РАЗДЕЛ 16
АНАЛИЗ СОСТОЯНИЯ И ОБОСНОВАНИЕ ПУТЕЙ СОВЕРШЕНСТВОВАНИЯ ПРОТОКОЛОВ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Аннотация. *Анализируются требования, предъявляемые к современным и перспективным телекоммуникационным системам, и сетям, в частности анализируются требования, предъявляемые к показателям качества передачи данных в инфокоммуникационных системах специального назначения (на примере телекоммуникационной сети системы управления бурением морских нефтедобывающих сооружений). Проводится анализ угроз безопасности информации в современных телекоммуникационных системах и сетях, а также стеков коммуникационных протоколов, используемых для их построения. Рассматриваются протоколы сетевой безопасности наиболее распространенных телекоммуникационных IP-сетей, исследуются особенности обеспечения достоверности при передаче пакетов данных.*

Ключевые слова: *протоколы безопасности, IP-сети, угрозы безопасности информации.*

Abstract. *The requirements are analized for future telecommunications systems and networks, in particular the requirements are analized for quality performance data in info-communication systems for special purposes (for example, a telecommunication network drilling offshore oil facilities management system). The information security threats in the modern telecommunication systems and networks are analized, as well as stacks of communications protocols used for their construction. We consider the network security protocols are the most common telecommunication IP-based networks, especially studied ensuring the reliability of the transmission of data packets.*

Keywords: *security protocols, IP-networks, information security threats.*

Современные телекоммуникационные системы и сети характеризуются быстрым ростом числа пользователей и потребителей информации, расширением спектра предоставляемых телекоммуникационных услуг, прежде всего, обеспечением доступа к различным мультимедийным сервисам и технологиям, поддержке удаленных пользователей, обслуживанию субъектов автоматизированного информационного взаимодействия, и т.д. [**Ошибка! Источник ссылки не найден.**] Эти тенденции обуславливают резкое повышение объемов обрабатываемых и передаваемых данных и, как следствие, ужесточение вероятностно-временных требований, предъявляемых к основным компонентам телекоммуникационных систем и сетей на всех этапах информационного обмена данными. Важнейшими показателями эффективности современных телекоммуникационных систем и сетей является их надежность и безопасность, от степени реализации этих характеристик непосредственно зависит уровень достоверности и

защищенности от современных угроз сетевой безопасности и, в конечном счете, качество предоставляемых телекоммуникационных услуг.

Анализ требований, предъявляемых к современным телекоммуникационным системам и сетям

Мировые тенденции в развитии телекоммуникационной отрасли определяют построение современных систем и сетей связи в виде мультисервисных телекоммуникационных сетей с обеспечением заданного уровня качества обслуживания (Quality of Service, QoS) (см. рис. 16.1) [**Ошибка! Источник ссылки не найден.**].

К основным требованиям функционирования телекоммуникационных систем и сетей относятся: производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость. Основные требования и их составляющие представлены на рис. 16.1.

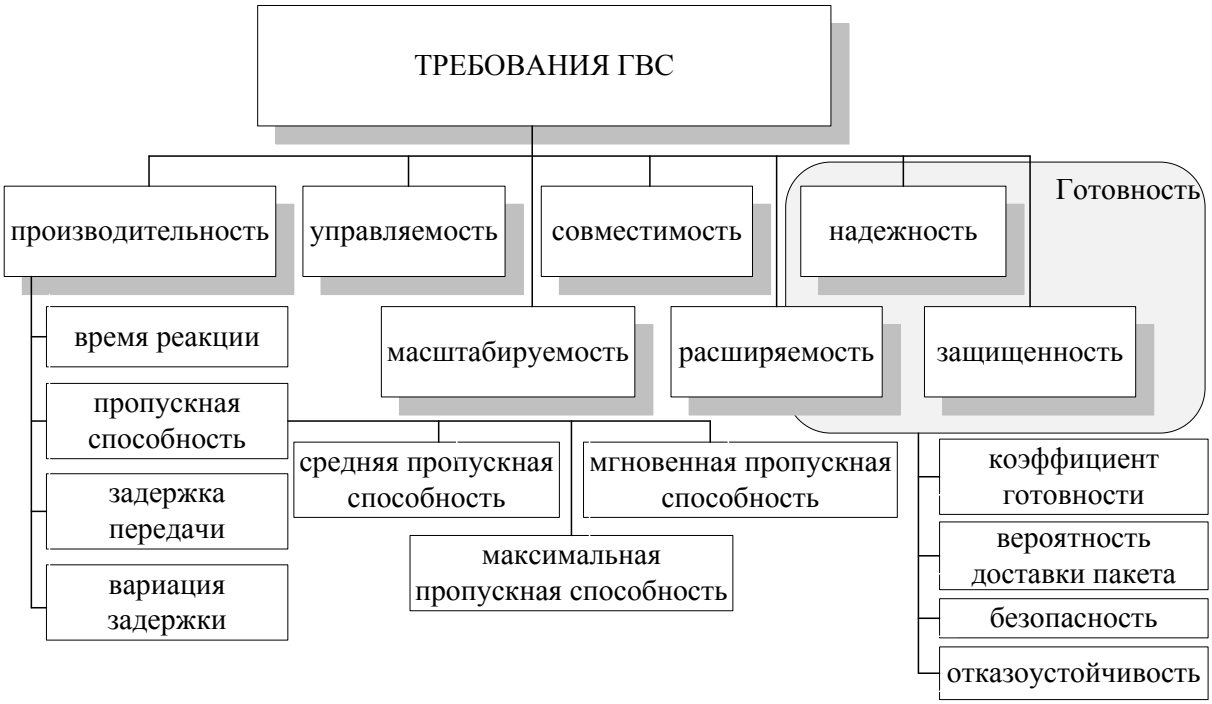

Рис. 16.1. Требования, предъявляемые к сетям

В настоящее время для оценки функционирования телекоммуникационных сетей к которым относятся локальные вычислительные сети (ЛВС) и глобальные вычислительные сети (ГВС) введено понятие “качество обслуживания” (Quality of Service, QpS) компьютерной сети, включающее только две самые важные характеристики сети – производительность и надежность [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**].

Проведенный анализ показателя качества обслуживания сети определяет два подхода к его обеспечению [**Ошибка! Источник ссылки не найден.**]. Первый подход, состоит в гарантированном обеспечении пользователю соблюдения некоторой числовой величины показателя качества обслуживания (обеспечения установленного показателя средней пропускной способности, показателя времени задержки передачи и т.д.). Так технологии Ethernet, Frame Relay и ATM позволяют строить сети, гарантирующие качество обслуживания по производительности (показатели средней пропускной способности, времени реакции, времени задержки и т.д).

Второй подход состоит в приоритетном обслуживании пользователей в соответствии с установленной иерархией сети. Таким образом, качество обслуживания зависит от степени привилегированности пользователя или группы пользователей, к которой он принадлежит. Для уполномоченных пользователей ГВС качество обслуживания не гарантируется, а гарантируется только уровень их привилегий. Такое обслуживание называется обслуживанием *best effort* – с наибольшим старанием. Проведенный анализ функционирования локальных сетей показывает, что по такому принципу работают IP-сети с технологией Ethernet, построенные на коммутаторах с поддержкой 802.1Q с приоритезацией кадров, на основе связанных стандартов IEEE 802.1Q и 802.1p.

Среди стандартов, посвященных качеству обслуживания в электросвязи, одно из центральных мест занимает Рекомендация МСЭ E.800 (Международный союз электросвязи). В ней качество обслуживания определяется как “суммарный эффект рабочих характеристик обслуживания, который определяет степень удовлетворенности пользователя данной службой”. Расширяя концепцию качества обслуживания, отвечающую Рекомендации E.800, Рекомендация МСЭ G.1000 разделяет рабочие характеристики обслуживания на функциональные компоненты и связывает их с сетевыми характеристиками, определенными в ряде рекомендаций МСЭ – таких как I.350, Y.1540 и Y.1541.

В дополнение к Рекомендации МСЭ G.1000, определяющей структуру связей между рабочими характеристиками (производительностью, надежностью, потерями, задержкой и др.) и характеристиками сети, Рекомендация МСЭ G.1010 содержит спецификации требований со стороны приложений, ориентированных на конечного пользователя [**Ошибка! Источник ссылки не найден.**].

