, его пароля. В отличие от парольных систем при использовании электронного ключа субъект имеет ряд преимуществ:

– ему не надо запоминать значение пароля, так как пароль записан в ключе;

– он освобожден от функции защиты пароля от компрометации при его вводе, так как пароль считывается из ключа;

– все функции по защите от подделки пароля или его несанкционированного использования возлагаются на электронный ключ;

– пароль можно сделать сколь угодно большим, так как субъект непосредственно с ним не работает.

В силу того, что, как и идентификационная магнитная карта, электронный ключ является физическим средством хранения идентификатора субъекта, его можно скопировать и подделать. Все многообразие электронных ключей классифицируется по основному признаку, определяющему их защищенность от копирования и подделки, так как быстродействие, объем хранимого идентификатора, габариты и другие характеристики являются, по существу, производными от него.

Ключ, который невозможно подделать, является активным устройством, содержащим в памяти идентификатор, не доступный для чтения. Например, электронный ключ может содержать криптосхему, в которую при изготовлении загружается случайное значение ключа. Вне криптосхемы это значение нигде не записывается. Устройство можно сконструировать таким образом, что попытка прочесть ключ приводит к его уничтожению. Устройство такого типа обладает «индивидуальностью», которую можно выявить только посредством задания устройству различных цифровых значений и записи его ответов.

К **биометрическому классу** средств аутентификации относятся методы, базирующиеся на определении индивидуальных характеристик, присущих каждому субъекту и позволяющих выделить его среди других. Биометрические методы аутентификации можно разделить на две большие категории – статические и динамические. К первой относятся методы, основанные на физиологической характеристике субъекта, т. е. неотъемлемой, уникальной характеристике, данной ему от рождения. Здесь анализируются такие признаки, как отпечатки пальцев, черты лица, структура глаза (сетчатки или радужной оболочки), ладонь, форма руки и т. п.

К группе динамических относят методы, которые основываются на поведенческой характеристике субъекта. Они используют особенности, характерные для подсознательных движений в процессе воспроизведения какого-либо действия. К таким характеристикам относятся голос субъекта, особенности его подписи, динамические параметры письма, особенности ввода текста с клавиатуры.

В основе метода опознания по отпечатку пальца лежит уникальность рисунка капиллярных узоров на пальцах у каждого субъекта. Устройство регистрирует некоторые участки рисунка, уникальные для конкретного отпечатка, и определяет их взаимное расположение или обрабатывается изображение всего отпечатка пальца.

Метод опознания субъекта по лицу основан на уникальности черт лица. Метод заключается в преобразовании черт конкретного лица в алгоритмическую модель, которая сравнивается или с фотографией на пропуске, или с содержимым базы фотографических данных.

Метод опознания субъекта по радужной оболочке глаза основан на уникальности рисунка радужной оболочки каждого субъекта. Радужная оболочка субъекта сканируется, разворачивается и преобразуется в цифровую последовательность. Подтверждение подлинности субъекта происходит на основании сравнения полученной цифровой последовательности с эталонной.

Метод опознания по образцу голоса основан на том, что у каждого субъекта неповторимый голосовой рисунок, который зависит от пола, физических особенностей, типа строения голосовых связок, полости носа, формы рта, таких характеристик, как частота и амплитуда. Этот метод построен на выделении различных сочетаний частотных и статистических характеристик голоса.

Методы аутентификации субъектов применяются для удаленного опознания субъектов. При этом проблемой становится передача по незащищенной сети аутентификатора субъекта, а также доверие удаленному средству, которое будет осуществлять опознание субъекта. В сетевых технологиях принято применять **строгую аутентификацию**, в процессе которой используются методы шифрования, а аутентификатор не передается по сети в открытом виде. Вместо аутентификатора может использоваться его хэш-код, полученный в результате применения односторонней функции хеширования.

Для реализации удаленной аутентификации в сетях используются **протоколы аутентификации**. Общая схема, используемая практически всеми протоколами аутентификации, состоит из следующих действий:

– Алиса желает установить защищенное соединение с Бобом или считающимся надежным **Центром распространения ключей** (**Key Distribution Center**, **KDC**);

– между сторонами пересылаются служебные сообщения;

– весь обмен данными шифруется с помощью одного из симметричных алгоритмов шифрования, так как их производительность намного выше производительности асимметричных алгоритмов;

– с помощью асимметричного метода шифрования происходит распространение секретного сеансового ключа, который будет использоваться для дальнейшего обмена информацией;

– по завершении работы протока Алиса должна быть уверена, что установлено соединение с Бобом, а Боб – с Алисой.

На рисунке 6.10 представлена упрощенная форма протокола аутентификации Отуэя-Риса, который был опубликован в 1987 году.

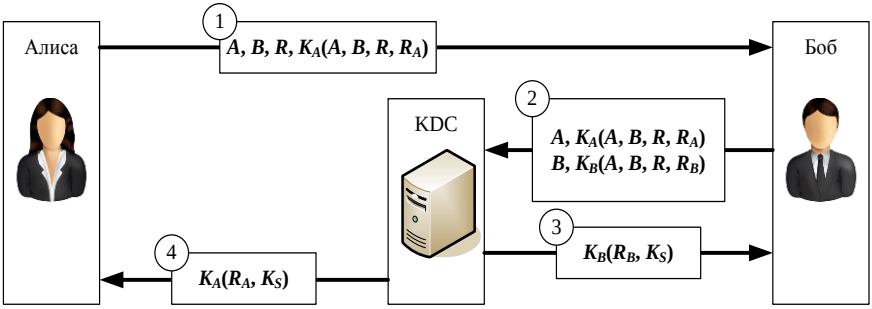

Рисунок 6.10 – Протокол аутентификации Отуэя-Риса

На рисунке используются следующие условные обозначения:

– A и B – субъекты аутентификации Алиса и Боб соответственно;

– R_i – оклик субъекта, где индекс означает его отправителя, при отсутствии индекса оклик является общим;

– K_i – ключ субъекта (для симметричного шифрования), где индекс означает владельца ключа;

– $K_i()$ – шифрование симметричным методом данных, указанных в скобочках, ключом K_i;

– E_i – открытый ключ субъекта (для асимметричного шифрования), где индекс означает владельца ключа;

– $E_i()$ – шифрование асимметричным методом данных, указанных в скобочках, ключом E_i;

– K_S – сеансовый ключ.

В протоколе Отуэя-Риса Алиса начинает с формирования пары случайных номеров: R, который будет использоваться в качестве общего оклика, и R_A, который Алиса будет использовать в качестве оклика Боба. Получив это сообщение, Боб формирует новое сообщение, используя зашифрованную часть сообщения Алисы $K_A(A, B, R, R_A)$ и аналогичную собственную часть $K_B(A, B, R, R_B)$. Обе эти части сообщения, зашифрованные ключами K_A и K_B, идентифицируют Алису и Боба, содержат общий и индивидуальные оклики.

Центр распространения ключей является доверенным сервером аутентификации для Алисы и Боба и владеет информацией о их ключах. Поэтому он расшифровывает обе части сообщения, поступившего от Боба, проверяет, совпадают ли общие оклики R в обеих частях сообщения. Если они не совпадают, то это говорит о возможной атаке на сервер аутентификации. Если оба общих оклика R совпадают, KDC считает сообщение, полученное от Боба, достоверным. Затем он генерирует сеансовый ключ K_S и распро-

страняет его между Алисой и Бобом, зашифровав соответствующими ключами Алисы и Боба. Каждое сообщение также содержит оклик субъекта, в доказательство того, что эти сообщения посланы KDC, а не злоумышленником. В результате выполнения алгоритма Алиса и Боб обладают одним и тем же сеансовым ключом и могут начать обмен информацией.

Аутентификация также может выполняться с помощью асимметричных методов шифрования (рисунок 6.11). Для этого оба субъекта (Алиса и Боб) должны быть пользователями системы, которая обслуживает шифрование с открытыми ключами, обеспечивает генерацию надежных закрытых и открытых ключей, а также распространение открытых ключей по запросам законных пользователей системы.

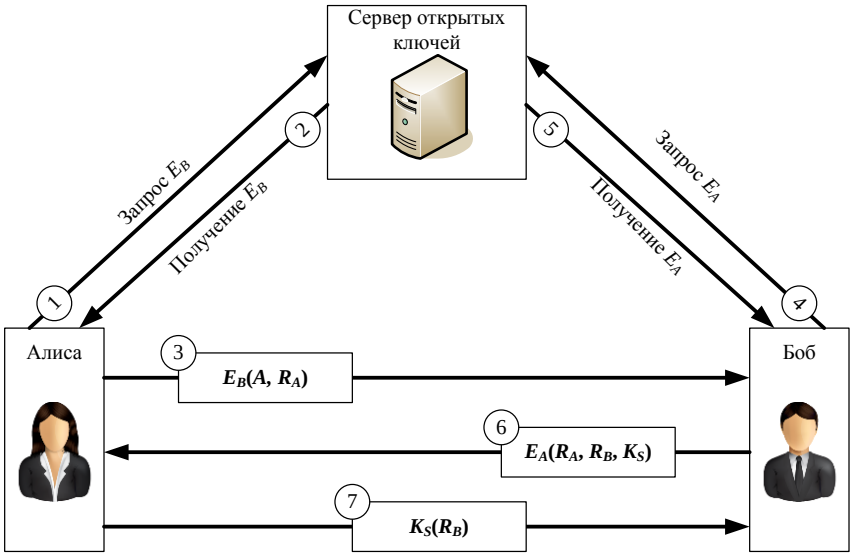

Рисунок 6.11 – Протокол аутентификации с помощью открытого ключа

Вначале Алиса запрашивает у сервера открытый ключ Боба, получает его и с его помощью шифрует свое сообщение Бобу с заявкой на установление соединения. Боб расшифровывает сообщение от Алисы своим секретным ключом, запрашивает у сервера открытый ключ Алисы, генерирует сеансовый ключ для шифрования симметричным методом последующих сообщений, которые будут передаваться Алисе. После этого Боб шифрует открытым ключом Алисы ответное сообщение на ее запрос. Полученное сообщение Алиса расшифровывает своим секретным ключом, убеждается с помощью оклика, что сообщение действительно получено от Боба и подтверждает установление соединения с использованием сеансового ключа.

6.8 Технологии разграничения доступа

Средства аутентификации необходимы для организации системы контроля доступа, которая решает, какие их операций разрешены при взаимодействии субъектов и объектов. После того как субъект, пройдя аутентификацию, доказал свою легальность, ему предоставляется некоторый набор прав по отношению к защищаемым объектам.

Наделение легальных субъектов правами доступа к объектам называется **авторизацией**. Процедура приведения авторизации в действие называется **разграничением (управлением) доступом**.

Существует несколько подходов к процессу организации разграничения доступа:

1) **списки контроля доступа** (**Access Control Lists**, **ACL**) – заключается в том, что для каждого защищаемого объекта составляется список всех тех субъектов, которым предоставлено право доступа к нему, или, наоборот, для каждого субъекта составляется список тех защищаемых объектов, к которым ему предоставлено право доступа;

2) **избирательное** (**дискреционное**) **управление доступом** (**Discretionary Access Control**, **DAC**) – предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы субъектов, по столбцам – идентификаторы защищаемых объектов, а в ячейках содержится информация об уровне полномочий соответствующего субъекта относительно соответствующего объекта;

3) **полномочное** (**мандатное**) **управление доступом** (**Mandatory Access Control**, **MAC**) – каждому защищаемому объекту присваивается персональная уникальная метка, после чего доступ к этому объекту будет разрешен только тому субъекту, который в своем запросе предъявит метку объекта (мандат), которую ему может выдать администратор или владелец объекта;

4) **ролевое управление доступом** (**Role Based Access Control**, **RBAC**) – права доступа субъектов к объектам группируются с учётом специфики их применения, образуя роли, набор которых должен соответствовать перечню различных должностей, существующих в организации.

У каждого из представленных подходов к процессу организации разграничения доступа есть свои достоинства и недостатки, а также определенные области применения. Например, недостатком метода разграничения доступа на основе матрицы полномочий является то, что с увеличением масштаба данная матрица может оказаться слишком громоздкой. Ролевая система доступа лучше всего работает в организациях, в которых существует четкое распределение должностных обязанностей.