На основании проведенного анализа в работе [**Ошибка! Источник ссылки не найден.**] в табл. 16.1 представлены основные критерии и показатели качества передачи информации в телекоммуникационных IP сетях, в соответствии с функциями, реализуемыми операторами

информационно-телекоммуникационных услуг [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**].

Таблица 16.1

Требования и показатели качества функционирования информационных систем

Показатель	Определение, раскрывающее смысл наименования	Показатели качества обслуживания
1	2	3
Достоверность информации		
Безошибочность информации	Свойство информации не иметь явных или скрытых ошибок и/или искажений	$P_{иск} \leq 10^{-5} - 10^{-7}$ – вероятность искажения двоичного символа
Безошибочность при хранении и передаче информации и сохранении её актуальности на момент использования	Свойство информации отражать реальное или оцениваемое состояние объектов и процессов прикладной области ИС со степенью приближения, обеспечивающей эффективное использование этой информации согласно целевому назначению системы	$P_{хран.} \leq 0{,}95$ – при угрозах проникновения в систему случайных источников опасности (в том числе вирусов), возникающих не чаще одного раза в неделю и активизируемых за среднее время 6 часов и более; $P_{хран.} \leq 0{,}9$ – при угрозах преднамеренного внедрения в систему источника опасного воздействия с частотой внедрения от одного раза в сутки до одного раза в час и активизацией в среднем за 1–3 часа и более
Полнота выходной информации	Свойство выходной информации отражать свойства всех требуемых объектов учёта предметной области ИС. Слагается из полноты реализации функций ИС, полноты ввода первоначальных информационных ресурсов и полноты оперативного отражения в ИС объектов учёта.	$T_{авт.вв} \leq 10$ с – время автоматического ввода в БД поступившей исходной информации от источников о чрезвычайном происшествии, а также время выдачи контрольной технологической информации о состоянии системы с $P_{пп} \geq 0{,}95$ $T_{отобр} \leq 10$ с – время представления на экран монитора поступивших в ИС команд, приказов и срочных сигналов с $P_{пп} \geq 0{,}9$

Продолжение табл. 16.1

1	2	3
Безопасность информации		
Конфиденциальность информации	Свойство используемой информации в течение заданного объективного периода конфиденциальности от ознакомления лицами, к ней не допущенными, и/или от несанкционированного считывания техническими средствами	$T_{без} \geq 200$ лет
Целостность информации	Состояние информации, при котором обеспечивается достижение целей её функционального применения в системе.	$T_{без.} \geq 200$ лет ,с $P_{мод} \geq 0,9$
Доступность информации	Состояние информации, её носителей и технологий обработки, при котором обеспечивается санкционированный доступ к ней и надёжность представления требуемой информации	$T_{без.} \geq 30$ лет , с $P_{НСД} \geq 0,9$
Оперативность информации		
Актуальность безошибочной информации	Свойство безошибочной информации (в том числе подлежащей последующей функциональной обработке или полученной в результате обработки) отражать текущее состояние объектов и процессов прикладной области ИС со степенью приближения, достаточной для получения на её основе достоверной выходной информации в интересах конечного пользователя. Актуальность характеризует старение информации во времени	$T_{стар} \leq 2,5$ мин. – время оперативных статистических отчетов с момента задания до начала выдачи результатов;
Время ввода информации	Время ввода оперативной информации от источников системы; Время ввода в базу данных (БД) статистической информации (например, о происходивших стихийных бедствиях, террористических актах и их исполнителях и др.)	$T_{вв} \leq 40$ с в БД другой оперативной исходной информации от источников с $P_{пп} \geq 0,8$; $T_{вв} \leq 180$ с $P_{пп} \geq 0,8$.

Окончание табл. 16.1

1	2	3
Время вывода информации	Время представления обобщенных справок с момента запроса; Время начала представления подробных справок с момента запроса;	$T_{выв} \leq 80$ с $P_{пп} \geq 0{,}8$; $T_{выв} \leq 100$ с $P_{пп} \geq 0{,}7$.
Пропускная способность	Максимальное количество переданной или полученной информации за единицу времени	ρ – зависит от параметров канала сети (IEEE802.X)
Вариация времени доставки пакета (IP packet delay variation, IPDV)	Разница сквозных задержек прохождения двух пакетов (RFC 3393), вследствие действия механизмов дифференцированного обслуживания сетевого трафика	IPDV $\leq 50^{-3}$ с
Время задержки (IP packet transfer delay, IPTD)	IPTD определяется как время доставки пакета между источником и получателем для всех пакетов – как успешно переданных, так и пораженных ошибками.	IPTD $\leq 100^{-3} – 400^{-3}$ с
Коэффициент потери пакетов (IP packet loss ratio, IPLR)	Коэффициент IPLR определяется как отношение суммарного числа потерянных пакетов к общему числу принятых в выбранном наборе переданных и принятых пакетов.	IPLR $\leq 10^{-3}$ с
Коэффициент ошибок пакетов IP (IP packet error ratio, IPER)	Коэффициент IPER определяется как суммарное число пакетов, принятых с ошибками, к сумме успешно принятых и пакетов, принятых с ошибками	IPER $\leq 10^{-3}$ с

Проведенный анализ табл. 16.1 показал, что показатели качества функционирования телекоммуникационной сети дифференцируются по функциям и решаемым задачам, реализуемыми соответствующими службами, и при возникновении повышенного риска программно-технической атаки, угрожающей безопасному функционированию системы, должен предусматриваться автоматический переход к специальному дежурному режиму функционирования. Реализация технологий защиты не должна приводить к нарушению требуемых вероятностно-временных характеристик функционирования информационных систем.

На основе данных, полученных в результате исследования Европейским исследовательским центром в области телекоммуникаций (RACE – Research on Advanced Communication) определены допустимые значения требований к основным показателям качества обслуживания в

информационно-телекоммуникационных системах (ИТКС), приведенные в табл. 16.2.

Таблица 16.2

Целевые показатели качества, воспринимаемого абонентом

Приложение	Типовые скорости передачи данных	Время задержки (IPTD)	Коэффициент потери пакетов (IPLR)	Коэффициент потери пакетов (IPLR)
Телефония	4–64 кбит/с	< 150 – 400 мс	< 1 мс	$\leq 10^{-3}$ с
Передача голосовых сообщений	4–32 кбит/с	< 1 с – для воспр.; < 2 с – для записи	< 1 мс	$\leq 10^{-3}$ с
Высококачественное потоковое аудио	16–128 кбит/с	< 10 с	< 1 мс	$\leq 10^{-3}$ с
Видеотелефония	16–384 кбит/с	< 150 – 400 мс		
Передача видео	16–384 кбит/с	< 10 с		
Web-навигация	≈ 80 кбит/с	< 2 с/страница; < 4 с/страница	Не применяется	
Передача массивов данных	80–10^4 Мбит/с	< 15 – 60 с		
Осуществление транзакций	< 80 кбит/с	< 2 – 4 с		
Команды (управление)	≈ 8 кбит/с	< 250 мс		
Неподвижное изображение	< 800 кбит/с	< 15 – 60 с		
Электронная почта (доступ к серверу)	< 80 кбит/с	< 2 – 4 с		
Электронная почта (сервер-сервер)	< 80 кбит/с	Несколько мин.		

Проведенный анализ показал, что в связи с быстрым ростом числа пользователей и потребителей информации, расширением спектра предоставляемых телекоммуникационных услуг, прежде всего, обеспечением доступа к различным мультимедийным сервисам и технологиям, резко повышаются объемы обрабатываемых и передаваемых данных, что, как следствие, приводит к ужесточению вероятностно-временных требований, предъявляемых к основным компонентам телекоммуникационных систем и сетей на всех этапах информационного обмена данными. Это относится, в первую очередь, к показателям безопасности передачи данных. Так по данным [**Ошибка! Источник ссылки не найден.**] актуальность создания телекоммуникационных систем и сетей с защищенными каналами передачи данных в последние годы резко возросла. Возросли и требования к показателям безопасности передачи данных в телекоммуникационных системах и сетях, особенно в сетях специального назначения, в которых

отказ в обслуживании или выход конкретных параметров качества за установленные пределы может привести к катастрофическим последствиям в финансовом секторе, промышленности, энергетическом комплексе и пр. В качестве примера можно привести сеть системы управления бурением морских нефтегазодобывающих сооружений – многоуровневую мультиканальную телекоммуникационную сеть с использованием различных типов сетей и технологий.

Современный подход к управлению системами нефтедобывающих сооружений подразумевает широкое применение геоинформационных систем (ГИС) – программно-аппаратных комплексов, осуществляющих сбор, отображение, обработку, анализ и распространение информации на основе электронных карт, баз данных и сопутствующих материалов с географически организованной информацией. Наиболее важный и трудоемкий этап в процессе создания и эксплуатации подобного рода информационных систем – своевременное получение достоверных данных о пространственно-распределенных объектах и явлениях. Одна из таких технологий – системы СКАДА [**Ошибка! Источник ссылки не найден.**]. СКАДА (от англ. SCADA supervisory control and data acquisition) – система диспетчерского управления и сбора данных, в реальном времени обрабатывающая информацию, получаемую по каналам связи с датчиков объекта управления. Количество датчиков может достигать несколько десятков тысяч. СКАДА используется для реализации автоматизированной системы управления технологическим процессом (АСУТП), автоматизированной системы контроля и учета энергоресурсов (АСКУЭ) и систем экологического мониторинга.

СКАДА представляет программно-аппаратный комплекс, обеспечивающий выполнение необходимых функций. Надежность системы осуществляется дублированием каналов оптоволоконной, спутниковой и радиосвязи, и передачи данных. Данные системы служат для предотвращения чрезвычайных ситуаций на производствах и обеспечения безопасной работы всей инфраструктуры, также СКАДА, совмещенная с системой обнаружения утечек (СОУ), позволяет определить наличие даже незначительных утечек. На рис.16.2 приведена структурная схема СКАДА СОПТ WaveControl [**Ошибка! Источник ссылки не найден.**].

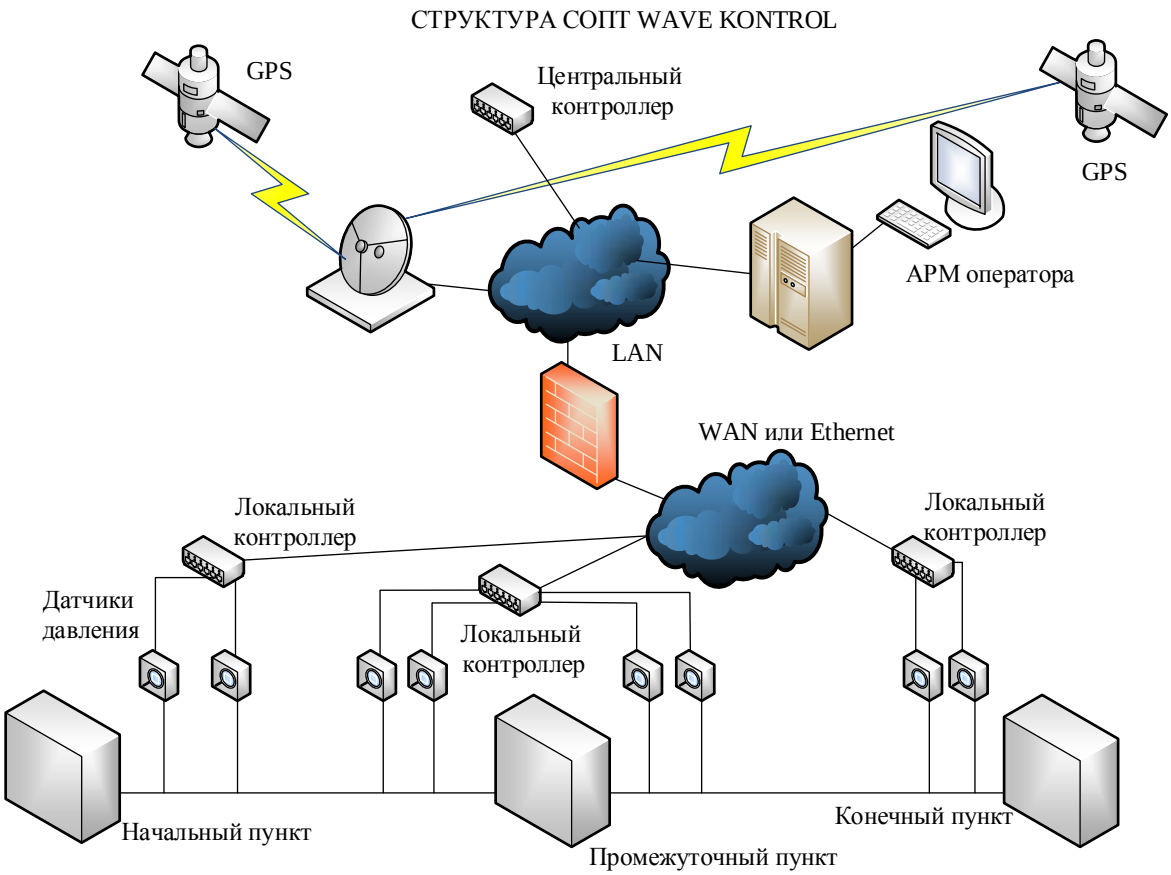

Рис. 16.2. Структурная схема СКАДА СОПТ WaveControl

Для обеспечения передачи данных в СКАДА используется система транспорта данных (аппаратно-программный комплекс), встроенным в систему “ИСМТ” (инфразвуковая система мониторинга трубопроводов), обеспечивающим передачу данных от модулей первичного сбора и обработки данных до компьютера управления. Система транспорта настраивается на передачу данных по одному из следующих каналов: оптоволоконный канал связи; радиоканал (GPRS); канал телемеханики (реализованы нескольких широко используемых протоколов связи); телефонная линия; физическая двухпроводная линия; УКВ – радиоканал; спутниковый канал. Проведенный анализ сети СКАДА показал, что для обеспечения безопасности используются стандартные процедуры, протоколы и программно-аппаратные средства, используемые в глобальных сетях Ethernet.

Для обеспечения управления бурением используется система управления бурением на основе сети управления бурением. Структурная схема сети управления бурением приведена на рис. 16.3.

Для обеспечения достоверности и безопасности данных, циркулирующих в сети управления бурением используются протоколы локальных и глобальных вычислительных сетей. В локальных сетях, используется разделительная среда передачи данных (моноканал) и основная роль отводится протоколам физического и канального уровней, поскольку эти уровни в наибольшей степени

отражают специфику локальных сетей. Глобальная вычислительная сеть, ГВС (Wide Area Network, WAN) служит для предоставления сервисов большому количеству конечных абонентов, распределенных на больших территориях.

Для обеспечения достоверности и безопасности данных, циркулирующих в сети управления бурением используются протоколы локальных и глобальных вычислительных сетей. В локальных сетях, используется разделительная среда передачи данных (моноканал) и основная роль отводится протоколам физического и канального уровней, поскольку эти уровни в наибольшей степени отражают специфику локальных сетей. Глобальная вычислительная сеть, ГВС (Wide Area Network, WAN) служит для предоставления сервисов большому количеству конечных абонентов, распределенных на больших территориях.