Ролевую систему управления доступом легче администрировать и контролировать, чем дискреционную. В ролевой системе права доступа выдаются в виде интегрированного набора разрешений, рассчитанных на воз-

можность выполнения некоторых относительно сложных операций. В настоящее время ролевое управление доступом является наиболее перспективным в силу того, что в нем сочетаются черты мандатного и дискреционного методов. Ролевой доступ является централизованным методом (как и в мандатном методе, пользователь лишен возможности управлять назначением прав), но более гибким, чем мандатный. Занимая промежуточное положение между мандатным и дискреционным методами, ролевое управление доступом уступает им обоим в масштабируемости.

6.9 IPSec

IPSec (**IP Security**) – это согласованный набор открытых стандартов, в ядро которого входят три протокола:

– **AH** (**Authentication Header**) – заголовок аутентификации – гарантирует целостность и аутентичность данных, кроме того может проверять дублирование пакетов;

– **ESP** (**Encapsulating Security Payload**) – инкапсуляция зашифрованных данных – шифрует передаваемые между сетевыми устройствами данные, обеспечивая конфиденциальность, может также поддерживать аутентификацию и целостность данных;

– **IKE** (**Internet Key Exchange**) – обмен ключами Интернета – предоставляет сетевым устройствам защищенное однонаправленное логическое соединение для распределения секретных ключей, необходимых для работы других протоколов, – **безопасную ассоциацию** (**Security Association**, **SA**).

Стандарты IPSec позволяют сетевым устройствам использовать любое количество безопасных ассоциаций с различными характеристиками, что дает возможность выбирать нужную степень детализации защиты. Установление безопасной ассоциации начинается с взаимной аутентификации сторон. Выбираемые далее параметры SA определяют, какой из двух протоколов, AH или ESP, будет применяться для защиты данных, и какие из доступных функций он будет выполнять.

Протокол IPSec допускает как автоматическое, так и ручное установление безопасной ассоциации. При ручном способе администратор конфигурирует конечные узлы так, чтобы они поддерживали согласованные параметры ассоциации, включая секретные ключи. При автоматической процедуре установления SA протоколы IKE, работающие на разных сетевых устройствах, выбирают параметры в ходе переговорного процесса.

IPSec может работать в двух режимах: транспортном и туннелирования. В транспортном режиме заголовок IPSec вставляется сразу за заголовком IP. В поле Protocol заголовка IP помещается комбинация (00110010 для ESP и 00110011 для AH), которая указывает на то, что далее следует заголовок IPSec, в котором содержится информация, касающаяся безопасности.

В режиме туннелирования весь IP-пакет вместе с заголовком вставляется внутрь нового IP-пакета с совершенно новым заголовком, что в большей степени увеличивает общий объем IP-пакетов по сравнению с транспортным режимом.

Возможны три схемы применения протокола IPSec: «хост-хост», «шлюз-шлюз» и «хост-шлюз» (рисунок 6.12).

В схеме «хост-хост» безопасная ассоциация устанавливается между двумя сетевыми устройствами и чаще всего используется транспортный режим защиты. При этом протокол IPSec работает на каждом из них.

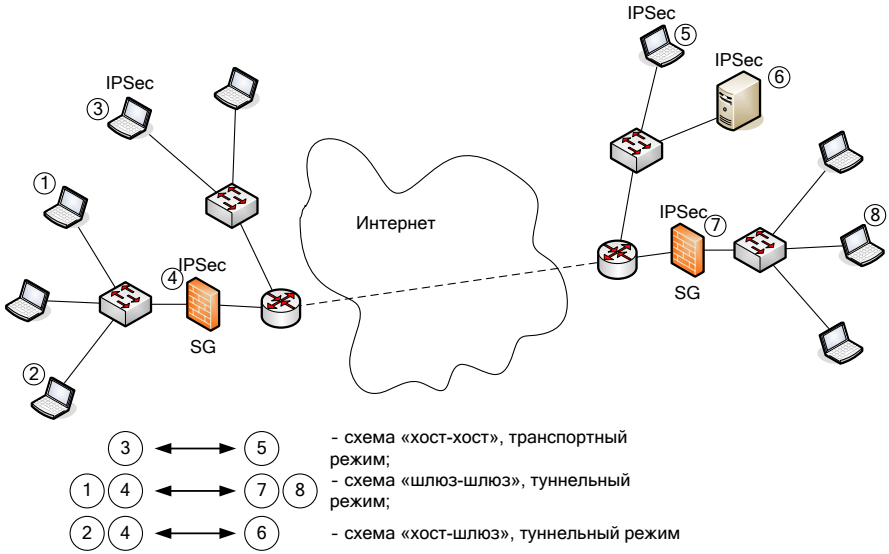

Рисунок 6.12 – Схемы работы IPSec

В схеме «шлюз-шлюз» защищенный канал устанавливается между двумя промежуточными узлами – **шлюзами безопасности** (**Security Gateway**, **SG**), на каждом из которых работает протокол IPSec и которым доступен только туннельный режим работы. Защищенный обмен данными может происходить между любыми двумя сетевыми устройствами локальных сетей, которые соединены с глобальной сетью с помощью шлюзов безопасности.

Схема «хост-шлюз» часто применяется при удаленном доступе. В этом случае защищенный канал прокладывается между удаленным сетевым устройством, на котором работает протокол IPSec, и шлюзом, защищающим трафик для всех сетевых устройств локальной сети организации.

Контрольные вопросы

1 Какие уровни модели OSI охватывают протоколы стека TCP/IP?

2 Назовите основные протоколы стека протоколов TCP/IP.

3 Приведите классификацию IP-адресов.

4 Для каких целей применяется маска вместе с IP-адресом?

5 Назовите основные поля заголовка IPv4.

6 Назовите основные поля заголовка IPv6.

7 Для каких целей применяется DHCP?

8 Назовите поля сообщения ICMP.

9 Для каких целей используются протоколы разрешения адресов?

10 Для чего предназначена DNS?

11 Опишите принцип работы ARP.

12 Назовите классы протоколов динамической маршрутизации.

13 Назовите этапы определения направления продвижения пакета по таблице маршрутизации.

14 Для каких целей при динамической маршрутизации используется административное расстояние?

15 Поясните принцип работы RIP.

16 Каковы основные отличия OSPF от RIP?

17 Каково назначение BGP?

18 Поясните принципы работы UDP.

19 Приведите особенности работы TCP.

20 Что такое сокет?

21 Назовите основные поля заголовка TCP-сегмента.

22 Какие методы применяются для организации надежного обмена данными на транспортном уровне модели OSI?

23 Что такое идентификация?

24 Что такое аутентификация?

25 Назовите классы средств аутентификации.

26 Поясните процесс удаленной аутентификации с использованием центра распределения ключей.

27 Поясните процесс удаленной аутентификации с использованием асимметричного шифрования.

28 Опишите способы организации разграничения доступа.

29 Что такое IPSec?

30 Назовите основные схемы работы IPSec.

7 СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ СЛУЖБЫ И ИХ БЕЗОПАСНОСТЬ

Сетевые службы чаще всего представляют собой распределенные приложения, включающие две части: клиентскую и серверную, которые могут выполняться как на одном сетевом устройстве, так и на разных. Один сервер обслуживает обычно большое число клиентов. Принципиальной разницей между клиентом и сервером является то, что инициатором всегда выступает клиент, а сервер всегда находится в режиме пассивного ожидания запросов. Клиентами сетевых служб могут быть другие сетевые службы. Ключевой составляющей клиентской части сетевой службы является пользовательский интерфейс.

Взаимодействие клиента и сервера, расположенных на разных сетевых устройствах, может выполняться только путем передачи сообщений через сеть в соответствии с выбранным протоколом прикладного уровня модели OSI.

По типам предоставляемых услуг сетевые службы делят на несколько групп:

– службы для конечных пользователей и их приложений;

– службы, обеспечивающие безопасность сети;

– службы, предназначенные для конфигурирования и управления сетевыми устройствами;

– службы, автоматизирующие работу сетевых устройств;

– службы поддержки распределенных вычислений.

7.1 Веб-служба

Сетевая служба WWW (**World Wide Web**) или **веб-служба** была изобретена в 1989 году Тимом Бернерсом-Ли и Робертом Кайо. Эта служба предоставляет возможность поиска нужных данных и доступа к ним, а также позволяет размещать собственную информацию в виде веб-страниц. **Веб-страница** (веб-документ) состоит из основного файла, написанного на **языке разметки гипертекста** (**HyperText Markup Language**, **HTML**) и некоторого количества ссылок на другие объекты, которыми могут быть прочие HTML-файлы, изображения, аудио- и видеофайлы.

В качестве клиентской части веб-службы выступает специальное приложение – браузер, которое устанавливается на компьютере пользователя и предназначено для просмотра веб-страниц. Одной из важных функций брау-

зера является поддержание графического пользовательского интерфейса, через который пользователь получает доступ к широкому набору услуг по поиску и просмотру информации.

Браузер находит веб-страницы и отдельные объекты по **унифицированным указателям ресурсов** (**Uniform Resource Locator**, **URL**), в котором можно выделить тип протокола доступа, DNS-имя сервера и путь к объекту. Например, URL https://www.bsut.by/rosters/personal/satirev включает в себя: тип протокола (https), DNS-имя сервера (www.bsut.by) и путь к объекту (/rosters/personal/satirev).

Веб-сервер – это приложение, обеспечивающее доступ к хранимым объектам по URL-адресам. Веб-сервер должен постоянно находиться в активном состоянии и прослушивать TCP-порт 80, который является назначенным портом **протокола передачи гипертекста** (**HyperText Transfer Protocol**, **HTTP**). С получением запроса от клиента сервер устанавливает TCP-соединение и получает от клиента имя объекта, который запрашивает пользователь. Затем сервер находит файл этого объекта, а также другие связанные с ним объекты, и отсылает их по TCP-соединению клиенту. Получив объекты от сервера, веб-браузер отображает их на экране компьютера.

Клиент и сервер веб-службы взаимодействуют друг с другом по протоколу HTTP, обмениваясь при этом текстовыми сообщениями стандартного формата в кодировке ASCII. HTTP-сообщения бывают двух типов – запросы и ответы. Они имеют единую обобщенную структуру, состоящую из трех частей: обязательной стартовой строки, а также необязательных заголовков и тела сообщения.

7.2 Почтовая служба

Сетевая почтовая служба – это распределенное приложение, которое предоставляет возможность пользователям сети обмениваться электронными сообщениями.

Почтовый клиент, который всегда располагается на компьютере пользователя, – это программа, предназначенная для поддержания пользовательского интерфейса, а также для предоставления пользователю широкого набора услуг по управлению и пересылке электронных сообщений. Почтовый сервер принимает сообщения от клиентов, для чего постоянно находится в активном состоянии, выполняет буферизацию сообщений, распределение поступивших сообщений по индивидуальным почтовым ящикам клиентов и т. п.

Почтовая служба оперирует **электронными сообщениями** – информационными структурами определенного стандартного формата, которые состоят из двух частей: заголовка и тела сообщения.

Важную роль в расширении возможности электронной почты по передаче мультимедийной информации сыграл стандарт **многоцелевого расши-**

рения почты Интернета (**Multipurpose Internet Mail Extensions**, **MIME**), который описывает структуру сообщения, состоящего из нескольких частей, каждая из которых имеет свои заголовок и тело.

В заголовке каждой части сообщения имеется информация о том, каким образом почтовый клиент должен обрабатывать тело данной части (отображать ее немедленно при открытии сообщения или считать это тело вложением, которое пользователь будет обрабатывать сам). Спецификация **S/MIME** (**Security MIME**) относится к расширениям безопасности и может включать шифрование информации и цифровую подпись, которые используются для обеспечения аутентичности, целостности и конфиденциальности электронного письма.

В качестве средства передачи сообщения почтовая служба Интернета использует **простой протокол передачи почты** (**Simple Mail Transfer Protocol**, **SMTP**). SMTP-клиент работает на сетевом устройстве отправителя, а SMTP-сервер, который постоянно ожидает запросов со стороны SMTP-клиента, – на стороне получателя (в данном случае почтового сервера). Работа протокола SMTP состоит из следующих этапов:

1 При отправке электронного сообщения SMTP-клиент посылает запрос на установление TCP-соединения на порт 25 SMTP-сервера.

2 Если сервер не готов принять сообщение, то он посылает соответствующее сообщение клиенту, который попытается установить повторное соединение, если готов – свои идентификационные данные. Получив идентификационные данные от сервера клиент передает ему почтовые адреса отправителя и получателя. Если имя получателя соответствует формату, то сервер дает согласие на установление SMTP-соединения, и в рамках этого логического канала происходит передача сообщения.

3 Если после приема тела сообщения сервер отвечает командой подтверждения, то это означает, что сервер принял на себя ответственность по дальнейшей передаче сообщения получателю.

Используя одно TCP-соединение, клиент может передать несколько сообщений, предваряя каждое из них указанием почтовых адресов отправителя и получателя. После завершения передачи сообщения TCP- и SMTP-соединения разрываются.

Для того чтобы получить электронное сообщение от сервера используются протоколы доступа к почтовому серверу: **протокол почтового отделения версии 3** (**Post Office Protocol v.3**, **POP3**) или **протокол доступа к электронной почте Интернета** (**Internet Mail Access Protocol**, **IMAP**). Оба этих протокола относятся к протоколам, ориентированным на прием данных. Инициатором передачи сообщений от почтового сервера почтовому клиенту по протоколу POP3 или IMAP является клиент. Почтовый сервер ожидает запрос на установление TCP-соединения по протоколу POP3 через порт 110, а по протоколу IMAP – через порт 143.

Различия между протоколами POP3 и IMAP состоит в том, что получая доступ к почтовому серверу по протоколу POP3, происходит перемещение электронных сообщений в память компьютера, а при доступе по протоколу IMAP в память компьютера передаются только копии сообщений, хранящихся на почтовом сервере. При работе пользователя со своей почтой из разных сетевых устройств использование протокола POP3 вызовет ряд затруднений.

7.3 Сетевая файловая служба

Сетевая файловая служба предоставляет пользователям сети услуги по совместному использованию файлов, хранящихся на сетевых устройствах. Клиенты сетевой файловой службы установлены на компьютерах, подключенных к сети, и обслуживают запросы приложений на доступ к сетевым файлам. Каждый клиент передает по сети запросы серверу сетевой файловой службы, работающему на удаленном сетевом устройстве. Сервер, получив запрос, может обслужить его либо самостоятельно, либо передать запрос для обслуживания локальной файловой системе. После получения ответа от локальной файловой системы сервер передает его по сети клиенту, а тот – приложению, обратившемуся с запросом.

Приложения обращаются к клиенту сетевой файловой службы, используя программный интерфейс, который чаще всего похож на интерфейс локальной файловой службы, чтобы соблюсти принцип прозрачности.

Клиент и сервер взаимодействуют друг с другом через сеть по протоколу сетевой файловой системы. Если интерфейсы локальной и сетевой файловых систем совпадают, например, при использовании на сервере локальной файловой системы – **таблицы размещения файлов** (**File Allocation Table**, **FAT**), то функции протокола заключаются в ретрансляции серверу запросов, принятых клиентом от приложений, с которыми тот затем будет обращаться к локальной файловой системе.

Протокол для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия (**Server Message Block, SMB**) и его первая версия – **единая файловая система Интернета** (**Common Internet File System**, **CIFS**) являются основой сетевой файловой службы в операционных системах Microsoft Windows. Работа протокола начинается с того, что клиент отправляет серверу специальное сообщение с запросом на установление соединения. Если сервер готов к установлению соединения, он отвечает сообщением-подтверждением. После установления соединения клиент может обращаться к серверу, передавая ему в SMB-сообщениях команды манипулирования файлами и каталогами. В среде операционной системы Unix наибольшее распространение получили две сетевые файловые системы и соответственно два протокола

клиент-сервер – **протокол передачи файлов по сети** (**File Transfer Protocol**, **FTP**) и протокол сетевого доступа к файловым системам (**Network File System**, **NFS**).

Протокол FTP целиком перемещает файл с удаленного сетевого устройства на локальное и наоборот, поддерживает несколько команд просмотра удаленного каталога и перемещения по каталогам удаленной файловой системы. В данный протокол встроены примитивные средства аутентификации удаленных пользователей на основе передачи по сети пароля в открытом виде. Также поддерживается анонимный доступ, который не подвергает пароли угрозе перехвата.

FTP-клиент и FTP-сервер поддерживают параллельно два сеанса – управляющий сеанс и сеанс передачи данных. Управляющий сеанс открывается при установлении первоначального FTP-соединения клиента с сервером, причем в течение одного управляющего сеанса может последовательно проходить несколько сеансов передачи данных, в рамках которых передается или принимается несколько файлов.

Схема взаимодействия клиента и сервера состоит из следующих этапов:

1 FTP-сервер всегда открывает управляющий TCP-порт 21 для прослушивания, ожидая прихода запроса на установление управляющего FTP-сеанса от удаленного клиента.

2 После установления управляющего соединения клиент отправляет на сервер команды, которые уточняют параметры соединения.

3 После согласования параметров пассивный участник соединения переходит в режим ожидания открытия соединения на порт передачи данных. Активный участник инициирует открытие соединения и начинает передачу данных.

4 После окончания передачи данных соединение по портам данных закрывается, а управляющее соединение остается открытым. Пользователь может по управляющему соединению активизировать новый сеанс передачи данных.

7.4 Служба управления сетью

Система управления сетью (**Network Management System**, **NMS**) – это сложный программно-аппаратный комплекс, который контролирует сетевой трафик и управляет коммуникационным оборудованием крупной компьютерной сети. Системы управления сетью работают, как правило, в автоматизированном режиме, выполняя наиболее простые действия автоматически и оставляя человеку принятие сложных решений на основе подготовленной системой информации.

Система управления сетью предназначена для решения следующих основных групп задач:

– управление конфигурацией сети – конфигурация параметров как отдельных элементов сети, так и сети в целом;

– обработка ошибок – определение и устранение последствий сбоев и отказов;

– анализ производительности и надежности – оценка статистической информации о пропускной способности каналов и интенсивности трафика;

– управление безопасностью – контроль доступа к ресурсам сети и обеспечение целостности хранимых на них данных;

– учет работы сети – регистрация времени использования различных ресурсов сети.

Для решения данных задач необходимо управлять каждым отдельным устройством, требующим достаточно сложного конфигурирования. Индивидуальный программный продукт, который встраивается в управляемое оборудование для его конфигурирования, называют агентом. Из-за многообразия типов управляемых устройств невозможно стандартизовать способ взаимодействия агента с устройством, поэтому данная задача решается разработчиками индивидуально при встраивании агентов в оборудование. Агент может выполнять следующие функции:

– хранить, извлекать и передавать по запросам информацию о технических и конфигурационных параметрах устройства;

– выполнять измерения характеристик функционирования устройства, хранить и передавать их результаты по запросу;

– изменять по командам, полученным извне, конфигурационные параметры.

Агент играет роль сервера, к которому с запросами обращается клиент (администратор). Одним из протоколов, который может применяться в качестве протокола взаимодействия клиента и сервера, является **протокол удаленного управления telnet**, клиентская часть которого должна быть установлена на сетевом устройстве администратора, а серверная – на управляемом устройстве. Серверная часть telnet должна также поддерживать интерфейс с агентом, от которого будет поступать информация о состоянии управляемого объекта и значении его характеристик.

Протокол telnet обеспечивает эмуляцию алфавитно-цифрового терминала и ограничивает пользователя режимом командной строки. Для аутентификации пользователей в технологии telnet применяются пароли, передаваемые через сеть в открытом виде. Это ограничивает использование протокола telnet пределами одной локальной сети. Для удаленного управления узлами через Интернет вместо telnet обычно применяется **протокол безопасной оболочки** (**Secure Shell**, **SSH**), который, как и telnet передает набираемые на терминале пользователя символы на удаленный узел без интерпретации их содержания. В SSH предусмотрены меры по защите передаваемых аутентификационных и пользовательских данных.

В настоящее время основной областью применения протоколов telnet и SSH является управление не компьютерами, а такими коммуникационными устройствами, как маршрутизаторы, коммутаторы.

Простой протокол сетевого администрирования (**Simple Management Network Protocol**, **SNMP**) используется в качестве стандартного протокола взаимодействия менеджера и агента. SNMP – это протокол типа «запрос-ответ», который для транспортировки своих сообщений использует протокол UDP. SNMP-сообщение состоит из трех основных частей:

– версия протокола;

– общая строка, которая используется для группирования устройств, управляемых определенным менеджером;

– область данных, в которой содержатся команды протокола, имена объектов и их значения.

Отличие между протоколами telnet (SSH) и SNMP принципиально. Протоколы telnet и SSH предусматривают обязательное участие человека в процессе администрирования – они транслируют команды, которые вводит администратор при конфигурировании или мониторинге сетевого устройства. Протокол SNMP рассчитан на автоматические процедуры мониторинга и управления, хотя и не исключает возможности участия администратора в этом процессе. Для защиты информации применяется многоуровневая схема доступа, согласно которой пароль, передаваемый в открытом виде, дает возможность только чтения базовых характеристик конфигурации устройства, а доступ к средствам изменения конфигурации требует пароля, передаваемого в зашифрованном виде.

7.5 Защита сетевых соединений

Для защиты сетевых соединений используют защищенные каналы, которые можно построить с помощью системных средств, реализованных на разных уровнях модели OSI. На канальном уровне защищенные каналы могут формироваться **протоколом двухточечного туннелирования** (**Point-to-Point Tunneling Protocol**, **PPTP**), который защищает кадры протокола **двухточечного соединения** (**Point-to-Point Protocol**, **PPP**) канального уровня, упаковывая их в IP-пакеты.

На сетевом уровне за безопасную передачу данных отвечает рассмотренный ранее набор стандартов IPSec. Средства защищенного канала являются прозрачными для приложений в тех случаях, когда безопасность обеспечивается на сетевом и канальном уровнях.

Защищенный канал, реализованный на прикладном уровне, защищает только определенную сетевую службу, например, протокол S/MIME защищает сообщения электронной почты. При таком подходе для каждой службы необходимо разрабатывать собственную защищенную версию протоко-

ла. Работа протокола защищенного канала на уровне представления делает его более универсальным средством, чем протокол безопасности прикладного уровня.

На уровне представления работает **протокол безопасности транспортного уровня** (**Transport Layer Security**, **TLS**), заменивший **протокол защищенных сокетов** (**Secure Socket Layer**, **SSL**), который в настоящее время признан уязвимым и не рекомендуется для использования.

Протокол SSL был разработан для защиты данных, передаваемых между веб-сервером и веб-браузером, но также мог быть использован и любыми другими приложениями. Для установления защищенного канала протоколы SSL и TLS используют следующие технологии безопасности:

– взаимная аутентификация приложений на обоих концах защищенного канала выполняется путем обмена цифровыми подписями с использованием асимметричного шифрования;

– для контроля целостности передаваемых данных используются хэш-коды;

– секретность обеспечивается симметричным шифрованием с использованием сеансовых ключей.

7.6 Безопасность сетевых служб

В настоящее время веб-браузер с его графическим интерфейсом является основным средством доступа пользователя к большинству сервисов сети Интернет. Особенностью защиты веб-службы является то, что такая защита требует решения двух задач: обеспечение безопасности программных и аппаратных средств сетевого устройства, на котором эта служба выполняется, и обеспечение приватности того лица, которое этой службой пользуется. Рассмотрим первую из задач (вторая задача будет рассмотрена в следующем разделе).

Веб-браузер для взаимодействия с веб-сервером по умолчанию использует протокол HTTP без дополнительных мер по обеспечению основных свойств безопасных коммуникаций. Основным способом обеспечения безопасности передаваемых между браузером и сайтом данных является использование **безопасного протокола передачи гипертекста** (**Hypertext Transfer Protocol Secure**, **HTTPS**), который на самом деле подразумевает совместную работу протоколов HTTP и TSL. В HTTPS-соединении сам протокол HTTP, работающий поверх протокола TSL, остается неизменным. Защита информации обеспечивается протоколом TSL. В HTTPS-соединении по умолчанию используется порт 443.