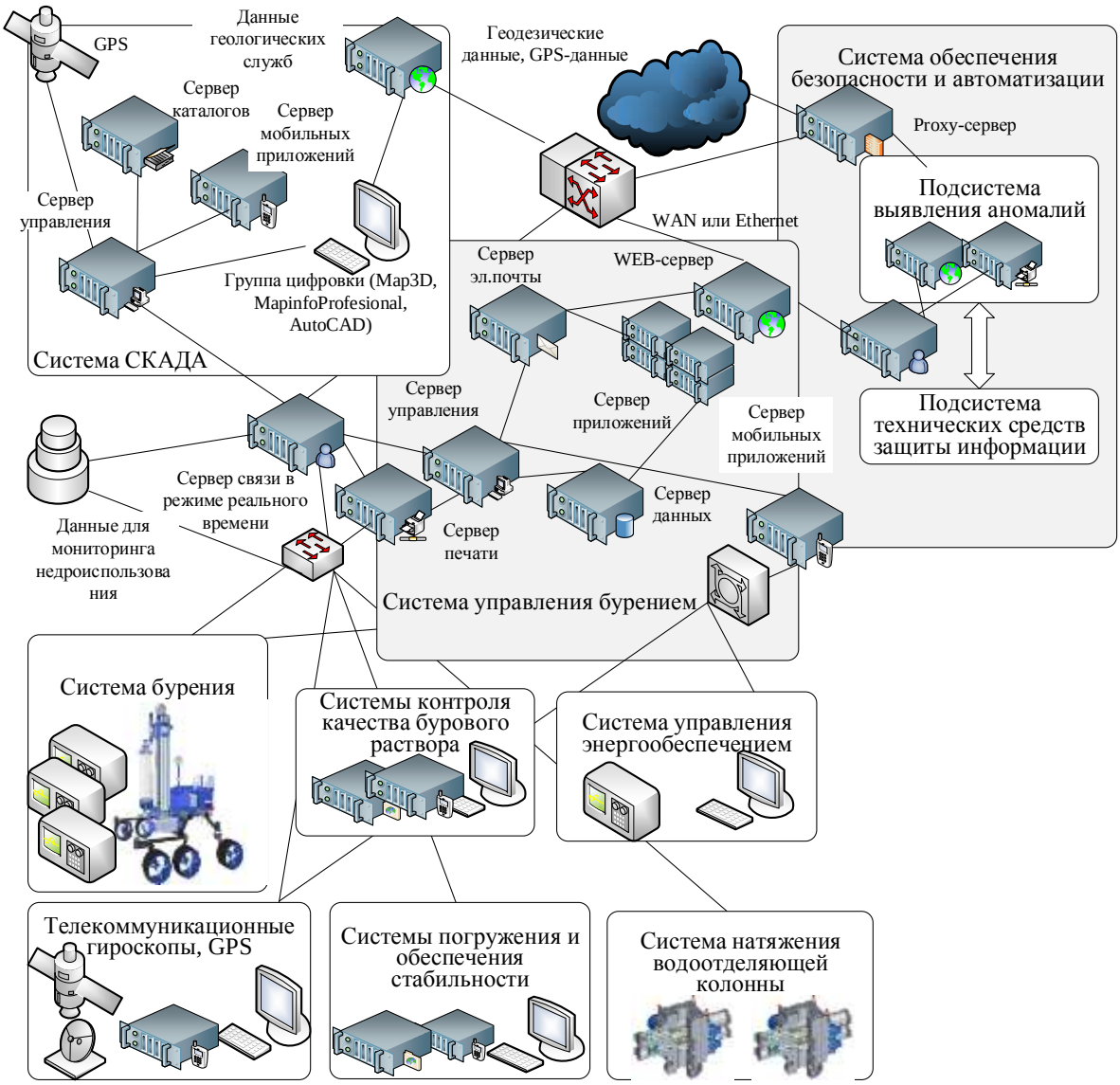

Рис. 16.3. Структурная схема сети управления бурением

Проведенный анализ [**Ошибка! Источник ссылки не найден.**] показал, система управления бурением морских нефтегазодобывающих сооружений

является многоуровневой автоматизированной системой реального времени, использующей элементы аппаратуры передачи данных с соответствующими процедурами и протоколами как локальных так и глобальных сетей (телекоммуникационных систем и сетей), относится к критическим системам – выход (сбой) одной из подсистем может привести к разрушению всей системы и техногенной катастрофе в целом.

Проанализируем возможные угрозы безопасности информационных технологий в телекоммуникационных системах и сетях, в том числе специального назначения, проведем обзор применяемых механизмов обеспечения целостности, аутентичности и конфиденциальности информации.

Анализ угроз безопасности информации в современных телекоммуникационных системах и сетях

Морские нефтегазовые сооружения является опасными производственными объектами и характеризуются высокой аварийностью. По данным [**Ошибка! Источник ссылки не найден.**] на континентальном шельфе за период с 1990 по 2013 только на стационарных платформах произошло 63938 несчастных случаев. В США с 2000 по 2013 гг. в результате аварий на морских нефтегазовых сооружениях погибли около 80 человек, 1393 – получили травмы различной степени тяжести. Следует иметь в виду, что экономический ущерб от потери одной нефтяной платформы составляет от 200 до 1000 млн. долларов США [**Ошибка! Источник ссылки не найден.**], а масштабные разливы нефти способны привести к экологической катастрофе. Анализ основных тенденций мирового рынка нефти показал наличие геополитической составляющей в его развитии. Данный рынок демонстрирует зависимость от внешней политики США и стран ОПЕК, в последние годы растет влияние России. Этот факт подтверждается периодами кризисных явлений на мировой арене, которые непосредственно отражаются на цене нефти и экономическими мерами реагирования государств. По оценкам зарубежных специалистов [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**] большинство войн в человеческой истории имело экономическую подоплеку. Если говорить о войнах XX столетия – в том числе, подоплеку энергетическую, и прежде всего нефтяную. Нефтяные войны ведут корпорации, так сказать, через голову народов и стран, то есть нечто, далеко выходящее за рамки классического определения деловой конкуренции: полноценная разведка конкурентов с использованием всех методов, применяемых обычной государственной разведкой, включая внедрение агентуры, прослушивание, корпоративные спецоперации, вплоть до организации диверсий в отношении активов и ресурсов конкурентов, а также их физического “устранения”. В таких войнах, помимо собственных корпоративных средств, корпорации

нередко активно задействуют и государственные ресурсы. Это характерно, прежде всего, для тех слабых государств, на территории которых расположены ценные для корпорации активы. Располагая корпоративными бюджетами, качественно превышающими бюджеты этих государств или сопоставимыми с этими бюджетами, – корпорации приводят в действие пружины элитных противоречий в этих государствах, организуют государственные перевороты, провоцируют гражданские войны. Наконец, подобные корпорации нередко входят в альянсы с так называемыми “частными армиями”. Имеются в виду структуры типа знаменитых “Экзектьютив ауткамз” и “Сендлайн Интернешнл”. В условиях обостряющейся мировой борьбы за контроль над энергоресурсами, Азербайджану необходимо не только сохранить достигнутые позиции, но и не позволить мировым державам превратить себя в очередной объект геостратегического противостояния [**Ошибка! Источник ссылки не найден.**].

Современные телекоммуникационные системы и сети, в том числе специального назначения к которым можно отнести систему управления бурением морских нефтегазовых сооружений, состоят из следующих основных структурно-функциональных элементов (см. рис. 16.2, 16.3):

– каналов и АПД (локальных, телефонных, с узлами коммутации и т.д.);

– межсетевых коммутаторов второго или третьего уровня (шлюзов, центров коммутации пакетов, коммуникационных рабочий станций) – элементов, обеспечивающих соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия;

– серверов или Host-машин (служб файлов, печати, баз данных и т.п.) не выделенных (или выделенных, то есть не совмещенных с рабочими станциями) высокопроизводительных рабочих станций, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п. действий;

– системы управления БД (СУБД) СКАДА, обеспечивающих непосредственный мониторинг и контроль нескольких тысяч датчиков объекта управления;

– оконечного оборудования, рабочих станций – отдельных рабочих станций (ПК) или удаленных терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов и т.д).

Каналы и средства связи в силу своей большой пространственной протяженности (через неконтролируемую или слабо контролируемую территорию) практически всегда подвержены угрозам подключения к ним, либо вмешательства в процесс передачи данных.

В особой защите нуждаются коммутационные элементы телекоммуникационных сетей и серверы БД, обеспечивающие передачу информационных потоков данных о состоянии объекта в режиме реального времени, хранение информации мониторинга, СУБД, системы принятия решений. Рабочие станции являются наиболее доступными компонентами телекоммуникационных сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. На рис. 16.4 представлена классификация основных угроз информационной безопасности в телекоммуникационных системах и сетях.

С рабочих станций осуществляется управление процессами обработки данных, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы [**Ошибка! Источник ссылки не найден.**].

В случае атак на систему управления бурением морских нефтегазовых сооружений будут направлены на сбор сведений в обход многоуровневых систем защиты от вторжений, а также угрозы информационным ресурсам, которые подразделяются на внешние (технические) и внутренние (неправомерные действия сотрудников).