При обращении браузера к веб-серверу по протоколу HTTPS каждая из сторон должна иметь выданную центром сертификации цифровую подпись, достоверность которой можно проверить по цепочке доверия, ведущей к

одному из доверенных корневых центров сертификации. Для браузеров такую встроенную цифровую подпись поставляет производитель с каждой копией браузера. Эта цифровая подпись не аутентифицирует пользователя, работающего с браузером, а служит только для создания защищенного канала при передаче данных между браузером и веб-сервером.

Аутентификация сервера при установлении HTTPS-соединения всегда выполняется на основе цифровой подписи сервера, получаемой владельцем сервера. Эта цифровая подпись подтверждает, что данный веб-сервер имеет определенные доменные имена.

Для защиты почтового сервиса необходимо аутентифицировать пользователей, которые пользуются данной службой. Для этого могут применяться средства провайдера услуг, который будет принимать по протоколу SMTP только те письма, которые отправляются клиентами этого провайдера, установленными по пулу IP-адресов. Также для этого может применяться расширение протокола SMTP – SMTP AUTH, которое описывает процедуру аутентификации пользователя при отправке сообщения агентом пользователя серверу провайдера почтовых услуг. В соответствии с этим расширением почтовый сервер и агент пользователя в начале SMTP-сеанса договариваются о методе аутентификации. Аутентификация пользователя может производиться на основе его личной цифровой подписи. Возможность включения цифровой подписи в качестве части сообщения описана в расширении S/MIME.

Аутентификация на основе цифровой подписи отправителя решает несколько задач:

– получатель может проверить аутентичность отправителя и целостность сообщения;

– отправитель не может отказаться от факта отправки письма;

– подпись квитанции о получении/чтении письма делает невозможным отказ получателя от факта получения письма.

Цифровая подпись в расширении S/MIME занимает две части сообщения:

– в первой части описывается используемый стандарт цифровой подписи (протокол) и примененная хеш-функция;

– во второй части, которая является приложением, находится сама цифровая подпись, охватывающая все части сообщения вместе с их заголовками.

Шифрование содержимого письма может происходить как «из конца в конец», так и отдельно между агентом пользователя и почтовым сервером, принимающим от него письма. Шифрование содержимого письма из конца в конец предусмотрено спецификацией S/MIME. Шифрование на отдельных участках чаще всего осуществляется средствами защищенного канала и организуется с помощью IPSec или TLS.

Для передачи шифрованного сообщения требуются две части: в первой части описывается способ шифрования, а во второй находится зашифрованная исходная часть сообщения.

Контрольные вопросы

1 Что такое сетевая служба?

2 Какие группы сетевых служб выделяют в зависимости от типа предоставляемых услуг?

3 Для каких целей используется веб-служба?

4 Что такое URL?

5 Для каких целей служит HTTP?

6 Для каких целей используется сетевая почтовая служба?

7 Для каких целей служит SMTP?

8 Опишите схему взаимодействия клиента и сервера при работе SMTP.

9 Для каких целей служит POP3?

10 Назовите основные отличия IMAP.

11 Для каких целей используется сетевая файловая служба?

12 Для каких целей служит FTP?

13 Опишите схему взаимодействия клиента и сервера при работе FTP.

14 Для каких целей используется служба управления сетью?

15 Для каких целей служит протокол telnet?

16 В чем основное отличие протоколов SSH и telnet?

17 Для каких целей используется SNMP?

18 Какие средства используются для защиты сетевых соединений?

19 Какие технологии безопасности используются протоколами TSL и SSL для установления защищенных каналов?

20 Какие протоколы используются для обеспечения безопасности сетевых служб?

8 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

8.1 Обзор инцидентов в сфере информационной безопасности

Инцидент информационной безопасности – это любое непредвиденное или нежелательное событие, которое может нарушить деятельность (функционирование) информационной системы или безопасность обрабатываемой ею информации.

Анализ инцидентов последних лет позволяет объективно оценивать тенденции киберугроз и методов, которые используют злоумышленники. В качестве источника инцидентов в сфере информационной безопасности выбраны данные, предоставляемые в ежегодных бюллетенях ЗАО «Лаборатория Касперского». Антивирусные программные продукты этой компании сертифицированы в Республике Беларусь и могут официально использоваться в подразделениях Белорусской железной дороги.

Общая статистика инцидентов в сфере информационной безопасности за последние четыре года представлена в таблице 8.1.

Таблица 8.1 – **Общая статистика инцидентов в сфере информационной безопасности**

Показатель статистики	Год			
	2018	2019	2020	2021
Доля компьютеров интернет-пользователей в мире, которые хотя бы один раз подверглись веб-атаке класса Malware, %	30,01	19,8	10,18	15,45
Количество атак с Интернет-ресурсов, отраженных решениями «Лаборатории Касперского»	1 876 998 691	975 491 360	666 809 967	687 861 449
Количество уникальных URL, на которых происходило срабатывание веб-антивируса «Лаборатории Касперского»	554 159 621	273 782 113	173 335 902	114 525 734

Окончание таблицы 8.1

Показатель статистики	Год			
	2018	2019	2020	2021
Количество уникальных вредоносных объектов, зафиксированных веб-антивирусом «Лаборатории Касперского»	21 643 946	24 610 126	33 412 568	64 559 357
Количество компьютеров, на которых отражены атаки шифровальщиков-вымогателей	765 538	755 485	549 301	336 256
Количество устройств, на которых отражены попытки запуска вредоносного программного обеспечения для кражи денежных средств через онлайн-доступ к банковским счетам	830 135	766 728	668 619	429 354
Количество пользователей, атакованных майнерами	5 638 828	2 259 038	1 523 148	1 184 986

Несмотря на то, что в 2020 году большинство значений показателей уменьшилось по сравнению с предыдущими годами, опасение должно вызывать увеличение количества уникальных вредоносных объектов зафиксированных веб-антивирусом «Лаборатории Касперского».

Рейтинг наиболее уязвимых приложений, представленный на рисунке 8.1, основывается на статистике «Лаборатории Касперского» по заблокированным уязвимостям, используемым киберпреступниками.

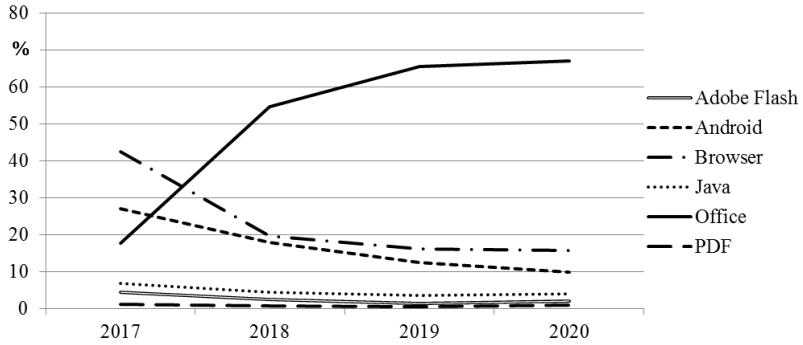

Рисунок 8.1 – Распределение уязвимостей, использованных в атаках злоумышленников, по типам атакуемых приложений

Несмотря на то, что с 2021 года продукт Adobe Flash перестал поддерживаться, интерес злоумышленников к нему не ослабевает. Незначительную долю уязвимостей сохраняют также Java-платформы и PDF. Веб-браузеры и Android в последние годы несколько снизили свои показатели, но все равно остаются одним из основных способов заражения незащищенных компьютеров. Лидирующее место по доле уязвимостей занимают приложения Microsoft Office и доля эта увеличивается из года в год. Основная причина заключается в популярности данных приложений при ведении документации, расчетов и отчетности. Также документы этих приложений чаще всего пересылаются по электронной почте и пользователи готовы их принимать и просматривать без дополнительного анализа.

В последние годы Республика Беларусь в соответствии со статистикой ЗАО «Лаборатория Касперского» входила в число стран, в которых пользователи подвергались наибольшему риску заражения через сеть Интернет (таблица 8.2).

Таблица 8.2 – **Положение Республики Беларусь среди стран, пользователи которых подвергались наибольшему риску заражения через сеть Интернет**

Показатель статистики	Год				
	2017	2018	2019	2020	2021
Доля уникальных пользователей, подвергшихся веб-атакам вредоносных объектов класса Malware, от всех уникальных пользователей продуктов «Лаборатории Касперского» в Республике Беларусь, %	38,39	43,00	24,52	12,54	27,98
Положение Республики Беларусь среди стран, пользователи которых подвергались наибольшему риску заражения через сеть Интернет	2	2	9	19	1
Страна-лидер и доля уникальных пользователей, подвергшихся веб-атакам вредоносных объектов класса Malware, в этой стране, %	Алжир (44,06)	Алжир (43,31)	Алжир (33,02)	Тунис (18,27)	Республика Беларусь (27,98)

Представленные данные агрессивности среды, в которой работают сетевые устройства пользователей, позволяют оценить степень риска заражения вредоносными программами через сеть Интернет, которому подвергаются сетевые устройства пользователей в Республике Беларусь.

«Лидирующее» положение Республики Беларусь в списках сран, в которых пользователи подвергались наибольшему риску заражения через сеть

Интернет за последние годы, вызывает серьезное опасение и однозначно указывает на необходимость использования средств защиты информации.

Помимо риска заражения вредоносным программным обеспечением при удаленном доступе к сети Интернет корпоративные пользователи компьютерных систем и сетей железнодорожного транспорта подвергаются опасности локального заражения, например, при использовании зараженных носителей информации. Чтобы оценить степень риска заражения сетевого устройства на территории Республике Беларусь, необходимо сравнить долю устройств, на которых в течении года хотя бы раз произошло срабатывание файлового антивируса «Лаборатории Касперского». При этом учитывались детектируемые объекты, найденные непосредственно на сетевых устройствах пользователей или же на подключенных к ним съемных носителях.

За последние четыре года Республика Беларусь единожды попала в ТОП-20 стран (17-я позиция в 2018 году), в которых пользователи подвергались наибольшему риску локального заражения. Доля устройств, на которых в течении года хотя бы раз произошло срабатывание файлового антивируса «Лаборатории Касперского», составила 52,38 % (лидером в этом году был Вьетнам с долей 62,29 %). На рисунке 8.2 представлена география локальных заражений вредоносным программным обеспечением в 2020 году, взятая из бюллетеня ЗАО «Лаборатория Касперского».

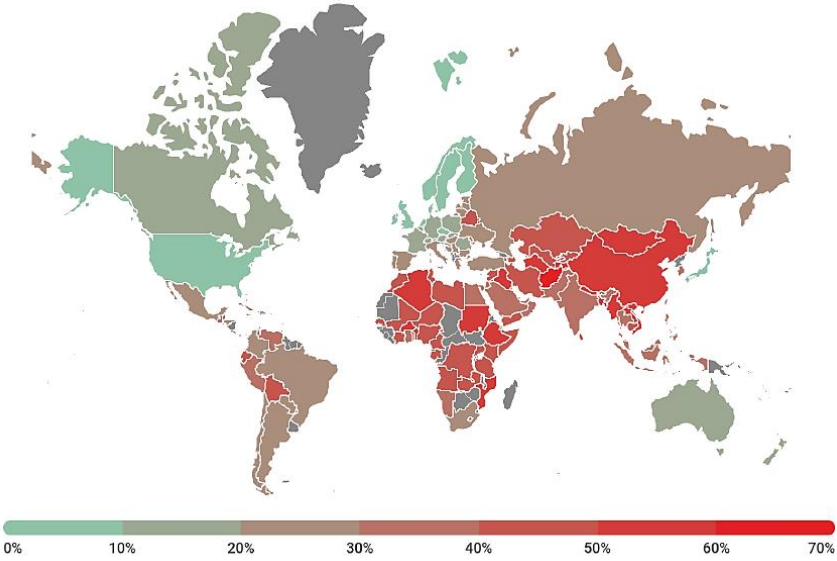

Рисунок 8.2 – География локальных заражений вредоносным программным обеспечением в 2020 году

Представленные данные также указывают на необходимость защиты информации – практически каждое второе сетевое устройство на территории Республики Беларусь, на котором установлен антивирус «Лаборатории Касперского», хотя бы раз в 2020 году подвергался атаке. Также следует обратить внимание на то, что в статистике участвуют только обнаруженные антивирусом атаки.

Наиболее опасными для компьютерных систем и сетей железнодорожного транспорта в настоящее время являются программы-шифровальщики и программы-майнеры.

Также актуальными как для работников железнодорожного транспорта, так и других отраслей являются атаки с использованием банковского вредоносного программного обеспечения.

Количество пользователей антивирусных приложений «Лаборатории Касперского» в мире, атакованных вредоносными шифровальщиками-вымогателями в период с ноября 2016 года по октябрь 2020 года, представлено на рисунке 8.3.

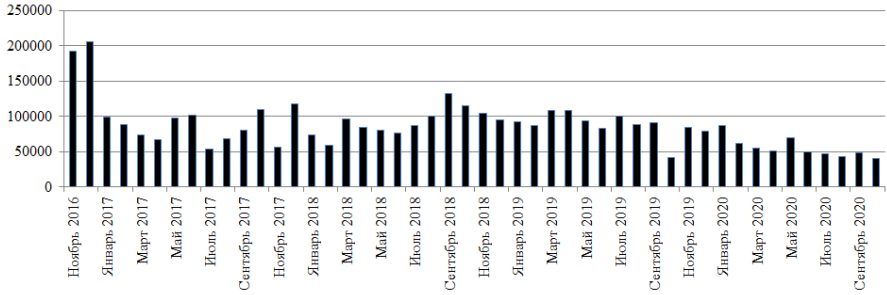

Рисунок 8.3 – Количество пользователей, атакованных вредоносными шифровальщиками-вымогателями

С 2019 года наметился спад количества пользователей, атакованных шифровальщиками-вымогателями, однако их все еще достаточно много. При этом только за один ноябрь 2019 года появилось 8660 модификаций вредоносного программного обеспечения такого рода. Основным способом распространения подобного вредоносного программного обеспечения являются вложения в электронные письма и сообщения в мессенджерах. Важно обращать внимание на файлы, прикрепляемые к электронным сообщениям и на достоверность их источников.

Заражение сетевого устройства программой, которая занимается майнингом криптовалюты, не является большой проблемой, по сравнению с шифрованием файлов, однако может вызывать затруднения с работой на этом устройстве, его «зависание» и перегрев. Республика Беларусь является

одной из стран мира, на территории которой атаки такого рода являются весьма распространенными.

Для каждого активного пользователя сети Интернет одними из самых опасных угроз в сфере информационной безопасности являются угрозы в финансовом секторе, которые блокируют или перехватывают транзакции, а также могут опустошать средства, хранимые на карт-счетах пользователей.

Количество пользователей во всем мире, атакованных вредоносными программами для кражи денежных средств с банковских счетов в период с ноября 2016 года по октябрь 2020 года, представлено на рисунке 8.4.

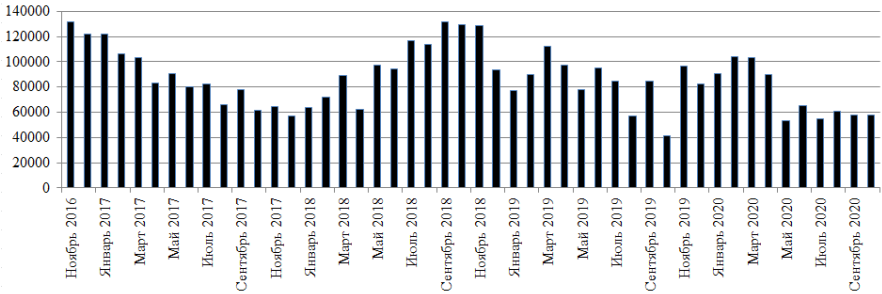

Рисунок 8.4 – Количество пользователей, атакованных вредоносными программами для кражи денежных средств с банковских счетов

Вся приведенная выше статистика указывает на крайнюю необходимость в использовании эффективных методов и средств защиты информации в компьютерных системах и сетях железнодорожного транспорта.

8.2 Системы автоматизированного сбора и учета фактов нарушения информационной безопасности объектов информатизации

Мониторинг сетевого трафика – это непрерывный процесс инструментального автоматизированного наблюдения за отдельными параметрами трафика в сети для проверки соблюдения соглашений об уровне обслуживания, предотвращения технических аварий, выявления реализации угроз и атак злоумышленников.

Существуют следующие средства мониторинга сетевого трафика:

– **анализаторы протоколов** или **сетевые сниферы**, которые позволяют захватывать трафик локальных сетей и представлять его в удобном для анализа виде;

– маршрутизаторы, поддерживающие **протокол NetFlow**, которые собирают обобщенные данные о трафике глобальных сетей, передавая его для анализа программным системам NetFlow;

– **системы обнаружения вторжений** (**Intrusion Detection Systems**, **IDS**), которые специализируются на автоматическом распознавании вторжений и угроз в прослушиваемом трафике локальных сетей.

Анализатор протоколов представляет собой самостоятельное специализированное устройство либо программное обеспечение сетевого устройства. В состав анализаторов может входить экспертная система, способная выдавать пользователю рекомендации о том, как проводить анализ трафика в конкретной ситуации, как устранить некоторые виды неисправностей в сети и т. п.

Система мониторинга NetFlow (поток данных, передающихся по сети) является в настоящее время основным средством учета и анализа трафика, проходящего через маршрутизаторы и коммутаторы сети. Большинство производителей сетевого оборудования поддерживают протокол NetFlow, благодаря чему сетевые узлы собирают статистику о проходящих через них потоках данных и периодически отправляют собранную информацию в коллекторы для хранения и обработки.

NetFlow собирает статистику не об отдельных пакетах, а о потоках пакетов, определяя поток как последовательность пакетов, объединенных набором общих признаков, в число которых чаще всего входят: IP-адреса источника и приемника, порты TCP/UDP источника и приемника, тип протокола, переносимого IP-пакетом и т. п. Кроме того, NetFlow собирает разнообразную статистику о потоке: время его начала и окончания, объем переданных данных, средняя скорость передачи данных. При этом Net Flow собирает только метаданные о трафике, не заглядывая в поля данных пакетов.

Данные NetFlow служат для поиска аномалий в характере метаданных, которые проявляются в отличиях от базового уровня характеристик сети. Система мониторинга трафика на базе NetFlow включает следующие функциональные компоненты:

– экспортер потока (сенсор) – маршрутизатор, который агрегирует пакеты в потоки и передает статистические данные об этих потоках в один или несколько коллекторов;

– коллектор – сервер, который отвечает за прием, хранение и предварительную обработку данных о потоках, полученных от экспортера потока;

– программа-анализатор – анализирует полученные данные о потоках с целью распознавания возможных атак или возникновения перегрузок сети, установления состава и тенденций изменения трафика в сети.

Система обнаружения вторжений – это программное или аппаратное средство, которое выполняет непрерывное наблюдение за сетевым трафиком и деятельностью субъектов системы с целью предупреждения, выявления и протоколирования атак. Они учитывают в своей работе различные

подозрительные события, происходящие в системе. Система обнаружения вторжений использует агентов, встроенных во многие точки сети. С их помощью она следит за трафиком сети и всеми обращениями к критически важным ресурсам отдельных сетевых устройств. При этом она не блокирует подозрительный трафик, а только предупреждает администратора сети о его наличии и протоколирует подозрительные пакеты.

Система IDS включает следующие функциональные элементы:

– источники данных – маршрутизаторы, коммутаторы и прочие сетевые устройства локальной сети, которые передают, генерируют и принимают трафик;

– датчики – отдельные сетевые устройства или программные компоненты маршрутизаторов, которые копируют пакеты, циркулирующие в сети, фильтруют и передают анализатору для выявления подозрительной активности;

– анализатор – ядро IDS, которое получает данные от датчиков и, в соответствии с правилами, составленными администратором, проверяет их на наличие угроз и подозрительной активности в сети, а затем информирует сигналом тревоги менеджера системы IDS;

– администратор – ответственное лицо, которое конфигурирует IDS и составляет правила ее работы в соответствии с политикой безопасности организации;

– менеджер – программный компонент, который хранит конфигурацию IDS и поддерживает удобный интерфейс с оператором IDS, с помощью которого оповещает оператора IDS о тревоге в виде звукового или светового уведомления;

– оператор – ответственное лицо, которое в результате поступления сигнала тревоги от менеджера принимает решение о реакции сети на подозрительную активность.

В минимальном варианте все функции IDS могут быть сосредоточены в программном обеспечении единственного сетевого устройства, сетевой адаптер которого исполняет роль датчика за счет того, что присоединен к зеркализованному порту коммутатора или маршрутизатора. Более масштабируемой является реализация IDS с несколькими датчиками в виде дополнительного программного обеспечения маршрутизатора или коммутатора, подключенными к различным сегментам сети и посылающими захваченный трафик центральному анализатору.

Помимо IDS существуют **системы предупреждения вторжений (Intrusion Prevention Systems, IPS)**, которые выполняют автоматические действия по прекращению атаки в случае ее обнаружения.

8.3 Методы и средства защиты информации от удаленных атак

Для защиты от удаленных атак локальные сети организации защищаются с помощью методов фильтрации трафика, использования межсетевых экранов, а также с помощью систем IDS и IPS, которые были рассмотрены выше.

Под **фильтрацией трафика** понимается обработка IP-пакетов маршрутизаторами, при которой часть пакетов отбрасывается или изменяет свои маршруты. Фильтрация трафика позволяет предотвратить атаку на сеть, блокируя доступ к ней для заранее известных внешних сетей или отдельных сетевых устройств. Если источник атаки заранее неизвестен, то фильтрация трафика позволяет оперативно остановить атаку.

Стандартные правила фильтрации определяются особенностями функционирования сетевых устройств. Например, коммутатор передает кадр только на тот интерфейс, к которому подключена подсеть, имеющая в своем составе узел с адресом назначения кадра. Аналогично поступает и маршрутизатор с пакетами. Если коммутатор не обладает информацией об адресе назначения кадра, то он передает его на все интерфейсы кроме того, из которого он поступил. В аналогичной ситуации с пакетами маршрутизатор отбрасывает пакет.

Дополнительные правила фильтрации или пользовательские фильтры задаются сетевыми администраторами исходя из политики безопасности либо с целью изменения стандартных маршрутов. Дополнительные правила фильтрации маршрутизаторов могут учитывать IP- и MAC-адреса источника и приемника, типы протоколов, сообщения которых несут IP-пакеты, номера портов TCP/UDP. С использованием стандартных и дополнительных правил фильтрации организуется технология разграничения доступа по спискам контроля доступа (ACL), рассмотренная ранее.

Межсетевой экран (файервол, брандмауэр) – это комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части компьютерной сети от другой путем анализа и фильтрации проходящего между ними трафика. При этом они осуществляют экранирование защищаемого объекта и формируют его внешнее представление. Для эффективного выполнения межсетевым экраном его функций необходимо, чтобы через него проходил весь трафик, которым обмениваются защищаемая сеть с внешними сетями.

Основными функциями межсетевого экрана являются фильтрация трафика в целях защиты внутренних ресурсов сети и аудит, который заключается в обнаружении и блокировке подозрительных пакетов. Помимо этого, на межсетевой экран могут быть возложены и другие вспомогательные функции защиты, например, антивирусная защита, шифрование трафика и пр.

На рисунке 8.5 представлена классификация межсетевых экранов исходя

из уровней модели OSI, которым соответствуют протокольные единицы данных (PDU), используемые межсетевым экраном для своего функционирования.

Управляемые коммутаторы обладают возможностью фильтрации кадров канального уровня на основе задаваемых администратором списков доступа.

Пакетные фильтры решают задачу фильтрации пакетов по IP-адресам источника и приемника, а также по значению поля протокола верхнего уровня. Кроме того, работают и на транспортном уровне на основе статических правил, с помощью которых можно запретить прохождение пакетов с определенными номерами портов TCP или UDP. Этому типу межсетевых экранов соответствуют маршрутизаторы, поддерживающие пользовательские фильтры, а также программные межсетевые экраны операционных систем.