Классификационные признаки потенциально-опасных событий (ПОС) при функционировании программного обеспечения и характерные последствия при их реализации в ИС приведены на рис. 16.5.

Нарушение конфиденциальности информации напрямую связано с реализацией угрозы несанкционированного доступа к ИС и является следствием нарушения системы защиты информации.

Угрозы нарушения конфиденциальности, как правило, выступают в форме несанкционированного обращения.

Термин “несанкционированное обращение” означает активные действия, направленные на сбор или хищение ценной информации, закрытой для доступа посторонних лиц.

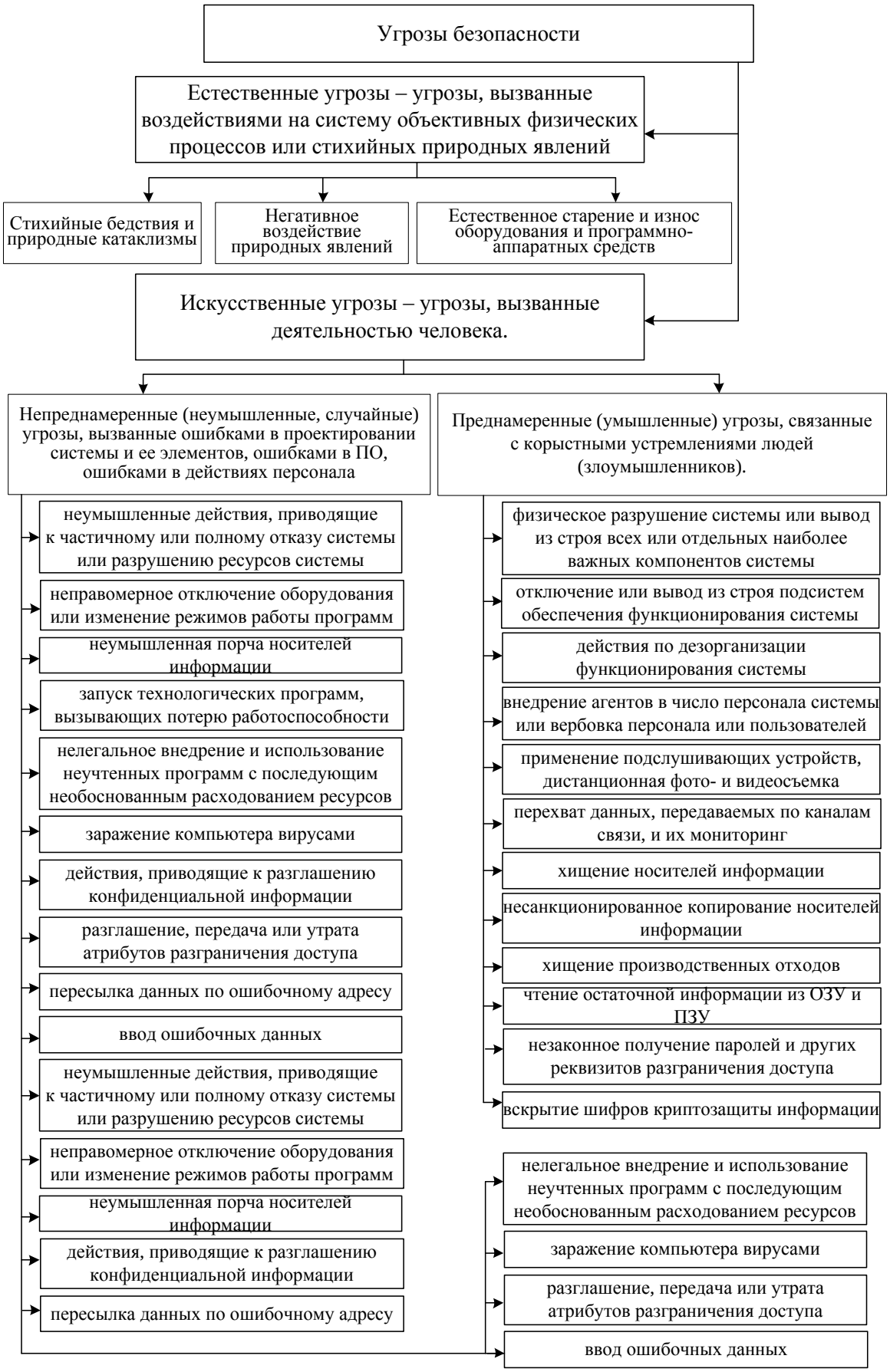

Рис. 16.4. Основные угрозы безопасности в телекоммуникационных системах и сетях

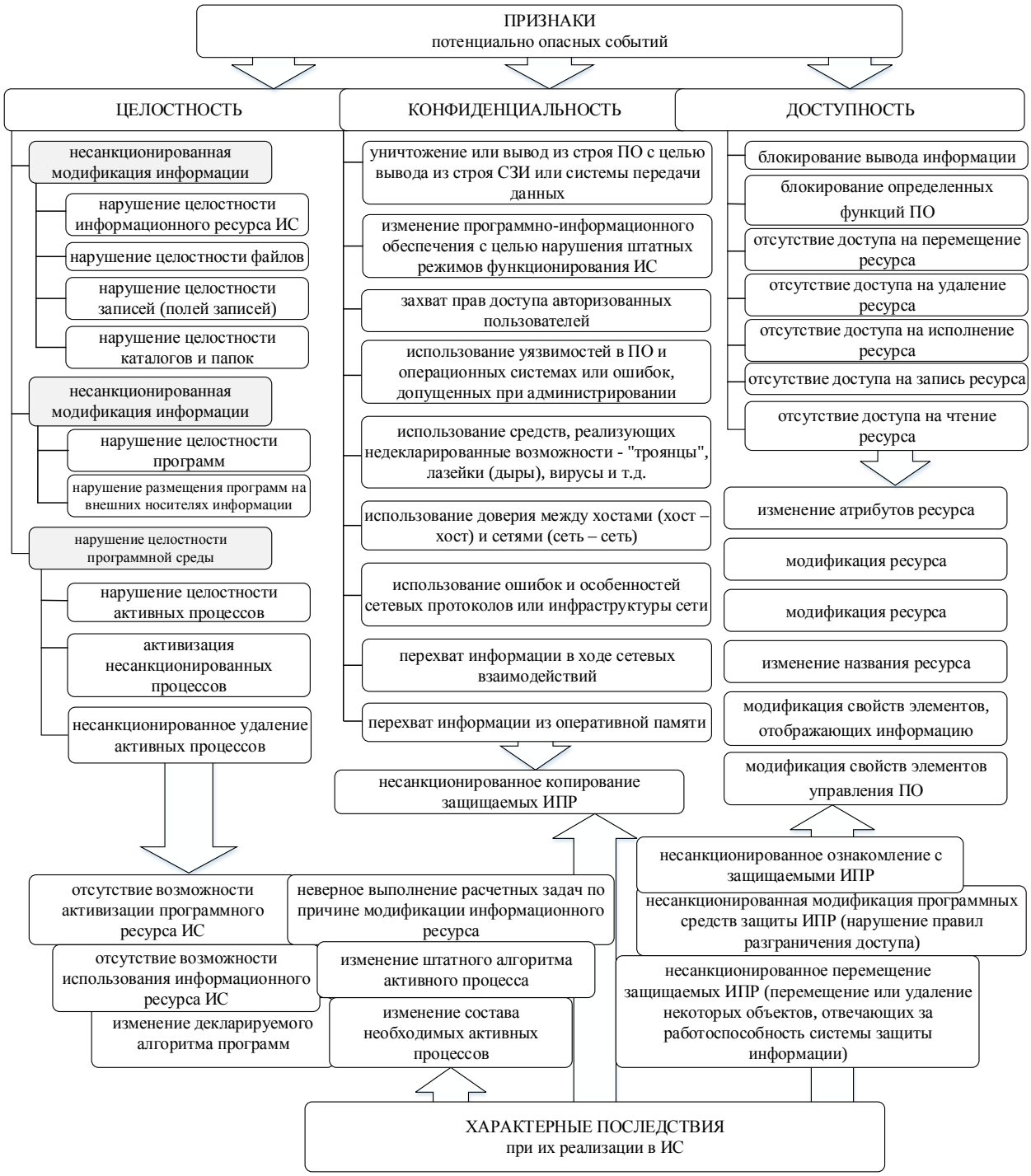

Рис. 16.5. Классификационные ПОС при функционировании ПО и характерные последствия при их реализации в ИС

Опыт эксплуатации показывает, что около 80% попыток НСД к конкретной ИС осуществляют лица, работающие или работавшие с данной системой. Поэтому считается, что потенциальный нарушитель имеет достаточно высокую квалификацию и ему известны принципы функционирования ИС.

На сегодняшний день многие злоумышленники пользуются инструментами для автоматизации проведения стандартных атак. За

последние несколько лет эти методы усовершенствовались, в них появились интеллектуальные алгоритмы, служащие для создания действительно комплексных смешанных угроз, которые распространяются автоматизированным путем с высокой степенью резервирования (рис. 16.6).

Рис. 16.6. Рост реализация сетевых атак

Проведенный анализ основных угроз показал, что дальнейшее развитие вычислительных возможностей и IT-технологий позволяет “модернизировать” виды угроз, расширять и совершенствовать технологии их реализации, создавать новые современные технологии взлома систем безопасности в телекоммуникационных системах и сетях, а в случае специфики нефтедобывающей отрасли (нефтяные войны) атаки могут нести и техногенный характер, ликвидацию системы автоматизации и защиты с последующей угрозой техногенной катастрофы.

Лидирующую позицию по реализации угроз сетевой безопасности занимают нарушения, приводящие как к утечке закрытой информации, так и к навязыванию ложной информации или неправильной работе компонентов телекоммуникационной системы – атаки на нарушение услуг целостности и конфиденциальности. Учитывая высокие темпы развития современных вычислительных систем, а также последние успехи в развитии методов криптоанализа, следует, очевидно, считать реализацию угроз сетевой безопасности вполне осуществимой [**Ошибка! Источник ссылки не найден.**]. Данный вывод обосновывает необходимость дальнейшего развития протоколов сетевой безопасности. В частности, совершенствование моделей и методов обеспечения целостности, аутентичности и конфиденциальности информации следует считать наиболее востребованным на сегодняшний день

направлением исследований в области современных телекоммуникационных систем и сетей.

Проведем анализ современных коммуникационных протоколов телекоммуникационных систем и сетей, в том числе, протоколов сетевой безопасности, исследуем особенности их реализации на различных уровнях модели OSI.

Анализ протоколов обеспечения достоверности и безопасности данных в современных телекоммуникационных системах

Взаимодействие компонентов современных телекоммуникационных сетей происходит в соответствии с определенными правилами обмена сообщениями и их форматами, то есть в соответствии с применяемыми коммуникационными протоколами. По определению, под коммуникационным протоколом понимается набор правил и процедур, регулирующих порядок осуществления связей в телекоммуникационных системах и сетях. Под стеком коммуникационных протоколов понимается иерархически организованная совокупность протоколов, решающих задачу взаимодействия узлов сети.

Для обеспечения достоверности данных в протоколах телекоммуникационных систем используются методы и процедуры помехоустойчивого кодирования (использование канального контроля ошибок обеспечивает надежную доставку кадров и реализуется канальным уровнем модели ISO/OSI (эталонной модели взаимодействия открытых сетей) и повторной передачи данных (использование сквозного контроля в промежуточных узлах позволяет удалять некорректные кадры, следовательно, некоторые кадры могут не прибыть к получателю. Тот обращается к отправителю с просьбой повторить передачу потерянных и неверных кадров. Таким образом, повторная передача кадров осуществляется снова через всю сеть. По терминологии ISO/OSI сквозной контроль ошибок реализует транспортный уровень).

Общая классификация известных на сегодняшний день протоколов коррекции ошибок (протоколов обеспечения достоверности передачи данных) в компьютерных системах и сетях приведена на рис. 16.7.

Обычно используется протокол LAP-B. Этот протокол обеспечивает сбалансированный режим работы, то есть оба узла, участвующих в соединении, равноправны. По протоколу LAP-B устанавливается соединение между ООД (DTE), т.е. компьютером, IP- или IPX-маршрутизатором, и АПД (DCE) т.е. коммутатором сети. Хотя стандарт это и не оговаривает, но по протоколу LAP-B возможно также установление соединения на канальном уровне внутри сети между непосредственно связанными коммутаторами.

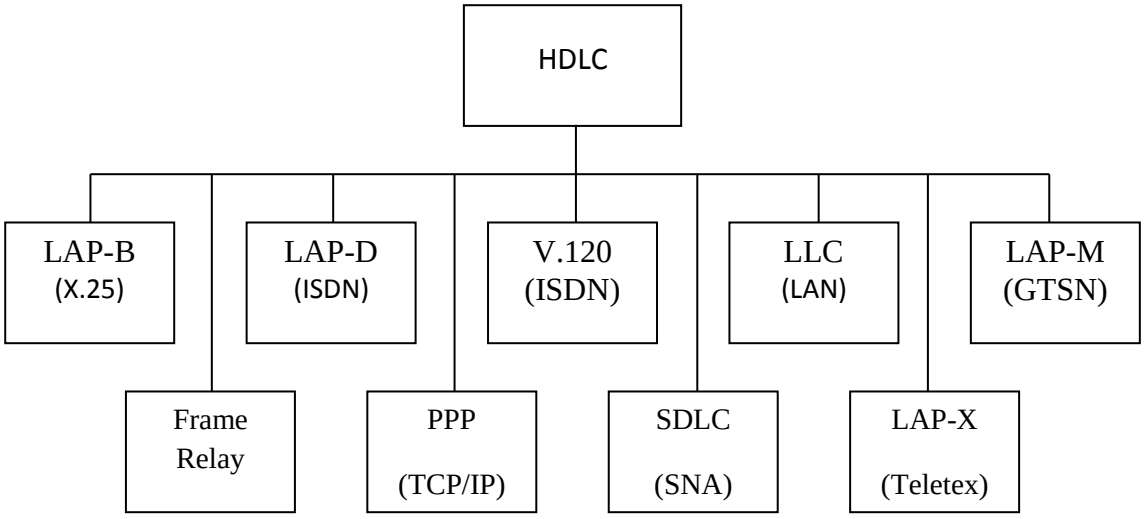

Рис. 16.7. Множество протоколов HDLC

Поддерживается как нормальный режим (с максимальным окном в 8 кадров и однобайтовым полем управления), так и расширенный режим (с максимальным окном в 128 кадров и двухбайтовым полем управления).

Для обеспечения передачи смешанной (текстовой и графической) информации по каналам высокого качества (широкополосные цифровые каналы, выделенные цифровые линии, оптоволоконные кабели), частота ошибки в которых составляет $10^{-9} \div 10^{-12}$, используются сетевые технологии и протоколы: ATM, Frame Relay, ISDN, SDH, TCP/IP, позволяющие обеспечить контроль ошибок либо в каждом канале отдельно, либо на оконечных узлах.

Для обеспечения достоверности в каналах с невысокими требованиями к достоверности передаваемой информации ($P_{ош} = 10^{-2}–10^{-3}$) используются методы помехоустойчивого кодирования.

Среди методов применения помехоустойчивых кодов выделяют два основных подхода: с автоматическим переспросом и с прямым исправлением ошибок.

Первый подход получил развитие преимущественно в системах коммерческого назначения. Это обусловлено невысокими требованиями к достоверности передаваемых сообщений ($P_{ош} = 10^{-5}–10^{-6}$) при жестких ограничениях на экономическую рентабельность употребляемых средств. Так в стандартизированных протоколах коррекции ошибок (V.42 MNP2 – MNP4) используется помехоустойчивое кодирование циклическими кодами в режиме выявления ошибок (проверочная часть 16 – 32 бита). Протоколы допускают наличие обратной связи и автоматический переспрос сообщений.

Второй подход – прямое исправление ошибок – получил развитие преимущественно в телекоммуникационных системах специального назначения, таких, например, как системы передачи данных АСУ

специального назначения. Он состоит в использовании помехоустойчивых кодов для исправления возникающих ошибок и не допускает наличие обратной связи.