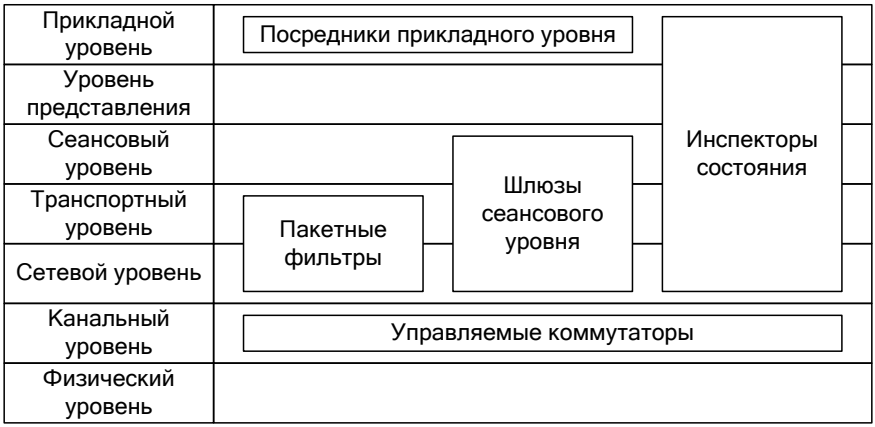

Рисунок 8.5 – Классификация межсетевых экранов по уровням модели OSI

Шлюзы сеансового уровня являются межсетевыми экранами с запоминанием состояний соединений на уровнях ниже прикладного – принимают решение о наличии угрозы динамически, с учетом текущего состояния сеанса и его предыстории. Такие межсетевые экраны используются для защиты и от атак, для распознавания которых требуется анализ не отдельных пакетов, а их последовательности. Например, они эффективно противодействуют тем видам атак на протокол TCP, в которых нарушается стандартная процедура установления соединения.

Посредники прикладного уровня – это приложения-посредники, каждое из которых обслуживает свой прикладной протокол. Для каждого протокола прикладного уровня специализированный посредник может

определять тип передаваемых данных и их содержимое, выполнять аутентификацию пользователя и проверять их электронную цифровую подпись. Недостатками данного типа межсетевых экранов являются большие затраты времени и ресурсов на анализ каждого пакета, в результате чего они не подходят для приложений реального времени.

Инспекторы состояния способны интерпретировать, анализировать и контролировать содержимое сообщений, которыми обмениваются приложения. Они также работают на основе фильтрации с запоминанием состояния, но анализируют состояния не только протоколов нижних уровней, но и прикладного уровня, например, SSH, HTTP, SMTP и пр.

Для защиты корпоративной сети может также использоваться **прокси-сервер** – особый тип приложения, которое выполняет функции посредника между клиентскими и серверными частями распределенных сетевых приложений. Клиенты этого приложения принадлежат защищаемой сети, а серверы – потенциально опасной сети. Находясь между защищаемой и потенциально опасной сетью, прокси-сервер логически разрывает прямое соединение между клиентом и сервером с целью контроля процесса обмена сообщениями между ними, при условии, что весь контролируемый трафик проходит через него.

Когда клиенту необходимо получить ресурс от какого-либо сервера, он посылает свой запрос соответствующему прокси-серверу, который его анализирует и на основании заданных ему администратором правил решает, каким образом он должен быть обработан. Помимо основных функций, прокси-серверы могут выполнять другие операции, например, обнаруживать вирусы еще до того, как они попали во внутреннюю сеть.

8.4 Защита сетевых устройств при работе в сети Интернет

Под приватностью физического лица подразумевается требование неприкосновенности информации о частной жизни этого лица без его согласия. В статье 18 Закона Республики Беларусь «Об информации, информатизации и защите информации» сказано, что никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь.

Популярность Интернета негативно повлияла на приватность физических лиц, которые им пользуются. Все действия пользователя в Интернете потенциально могут быть зафиксированы и проанализированы. Веб-серверы и браузеры ведут журналы посещений сайтов и страниц, запоминают IP-

адреса. Угроза приватности исходит также от cookies (текстовые данные, которыми обмениваются веб-сервер и браузер), которые содержат информацию о состоянии сеансов связи, аутентификаторы, персональные настройки и данные, номера карт и т. п.

Согласно рекомендациям, приведенным в юбилейном издании учебника «Компьютерные сети» Виктора и Натальи Олифер, пользователи, обменивающиеся сообщениями электронной почты через сеть Интернет, должны принимать во внимание наличие следующих угроз:

– спуфинг (подмена) имени отправителя – случай, когда злоумышленник выдает себя за другого пользователя;

– спуфинг почтовых серверов – сервер предъявляет при передаче сообщения ложное имя домена;

– модификация (изменение содержимого) сообщения – искажение или отбрасывание сообщения (нарушение целостности сообщений сервиса, что может стать причиной нарушения доступности сервиса);

– утечка информации – потенциальное ознакомление злоумышленника с содержимым информации (нарушение конфиденциальности);

– нарушение последовательности сообщений;

– нарушение свойства неотказуемости – отказ отправителя от факта отправки сообщения, отказ почтового сервера или получателя от факта приема сообщения;

– спам – засорение почтовых ящиков пользователей сообщениями, которые пользователи не просили или же не ожидали получить (обычно спам состоит из рекламных сообщений);

– нарушение приватности пользователя за счет сбора метаданных почтового сервиса;

– фишинг – электронное письмо обычно является первым этапом фишинга (целью фишинговой атаки является завладение учетными данными пользователя).

Реализация всех этих угроз доступна злоумышленнику из-за того, что изначально почтовая служба Интернета, основанная на протоколе SMTP, не поддерживала никаких механизмов защиты почтового обмена. В SMTP-пакетах текст сообщения передавался в открытом виде, аутентификация отправителя не была предусмотрена, проверить подлинность автора сообщения не представлялось возможным.

Достаточно часто электронная почта Интернета используется в своем первозданном виде, что ставит в уязвимое положение передаваемые с ее помощью данные, а также, например, из-за фишинга, информацию, хранимую в памяти сетевых устройств, использующих такую почтовую службу.

Опасность также представляют социальные сети, которые в настоящее время являются популярной платформой для общения, размещения или обмена информацией, развития бизнеса.

При работе в социальных сетях необходимо следовать нескольким простым правилам, которые позволят сохранить свою персональную информацию:

1 Важно представлять кем является субъект, который просит добавить себя в «друзья» в социальной сети. Став «другом», злоумышленнику будет гораздо проще реализовать свою атаку.

2 Рекомендуется для регистрации в социальных сетях завести и указывать отдельную электронную почту, не связанную с работой.

3 Следует избегать посещения социальных сетей с сетевых устройств организации, если это не входит в обязанности сотрудника.

4 Необходимо удалять ненужные аккаунты социальных сетей. Оставив аккаунт без внимания на длительный срок, можно упустить момент, когда он будет взломан злоумышленником и станет использоваться им в приступных целях.

5 Следует использовать сложные пароли для аутентификации, которые должны содержать символы нескольких алфавитов, цифры и служебные знаки. Рекомендуется периодически менять пароли на новые, логически не связанные со старыми паролями. Не рекомендуется для нескольких аккаунтов использовать одинаковые пароли, а также позволять браузерам автоматически их запоминать.

6 Рекомендуется использовать двухфакторную аутентификацию, которая привязывает аккаунт пользователя к его личному физическому устройству, например, смартфону или айфону. При этом для получения доступа к аккаунту социальной сети с неизвестного устройства потребуется ввести код, который будет доставлен на это устройство.

7 Следует минимизировать количество конфиденциальной информации, размещаемой в социальных сетях. Нельзя размещать фотографии каких-либо конфиденциальных документов или пересылать их с помощью социальных сетей.

8 Ну в коем случае не следует использовать социальные сети в качестве основного хранилища персональной информации и фотографий. Социальная сеть – это ресурс, который не принадлежит пользователю, и может не обеспечивать резервное хранение данных.

Основную опасность для пользователя корпоративной сети представляют вредоносные программы, которые тем или иным способом могут попасть на его сетевое устройство. **Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. Пользователь может принести ее на своем носителе, получить в качестве вложения в электронном письме или сообщении в каком-либо мессенджере. К вредоносным относятся такие программы, как троянские программы, сетевые черви, вирусы, программы-закладки, программы-боты и т. п.

Троянская программа – это вредоносная программа, которая может нанести ущерб операционной системе и информации пользователя, маскируясь под какое-либо полезное или знакомое пользователю приложение. Такая программа может уничтожать или искажать информацию на жестком диске, передавать данные на удаленный сервер, нарушать функционирование установленного программного обеспечения, участвовать в проведении DDoS-атак.

Сетевой червь – это вредоносная программа, способная к самостоятельному распространению своих копий в пределах локальной сети, а также по глобальным связям, перемещаясь от одного сетевого устройства к другому без всякого участия в этом процессе пользователей сети. Главная цель и результат деятельности червя – это распространение своих копий на максимально возможное число сетевых устройств – новых потенциальных жертв. Червь может рассылать свои копии по сети в виде вложений в сообщения электронной почты или путем размещения ссылок на зараженный файл на каком-либо веб-сайте. Он не удаляет и не искажает файлы, не перехватывает и не модифицирует электронные сообщения, а наносит вред за счет потребления ресурсов своих жертв для рассылки спама, троянских или других вредоносных программ.

Вирус – это вредоносный программный код, который может внедряться в другие файлы разных типов, включая файлы исполняемых программ. В отличие от червей вирусы не содержат в себе встроенного механизма активного распространения по сети и способны размножаться своими силами только в пределах одного компьютера.

Программная закладка – это встроенный в программное обеспечение объект, который при определенных условиях инициирует выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию. Функции, описание которых отсутствует в документации к программному обеспечению, называют **недекларированными возможностями.** Программные закладки могут шпионить за действиями пользователя и передавать эту информацию на определенный сервер, получать доступ к конфиденциальной информации, искажать и разрушать данные.

Бот – программа, которая выполняет некоторые действия по командам, поступающим от удаленного источника (центра управления). Бот находится в следящем режиме, анализируя сообщения и ожидая команды из центра управления или возникновения заранее определенной ситуации. На сетевое устройство пользователя боты проникают нелегально и скрытно. Зараженному сетевому устройству, которое называется зомби, бот не причиняет

вреда – его цели находятся где-то в Интернете. Группа согласованно работающих ботов называется **ботнетом** или сетью ботов. Для управления ботами центр управления использует различные протоколы, например, **протокол передачи мгновенных сообщений** (**Internet Relay Chat**, **IRC**).

Для защиты сетевых устройств от вредоносного программного обеспечения необходимо использовать антивирусные программы. На частных сетевых устройствах – индивидуальные пакеты антивирусной защиты, а на предприятиях – корпоративные пакеты, состоящие из клиентской программы и сервера, рассылающего обновления.

Антивирусные программы используют различные методы для обнаружения сигнатуры вирусов – характерных последовательностей программных кодов, которые их с какой-то степенью вероятности идентифицируют. Чтобы обнаружить вирус, антивирусная программа должна иметь библиотеку сигнатур, которая должна быть актуальной и периодически обновляться.

Метод сигнатур является основным методом обнаружения вирусов, но обладает принципиальным недостатком – неспособностью обнаружить новый тип вируса или вируса с замаскированной сигнатурой. Антивирусные программы используют также эвристические методы, которые пытаются выявить вирус на основе структуры его кода или его поведения, не имея точной сигнатуры кода, но используя некоторые обобщенные признаки подозрительной структуры кода или подозрительного поведения.

В настоящее время в корпоративных сетях все чаще используются облачные сервисы. Если сервисы реализованы внутри организации, то это не несет существенного вреда. В том случае, когда используются услуги облачного провайдера, персональные данные пользователей хранятся в справочной службе провайдера. При этом с помощью механизмов виртуализации происходит разделение инфраструктуры защищаемой сети с другими арендаторами, что позволяет злоумышленнику попытаться получить несанкционированный доступ к конфиденциальной информации. Кроме того, нельзя исключать ошибки персонала провайдера, в результате которых виртуальные барьеры между арендаторами могут быть нарушены.

Несмотря на то, что облачные сервисы принято рассматривать как источник новых угроз безопасности, они могут существенно улучшить информационную безопасность организации. С помощью облачных сервисов можно организовать резервирование информации, защиту от DDoS-атак и т. п.