Существенным недостатком современных сетевых технологий является необходимость перехода на новые качественные кабели (витую пару неэкранированную – UTP 5 категории, экранированную витую пару – STP; оптоволоконные кабели), что не всегда является рентабельным и экономически выгодным. Поэтому используются линии связи уже существующих каналов проводной и радиосвязи, телефонной сети общего назначения, ведомственных и производственных сетей, качество которых существенно ниже требуемого (частота появления ошибок составляет 10^{-2} – 10^{-3}), что приводит к существенному увеличению времени передачи одного кадра. Широкое применение протоколов с автопереспросом в компьютерных сетях приводит к необходимости усовершенствования существующих протоколов ГВС, что влечет при повышении надежности к снижению эффективности обмена данными.

Проведенный анализ позволяет сделать следующие выводы:

современные телекоммуникационные системы и сети создаются и функционируют с использованием большого числа коммуникационных протоколов, которые, используя конкретные наборы процедур и правил, реализуют порядок осуществления связей на соответствующих уровнях модели взаимодействия открытых систем. Большинство применяемых коммуникационных протоколов объединены в иерархически организованную совокупность (стеки протоколов) для решения задач взаимодействия узлов телекоммуникационных сетей;

применяемые коммуникационные протоколы предназначены для решения конкретных технических задач и по этому признаку могут быть классифицированы на: транспортные протоколы, протоколы аутентификации пользователей и устройств, протоколы маршрутизации, протоколы обеспечения безопасности передачи данных. Коммуникационные протоколы верхних уровней модели OSI реализуются, преимущественно, в программном виде через элементы сетевой операционной системы, например, в виде драйверов сетевых адаптеров, серверных и клиентских компонент сетевых сервисов. Коммуникационные протоколы нижних уровней модели OSI реализуются, как правило, в аппаратном виде, регламентируя правила функционирования сетевых устройств. Кроме того, как показал проведенный анализ, практически во всех стеках коммуникационных протоколов на нижних уровнях модели OSI используются одни и те же протоколы (Ethernet, Token Ring, FDDI и пр.), которые позволяют использовать во всех телекоммуникационных системах и сетях идентичную технологическую платформу;

в качестве транспортной основы подавляющего большинства телекоммуникационных сетей и систем выступают сети, использующие стеки протоколов технологий IP. Например, по данным настоящее время в мире только 1% компьютерных систем не поддерживает протокол IP вообще, остальные 99% используют его либо как единственный протокол, либо в качестве одного из нескольких протоколов. Кроме того, протоколы IP хорошо работают в сетях со сложной топологией, рационально используя наличие подсистем и экономно расходуя пропускную способность низкоскоростных линий связи, что особенно актуально для сложных распределенных телекоммуникационных систем специального назначения.

Одним из основных признаков обеспечения безопасности информации в ИС является сохранение ее целостности, конфиденциальности и доступности.

В ГОСТ РВ 51987-2002 “Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения” введены следующие определения [**Ошибка! Источник ссылки не найден.**]:

целостность информации – состояние информации, при котором обеспечивается достижение целей ее функционального применения;

конфиденциальность информации – свойство используемой информации быть сохраненной в течение заданного объективного периода конфиденциальности от ознакомления лицами, к ней не допущенными, и/или от несанкционированного считывания техническими средствами;

доступность информации – это состояние информации, ее носителей и технологий обработки, при котором обеспечивается санкционированный доступ к ней и надежность представления требуемой информации.

Для обеспечения безопасности в proxy-серверах, а также в протоколах транспортного уровня ISO/OSI глобальных вычислительных систем используются криптографические алгоритмы, общая классификация представлена на рис. 16.8.

На прикладном уровне модели ISO/OSI используются программные средства защиты и выявления аномалий: брандмауэры, firewall-ы, антивирусные программы, NAT-ы, алгоритмы шифрования полей БД. Основные способы использования МСЭ приведены в прил. А.

Для минимизации риска и сохранения функциональности dns- и web-серверов используют их “логическое размещение” за основным шлюзом сети, но перед межсетевым экраном, который обеспечивает защиту внутренних рабочих станций в хостах сети. Логическую область их размещения называют демилитаризированной зоной.

Основные протоколы обеспечения достоверности и безопасности в IP-сетях представлены в табл. 16.2.

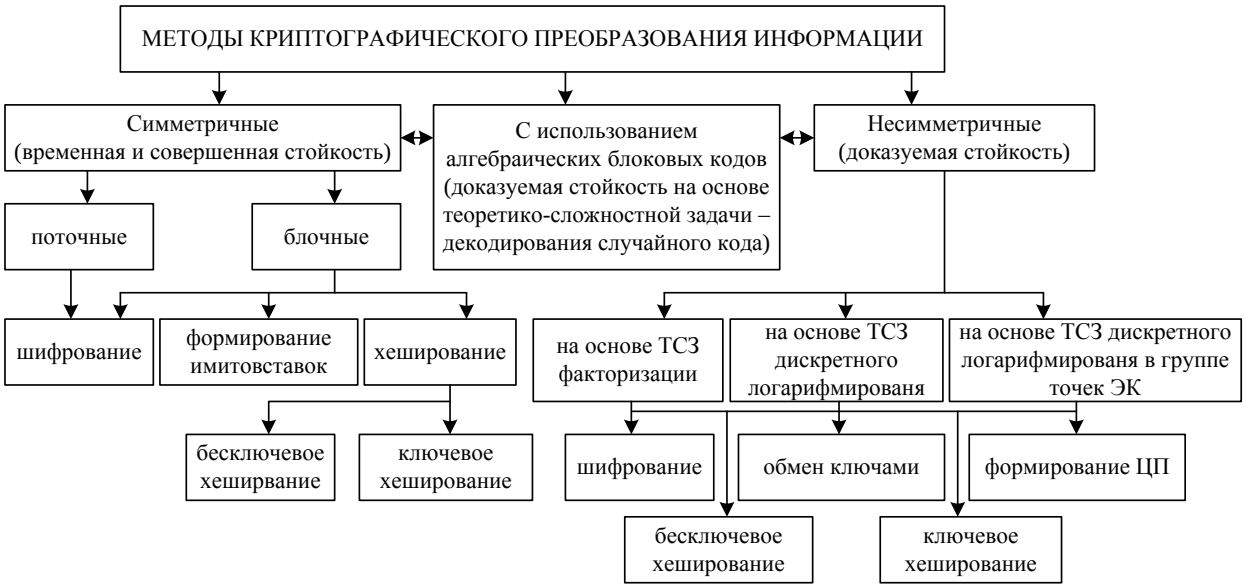

Рис. 16.8. Общая классификация криптографических методов защиты

Таблица 16.2

Основные протоколы обеспечения достоверности и безопасности в IP-сетях

Приложение	Протоколы обеспечения достоверности	Протоколы обеспечения безопасности
Факсимильная связь	Т.38 (на транспортном уровне используется TCP/IP и UDP)	
Передача голосовых сообщений	H. 323, RTP/RTCP, UDP, TCP/IP	
Высококачественное потоковое аудио	UDP (RTP/RTCP)	IPSec
Видеотелефония	UDP (RTP/RTCP)	IPSec
Передача видео	UDP (RTP/RTCP)	IPSec
Web-навигация	≈ 80 кбит/с	IPSec, SSL (TLS)
Передача массивов данных	SMTP, TCP/IP, FTP	IPSec, SSL (TLS)
Команды (управление)	TCP	IPSec, SSL (TLS)
Неподвижное изображение	UDP (RTP/RTCP)	IPSec
Электронная почта (доступ к серверу)	TCP/IP, FTP	IPSec, SSL (TLS)
Электронная почта (сервер-сервер)	TCP/IP, FTP	IPSec, SSL (TLS)

Проведенный анализ табл. 16.2 показал, что для обеспечения контроля достоверности передаваемых пакетов (кадров) в IP-сетях на канальном уровне используется подмножество протокола HDLC (High-level Data Link Control – высокоуровневая процедура управления каналом), обеспечивающее

возможность автоматической передачи в случае возникновения ошибок в линии связи, либо на транспортном уровне используются протоколы TCP (Transmission Control Protocol, протокол управления передачей), а при передачи видеоданных используется протокол UDP (User Datagram Protocol, протокол пользовательских дейтаграмм).

Данные протоколы обеспечивают контроль достоверности передаваемых данных и при возникновении ошибок в пакете (кадре) обеспечивают повторную передачу соответствующих пакетов, что при реализации атаки с увеличением уровня вероятности ошибки в канале связи значительно снижают скорость передачи данных.