Контрольные вопросы

1 Что такое инцидент информационной безопасности?

2 Какие параметры могут использоваться для оценки общей статистики инцидентов в сфере информационной безопасности?

3 Какие приложения или файлы созданные с помощью каких приложений чаще всего за последние годы использовались злоумышленниками для организации атак против информационной безопасности?

4 Оцените положение Республики Беларусь среди прочих стран, пользователи которых подвергались наибольшему риску заражения через сеть Интернет, за последние годы.

5 Проанализируйте географию локальных заражений вредоносным программным обеспечением в 2020 году.

6 Что такое шифровальщики-вымогатели?

7 Проанализируйте количество пользователей, атакованных вредоносными программами для кражи денежных средств с банковских счетов за последнее время.

8 Что такое программы-майнеры?

9 Что такое мониторинг сетевого трафика?

10 Какие средства используются для мониторинга сетевого трафика?

11 Какие функции выполняет система обнаружения вторжений?

12 Для чего используется фильтрация трафика?

13 Что такое файервол?

14 Какие функции выполняет межсетевой экран?

15 Приведите классификацию межсетевых экранов по уровням модели OSI.

Дайте понятие прокси-серверу.

16 Какие угрозы наиболее опасны для пользователей при работе в сети Интернет?

17 Дайте понятие вредоносному программному обеспечению.

18 Для каких целей используются троянские программы?

19 Что такое программная закладка?

20 Что такое ботнет?

21 Какие методы используются антивирусными приложениями для обнаружения сигнатур вирусов?

9 КОМПЛЕКСНЫЙ ПОДХОД ПРИ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

9.1 Комплексный подход при обеспечении защиты информации

Комплексная система защиты информации создается для защиты от наиболее вероятных угроз и охватывает следующие вопросы:

– разработка правового обеспечения защиты информации;

– определение потенциальных угроз безопасности информации;

– составление перечня данных, подлежащих защите;

– создание подразделения, ответственного за вопросы защиты информации;

– определение основных направлений обеспечения информационной безопасности.

Все методы защиты информации по характеру проводимых действий можно разделить:

– на законодательные (правовые);

– организационные;

– технические;

– комплексные, включающие элементы всех предыдущих.

В силу многообразия угроз для защиты компьютерной системы или сети необходимо использовать обширный арсенал технических средств защиты, однако именно организационные методы являются стержнем комплексной системы защиты информации в компьютерных системах и сетях. Только с помощью этих методов возможно объединение на правовой основе всех технических средств защиты информации в единую комплексную систему.

Комплексные системы защиты информации всегда должны иметь централизованное управление. Централизация управления защитой информации объясняется необходимостью проведения единой политики в области безопасности информационных ресурсов в рамках организации. Для осуществления централизованного управления в системе защиты информации должны быть предусмотрены специальные средства дистанционного контроля, распределения ключей, разграничения доступа и пр.

Комплексная система защиты информации должна быть дружественной по отношению к пользователям и обслуживающему персоналу. Она должна быть максимально автоматизирована и не должна требовать от пользователя

выполнять значительный объем действий, связанных с защитой информации. Вместе с тем комплексная система защиты информации не должна создавать ограничений в выполнении пользователем своих функциональных обязанностей.

В Республике Беларусь была выделена особая категория информационных систем – **критически важные объекты информатизации (КВОИ).**

В соответствии с Указом Президента Республики от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации» КВОИ – объект информатизации, который на основании критериев отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации. В этом же указе утверждено положение о порядке отнесения объектов информатизации к КВОИ и представлен перечень соответствующих критериев.

9.2 Методы оценки эффективности комплексных средств защиты информации

Оценка эффективности функционирования комплексной системы защиты информации представляет собой сложную задачу. В процессе разработки такой системы используется метод синтеза путем согласованного объединения блоков, устройств, подсистем с последующим анализом эффективности полученного решения. Анализ осуществляется с помощью моделирования, по результатам которого из множества синтезированных систем выбирается лучшая. Реализация модели позволяет получать и исследовать характеристики реальной системы.

Для оценки систем используются аналитические и имитационные модели. В аналитических моделях функционирование исследуемой системы записывается в виде математических или логических соотношений. При имитационном моделировании система представляется в виде некоторого аналога реальной системы. Также модели делятся на детерминированные (взаимодействуют с закономерными факторами) и стохастические (взаимодействуют со случайными факторами). В связи с тем, что на процессы защиты информации основное влияние оказывают случайные факторы, то модели систем защиты являются стохастическими.

Эффективность систем оценивается с помощью показателей эффективности, которые характеризуют степень соответствия оцениваемой системы своему назначению. В оценке эффективности комплексной системы защиты информации, в зависимости от используемых показателей эффективности и способов их получения, выделяют классический, официальный и экспериментальный подходы.

Под **классическим подходом** к оценке эффективности понимается использование критериев эффективности, полученных с помощью показателей эффективности. Значения показателей эффективности получаются путем моделирования или вычисляются по характеристикам реальной системы. Высокая степень неопределенности исходных параметров, сложность формализации процессов функционирования, отсутствие общепризнанных методик расчета показателей эффективности и выбора критериев оптимальности создают значительные трудности для применения таких методов оценки эффективности.

Официальный подход к определению эффективности комплексных систем защиты информации опирается на нормативные акты, в которых определены требования по защите информации. Требования могут задаваться перечнем механизмов защиты информации, которые необходимо иметь или реализовать в компьютерной системе, чтобы она соответствовала определенному классу защиты. Критерием эффективности комплексной системы защиты информации при официальном подходе является ее класс защищенности. Достоинством этого подхода является простота его использования, недостатком – констатация факт наличия или отсутствия конкретного механизма защиты, а не качество его использования.

В настоящее время в Республике Беларусь официальный подход к оценке эффективности системы защиты информации регламентируется приказом Оперативно-аналитического центра при Президенте Республики Беларусь № 66 от 20 февраля 2020 года «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449», в котором описаны классы типовых информационных систем, приведен перечень требований к системе защиты информации, подлежащих включению в техническое задание, а также представлены требования к организации взаимодействия информационных систем. Сами классы устанавливаются стандартом СТБ 34.101.30-2017 «Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация».

Под **экспериментальным подходом** понимается организация процесса определения эффективности существующих комплексных систем защиты информации путем попыток преодоления защитных механизмов системы специалистами, выступающими в роли злоумышленников. Такой подход к оценке эффективности позволяет получать объективные данные о возможностях существующих систем защиты, но требует высокой квалификации исполнителей и больших материальных и временных затрат.

9.3 Политика безопасности информационных систем

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая политика безопасности

информационной системы. Согласно государственному стандарту Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения» **политика безопасности (информации в организации)** – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которым руководствуется организация в своей деятельности.

Разработка и реализация политики информационной безопасности организации осуществляется высшим руководством путем выработки четкой позиции в решении вопросов информационной безопасности. Политика информационной безопасности должна быть утверждена, издана и надлежащим образом доведена до сведения всех сотрудников организации.

Согласно СТБ ISO/IEC 27001-2016 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» высшее руководство должно установить политику информационной безопасности, которая:

– соответствует назначению организации;

– включает цели (задачи) в области информационной безопасности или служит основой для задания таких целей (задач);

– включает обязательство соответствовать действующим требованиям, связанным с информационной безопасностью;

– включает обязательство непрерывного улучшения системы менеджмента информационной безопасности.

Политика безопасности устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Она должна быть:

– оформлена как документированная информация;

– доведена до сведения сотрудников в организации;

– доступной в установленном порядке для заинтересованных сторон.

Фундаментом для создания системы защиты информации является документ, в котором формулируются принципы и основные положения политики предприятия в области информационной безопасности. Документацию политики безопасности разделяют на документацию верхнего, среднего и нижнего уровней. Документы верхнего уровня политики информационной безопасности отражают позицию организации к деятельности в области защиты информации, её стремление соответствовать государственным, международным требованиям и стандартам в этой области.

Согласно ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» на верхнем уровне политики информационной безопасности должны быть оформлены следующие документы: «Концепция обеспечения информационной безопасности», «Правила допустимого использования ресурсов информационной системы», «План обеспечения непрерывности бизнеса».

К среднему уровню относят документы, касающиеся отдельных аспектов информационной безопасности. Это требования на создание и эксплуатацию средств защиты информации, организацию информационных и бизнес-процессов организации по конкретному направлению защиты информации.

В политику информационной безопасности нижнего уровня входят регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности.

Как минимум, политика безопасности должна включать следующее:

– определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

– изложение целей и принципов информационной безопасности, сформулированных руководством;

– краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований;

– определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

– ссылки на документы, дополняющие политику информационной безопасности.

9.4 Концепция национальной безопасности Республики Беларусь

Действующая в настоящее время Концепция национальной безопасности Республики Беларусь утверждена Указом Президента Республики от 09.11.2010 № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» и дополнена Указами Президента Республики от 30.12.2011 № 621 и от 24.01.2014 № 49.

Концепция национальной безопасности Республики Беларусь закрепляет совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз. Являясь базисом для консолидации усилий личности, общества и государства в целях реализации национальных интересов, Концепция национальной безопасности Республики Беларусь призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения национальной безопасности, а также методологическую основу совершенствования актов законодательства в различных сферах национальной безопасности, разработки документов стратегического планирования. Данная концепция охватывает политическую, экономическую, научно-техническую, социальную, демографическую, информационную, военную и экологическую сферы жизнедеятельности личности, общества и государства.

В концепции указано, что информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств. Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Вместе с тем сохраняется отставание Республики Беларусь от ведущих стран мира по уровню информатизации. В условиях открытости информационного пространства страны и конкуренции со стороны иностранного информационного продукта недостаточными остаются качество и популярность белорусского национального контента.

Основными национальными интересами в информационной сфере, которые касаются вопросов информационной безопасности, являются:

– преобразование информационной индустрии в экспортно-ориентированный сектор экономики;

– обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

В информационной сфере внутренними источниками угроз национальной безопасности, которые касаются вопросов информационной безопасности, являются:

– зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;

– недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

– рост преступности с использованием информационно-коммуникационных технологий;

– несовершенство системы обеспечения безопасности критически важных объектов информатизации.

В информационной сфере внешними источниками угроз национальной безопасности, которые касаются вопросов информационной безопасности, являются:

– открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;

– нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

– попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

Согласно Концепции национальной безопасности Республики Беларусь

приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

9.5 Концепция информационной безопасности Республики Беларусь

Концепция информационной безопасности Республики Беларусь утверждена Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь».

Концепция представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности.

Концепция обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере.

Базируясь на Концепции национальной безопасности Республики Беларусь, Концепция информационной безопасности:

– исходит из понимания основных тенденций современного мира, опре-

деленных в ней основных национальных интересов в информационной сфере, потенциальных либо реально существующих угроз национальной безопасности;

– конкретизирует цели, задачи и принципы обеспечения национальной безопасности в информационной сфере, основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в данной сфере;

– предполагает реализацию этих целей, задач и принципов как неотъемлемую часть функционирования общей системы обеспечения национальной безопасности.

В данной концепции отмечено, что на нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах. В результате повышения насыщенности и динамики общественных отношений, мировых и региональных событий, роста всеобщего интеллектуального потенциала значительно увеличиваются информационные потребности людей. Формируемое в глобальном масштабе информационное общество представляет собой новый этап развития цивилизации с преобладанием знаний и информации, воздействием информационных технологий на все сферы человеческой деятельности. Кардинально повышается роль информационных технологий в реализации прав и свобод граждан. Индустрия телекоммуникации стала одной из наиболее динамичных и перспективных сфер мировой экономики. С процессами информатизации все больше связываются национальные экономические интересы и перспективы инвестиций.

Вместе с тем трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов.

В рамках обусловленности мер по обеспечению безопасности информационной инфраструктуры в Концепции информационной безопасности Республики Беларусь указывается, что цифровая трансформация экономики и инновации в области информационно-коммуникационных технологий наряду с мировым развитием и наращиванием технологических возможностей во взаимодействии людей, бизнеса, государственных институтов обуславливают необходимость принятия особых мер, обеспечивающих доверие и безопасность при создании и использовании в современном информационном обществе информационной инфраструктуры и данных в информационных системах.

Политическая и социально-экономическая сферы, общественная и военная безопасность становятся все более уязвимыми перед преднамеренными или случайными технологическими воздействиями, формирующимися в том числе в условиях недостаточных глобальных механизмов согласованного и действенного предупреждения и сдерживания киберинцидентов в сети Интернет.

Повсеместное функционирование объектов промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности. Кибератаки на информационную инфраструктуру рассматриваются в мире как одна из наиболее значимых угроз безопасности.

Во многих национальных вооруженных силах создаются и развиваются кибервойска, а проведение кибероперации предусматривается в доктринальных и стратегических документах. Одновременно рассматривается возможность реагирования на кибератаки как на вооруженную агрессию, что в условиях практической невозможности точной идентификации их источников (инициаторов) может привести к бездоказательной и произвольной трактовке обоснованности встречных военных действий.

Неуклонно растет количество киберпреступлений. Информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными.

Однако ни в глобальном, ни в региональных масштабах пока не удается эффективно воспрепятствовать разработкам и распространению средств, заведомо предназначенных для уничтожения, блокирования, модификации, похищения информации в сетях и ресурсах или нейтрализации мер по ее защите. Выработка правовых, процедурных, технических и организационных мер против кибервоздействий на информационные ресурсы отстает от формирования реальных и потенциальных угроз их осуществления.

Также в Концепции информационной безопасности Республики Беларусь указываются наиболее вероятные источники угроз для информационной инфраструктуры нашего государства:

– отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

– противоправная деятельность отдельных лиц и преступных групп;

– преднамеренные действия и ошибки персонала информационных систем, выражающиеся в нарушении установленных регламентов их эксплуатации и правил обработки информации;

– зависимость Республики Беларусь от других стран – производителей программных и аппаратных средств при создании и развитии информационной инфраструктуры.

Перед Республикой Беларусь стоит стратегическая цель развития системы обеспечения кибербезопасности, базирующейся на передовых международных подходах управления рисками и предназначенной для реализации долгосрочных мер по их сокращению до приемлемого уровня.

Национальная система обеспечения кибербезопасности должна реализовывать весь возможный комплекс правовых, организационных и технических мер по обеспечению безопасности национальной информационной инфраструктуры, в том числе информационных систем, обеспечивать конфиденциальность, доступность и целостность информации, а также легко трансформироваться и адаптироваться в изменяющейся обстановке за счет постоянного анализа на предмет соответствия актуальным рискам кибербезопасности.

В первую очередь необходимо обеспечить киберустойчивость национального сегмента сети Интернет, критически важных объектов информатизации и государственных информационных систем, эффективное противодействие киберпреступлениям.

Контрольные вопросы

1 Какие вопросы охватывает комплексная система защиты информации?

2 Что такое критически важный объект информатизации?

3 Какие подходы выделяют при оценке эффективности комплексной системы защиты информации?

4 В чем заключается сущность классического подхода к оценке эффективности комплексной системы защиты информации?

5 В чем заключается сущность официального подхода к оценке эффективности комплексной системы защиты информации?

6 Что такое политика безопасности?

7 Какие элементы должна включать в свой состав политика безопасности?

8 Что такое Концепция национальной безопасности Республики Беларусь?

9 Каковы основные национальные интересы в информационной сфере, которые касаются вопросов информационной безопасности, в соответствии с Концепцией национальной безопасности Республики Беларусь?

10 Что такое Концепция информационной безопасности Республики Беларусь?

11 Какие наиболее вероятные источники угроз для информационной инфраструктуры Республики Беларусь указываются в Концепции информационной безопасности Республики Беларусь?

СПИСОК ЛИТЕРАТУРЫ

1 **Анищенко, В. В.** Методы оценки эффективности защиты активов в объектах информационных технологий / В. В. Анищенко, А. М. Криштофик // Информатика. – 2004. – № 3. – С. 95–105.

2 **Белоусова, Е. С.** Политика безопасности информационных систем : учеб.-метод. пособие / Е. С. Белоусова, П. М. Буй. – Гомель : БелГУТ, 2016. – 38 с.

3 **Буй, П. М.** Криптографические методы защиты информации в управляющих системах на транспорте : учеб.-метод. пособие / П. М. Буй, В. О. Матусевич. – Гомель : БелГУТ, 2011. – 56 с.

4 **Буй, П. М.** Методика перекрестной оценки угроз и уязвимостей безопасности объектов информатизации железнодорожного транспорта / П. М. Буй, С. Г. Кульгавик // Вестник БелГУТа: Наука и транспорт. – 2017. – № 2 (35). – С. 40–43.

5 **Буй, П. М.** Оценка рисков кибербезопасности инфокоммуникационных систем железнодорожного транспорта / П. М. Буй // Вестник БелГУТа: Наука и транспорт. – 2020. – № 2 (41). – С. 20–23.

6 **Буй, П. М.** Проектирование волоконно-оптической сети связи железной дороги : учеб.-метод. пособие / П. М. Буй, Н. Ф. Семенюта. – Гомель : БелГУТ, 2014. – 99 с.

7 **Буй, П. М.** Средства аутентификации в управляющих системах на транспорте : учеб.-метод. пособие / П. М. Буй, Д. Д. Семиход. – Гомель : БелГУТ, 2010. – 39 с.

8 **Вихорев, С. В.** Как узнать – откуда напасть или откуда исходит угроза безопасности информации / С. В. Вихорев, Р. Ю. Кобцев // Защита информации. Конфидент. – 2002. – № 2. – С. 44–49.

9 **Вихорев, С. В.** Как узнать – откуда напасть или откуда исходит угроза безопасности информации (окончание) / С. В. Вихорев, Р. Ю. Кобцев // Защита информации. Конфидент. – 2002. – № 3. – С. 80–84.

10 ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью. – Введ. 2007–01–01. – М. : Стандартинформ, 2006. – 62 с.

11 ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – Взамен ГОСТ Р 50922–96 ; введ. 2008–02–01. – М. : Стандартинформ, 2006. – 12 с.

12 Гражданский кодекс Республики Беларусь [Электронный ресурс] : 7 декабря 1998 г., № 218-З : с изм. и доп. от 29 июня 2020 г., № 33-З // Эталон Online / Нац. центр правовой информации Респ. Беларусь. – Минск, 2020.

13 **Домарев, В. В.** Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К. : ООО «ТИД “ДС”», 2001. – 688с.

14 **Завгородний, В. И.** Комплексная защита информации в компьютерных системах : учеб. пособие / В. И. Завгородний. – М. : Логос, 2001. – 264 с.

15 О государственных секретах [Электронный ресурс] : Закон Респ. Беларусь от 19 июля 2010 г., № 170-З : с изм. и доп. от 17 июля 2018 г., № 124-З // ЭТАЛОН Online / Нац. центр правовой информации Респ. Беларусь. – Минск, 2019.

16 Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь от 10 ноября 2008 г., № 455-З : с изм. и доп. от 11 мая 2016 г., № 362-З // ЭТАЛОН Online / Нац. центр правовой информации Респ. Беларусь. – Минск, 2017.

17 **Маммадов, Р.** Принципы работы протокола EIGRP [Электронный ресурс]. – Режим доступа : https://habr.com/ru/post/420667/#:~:text=Feasible%20successor%20—%20резервный%20маршрутизатор%20с,чем%20FD%20текущего%20маршрута%20successor. – Дата доступа : 09.11.2020.

18 О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН Online. Законодательство Республики Беларусь / Нац. центр правовой информации Респ. Беларусь. – Минск, 2019.

19 О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г., № 449 [Электронный ресурс] : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 20 февр. 2020, № 66 // ЭТАЛОН Online / Нац. центр правовой информации Республики Беларусь. – Минск, 2020.

20 О совершенствовании государственного регулирования в области защиты информации [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 дек. 2019 г., № 449 // ЭТАЛОН Online / Нац. центр правовой информации Респ. Беларусь. – Минск, 2020.

21 Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 ноя. 2010 г., № 575; с изм. и доп. от 24 января 2014 г., № 49 // ЭТАЛОН Online / Нац. центр правовой информации Респ. Беларусь. – Минск, 2018.

22 **Олифер, В.** Компьютерные сети. Принципы, технологии, протоколы : Юбилейное издание : учеб. для вузов / В. Олифер, Н. Олифер. – 6-е изд. – СПб. : Питер, 2020. – 1008 с.

23 **Рожошенко, Ю**. Безопасность в социальных сетях [Электронный ресурс]. – Режим доступа : https://vc.ru/social/81702-bezopasnost-v-socialnyh-setyah. – Дата доступа : 21.12.2020.

24 СТБ ISO/IEC 27001–2016. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Взамен СТБ ISO/IEC 27001–2011 ; введ. 2016–10–01. – Минск : БелГИСС, 2016. – 28 с.

25 СТБ 34.101.1–2014. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1: Введение и общая модель. – Взамен СТБ 34.101.1-2004 ; введ. 2014–09–01. – Минск : БелГИСС, 2014. – 60 с.

26 СТБ 34.101.30-2017. Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация. – Взамен СТБ 34.101.30-2007 ; введ. 2017–10–01. – Минск : БелГИСС, 2017. – 12 с.

27 **Семенов, Ю.** Алгоритмы телекоммуникационных сетей : учеб. пособие: в 3 ч. Ч. 3. Процедуры, диагностика, безопасность / Ю. Семенов. – Бином. Лаборатория знаний, 2016. – 511 с.

28 **Таненбаум, Э.** Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – Спб. : Питер, 2012. – 960 с.

29 Теория прикладного кодирования : учеб. пособие : в 2 т. Т. 1. Теория прикладного кодирования / В. К. Конопелько [и др.] ; под общ. ред. В. К. Конопелько. – Минск. : БГУИР, 2004.. – 285 с.

30 **Теренин, А. А.** Как построить модель типового нарушителя информационной безопасности / А. А. Теренин // Защита информации. INSIDE. – 2005. – № 5. – С. 18–24.

31 **Третьякович, К.** Защита компьютерных сетей на четырех уровнях модели ISO/OSI [Электронный ресурс] / К. Третьякович. – Режим доступа : https://nestor.minsk.by/sr/2004/02/40217.html. – Сетевые решения. – 2004. – № 2. – Дата доступа : 28.10.2020.

32 Kaspersky Security Bulletin: Статистика 2017 [Электронный ресурс]. – Режим доступа : https://securelist.ru/ksb-overall-statistics-2017/88203/. – Дата доступа : 11.09.2020.

33 Kaspersky Security Bulletin 2018. Статистика [Электронный ресурс]. – Режим доступа : https://securelist.ru/kaspersky-security-bulletin-2018-statistics/92906/. – Дата доступа : 11.09.2020.

34 Kaspersky Security Bulletin 2019. Статистика [Электронный ресурс]. – Режим доступа : https://securelist.ru/kaspersky-security-bulletin-2019-statistics/95264/. – Дата доступа : 11.09.2020.

35 Kaspersky Security Bulletin 2020. Статистика [Электронный ресурс]. – Режим доступа : https://securelist.ru/kaspersky-security-bulletin-2020-statistics/99505/. – Дата доступа : 13.12.2020.

36 Kaspersky Security Bulletin 2021. Статистика [Электронный ресурс]. – Режим доступа : https://securelist.ru/kaspersky-security-bulletin-2021-statistics/104160/ . – Дата доступа : 15.12.2021.

АЛФАВИТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

Учебное издание

БУЙ Павел Михайлович

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Учебно-методическое пособие

Редактор *Я. А. Васькевич*
Технический редактор *В. Н. Кучерова*

Подписано в печать 29.12.2021 г. Формат 60x84 1/16
Бумага офсетная. Гарнитура Times. Печать на ризографе.
Усл. печ. л. 10,93. Уч.-изд. л. 11,63. Тираж 100 экз.
Зак № 3170. Изд. № 54

Издатель и полиграфическое исполнение:
Белорусский государственный университет транспорта.
Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий
№ 1/361 от 13.06.2014.
№ 2/104 от 01.04.2014.
№ 3/1583 от 14.10.2017.
Ул. Кирова, 34, 246653, г. Гомель