Наиболее компромиссным вариантом реализации функций безопасности в телекоммуникационных системах и сетях являются протоколы сетевой безопасности IPSec, функционирующие на сетевом уровне [**Ошибка! Источник ссылки не найден.**]. С одной стороны, они прозрачны для приложений, а с другой – могут работать практически во всех сетях, так как основаны на широко распространенном протоколе IP [**Ошибка! Источник ссылки не найден.**].

Протоколы сетевой безопасности IPSec (Internet Protocol Security (IPSec) – это согласованный набор открытых стандартов, имеющий на сегодняшний день конкретную спецификацию, который, в то же время, может быть дополнен новыми протоколами, алгоритмами и функциями сетевой безопасности.

Основное назначение протоколов IPSec – обеспечение безопасной передачи данных по IP-сетям. Их применение обеспечивает [**Ошибка! Источник ссылки не найден.**]:

целостность – способность телекоммуникационной сети обеспечивать передачу данных без искажения, потери или дублирования;

аутентичность – способность телекоммуникационной сети обеспечивать передачу данных с возможностью доказательства их подлинности (т.е. того, что данные переданы именно тем отправителем, за кого он себя выдает);

конфиденциальность – способность телекоммуникационной сети обеспечивать передачу данных в форме, предотвращающей их несанкционированный просмотр.

Основными компонентами IPsec являются:

RFC2402 “IP Authentication Header” (AH), предназначенный для контроля целостности и аутентичности пакетов данных в IP-сетях;

RFC2406 “IP Encapsulation Security Payload” (ESP), предназначенный для обеспечения конфиденциальности, контроля целостности и аутентичности пакетов данных в IP-сетях;

RFC2408 “Internet Security Association and Key Management Protocol” (ISAKMP), предназначенный для обеспечения согласования параметров, создания, изменения, уничтожения контекстов защищенных соединений (Security Association, SA) и управления ключами в IP-сетях;

RFC2409 “The Internet Key Exchange” (IKE), являющийся дальнейшим развитием и адаптацией ISAKMP, предназначенный для работы с протоколами IPsec. Ядро IPSec составляют три протокола: протокол аутентификации (Authentication Header, AH), протокол шифрования (Encapsulation Security Payload, ESP) и протокол обмена ключами (Internet Key Exchange, IKE). Функции по поддержанию защищенного канала распределяются между этими протоколами следующим образом:

протокол AH обеспечивает целостность и аутентичность данных;

протокол ESP шифрует передаваемые данные, гарантируя конфиденциальность, но он может также поддерживать аутентификацию и целостность данных;

протокол IKE решает вспомогательную задачу автоматического предоставления секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных. Структурная схема IPSec приведена на рис. 16.9

Рис. 16.9. Структурная схема протокола IPSec

Протокол ESP реализует: шифрование данных IP-пакетов для обеспечения конфиденциальности информации; дополнительно (аналогично протоколу AH) аутентификацию источника каждого пакета, целостность данных каждого пакета, защиту от повторной передачи пакетов. Для обеспечения конфиденциальности данных IP-пакетов предусмотрено использование криптографических алгоритмов шифрования, среди которых

предусмотрены обязательные алгоритмы (для обеспечения совместимости программных продуктов различных производителей), такие, например, как DES-CBC (описанный в стандарте RFC 2405), NULL (описанный в стандарте RFC 2410). Кроме того, предусмотрены некоторые другие (дополнительные) алгоритмы шифрования, например, CAST-128, IDEA, 3DES (описанные в стандарте RFC 2451), а также национальный стандарт шифрования США AES-128, 192, 256 (FIPS-197) и отечественный стандарт ГОСТ-28147-89. Протоколы ESP и AH могут использоваться как в туннельном, так и в транспортном режиме, как самостоятельно, так и в комбинации.

Установление SA начинается с взаимной аутентификации сторон. Выбираемые далее параметры SA определяют, какой из двух протоколов, AH или ESP, применяется для защиты данных, какие функции выполняет протокол защиты: например, только аутентификацию и проверку целостности или, кроме того, еще и защиту от ложного воспроизведения.

Протоколы AH и ESP обеспечивают защиту данных в двух режимах: транспортном и туннельном (см. рис. 16.10, 16.11).

В транспортном режиме (рис. 16.10) передача IP-пакета выполняется с помощью оригинального заголовка этого пакета данных. Достоинством такого режима является существенно меньшие вычислительные и коммуникационные затраты. В тоже время, с точки зрения обеспечения безопасности телекоммуникационной сети, для транспортного режима функционирования протоколов AH и ESP присущи следующие недостатки: протокол ESP в транспортном режиме не защищает заголовок пакта данных; невозможно скрыть топологию сети, поскольку заголовки пакетов данных передаются в открытом (не защищенном) виде.

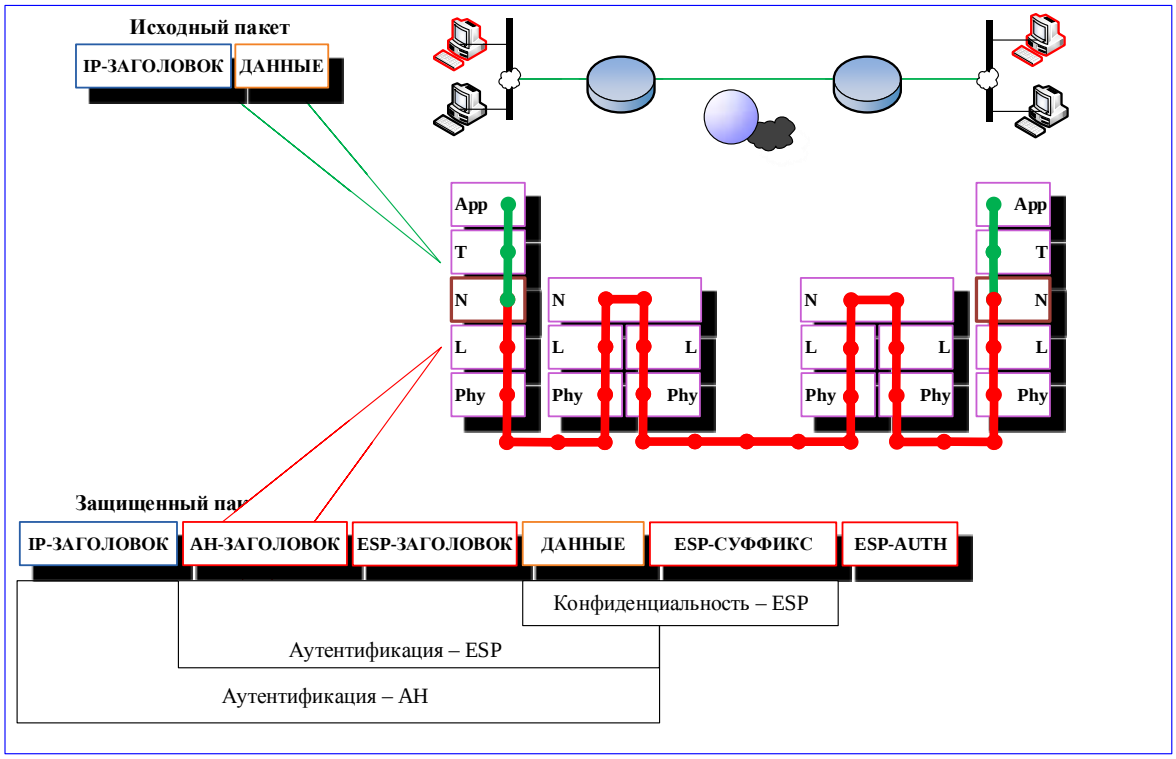

Рис. 16.10. Передача IP-пакета в транспортном режиме

В туннельном режиме (рис. 16.11) исходный IP-пакет помещается в новый, после чего осуществляется передача данных по сети выполняется на основании заголовка нового IP-пакета.

Этот режим обеспечивает защиту заголовка пакета данных, в результате чего скрывается топология сети, что является безусловным преимуществом при построении защищённых телекоммуникационных систем и сетей. В тоже время реализация туннельного режима требует больших вычислительных и коммуникационных ресурсов.

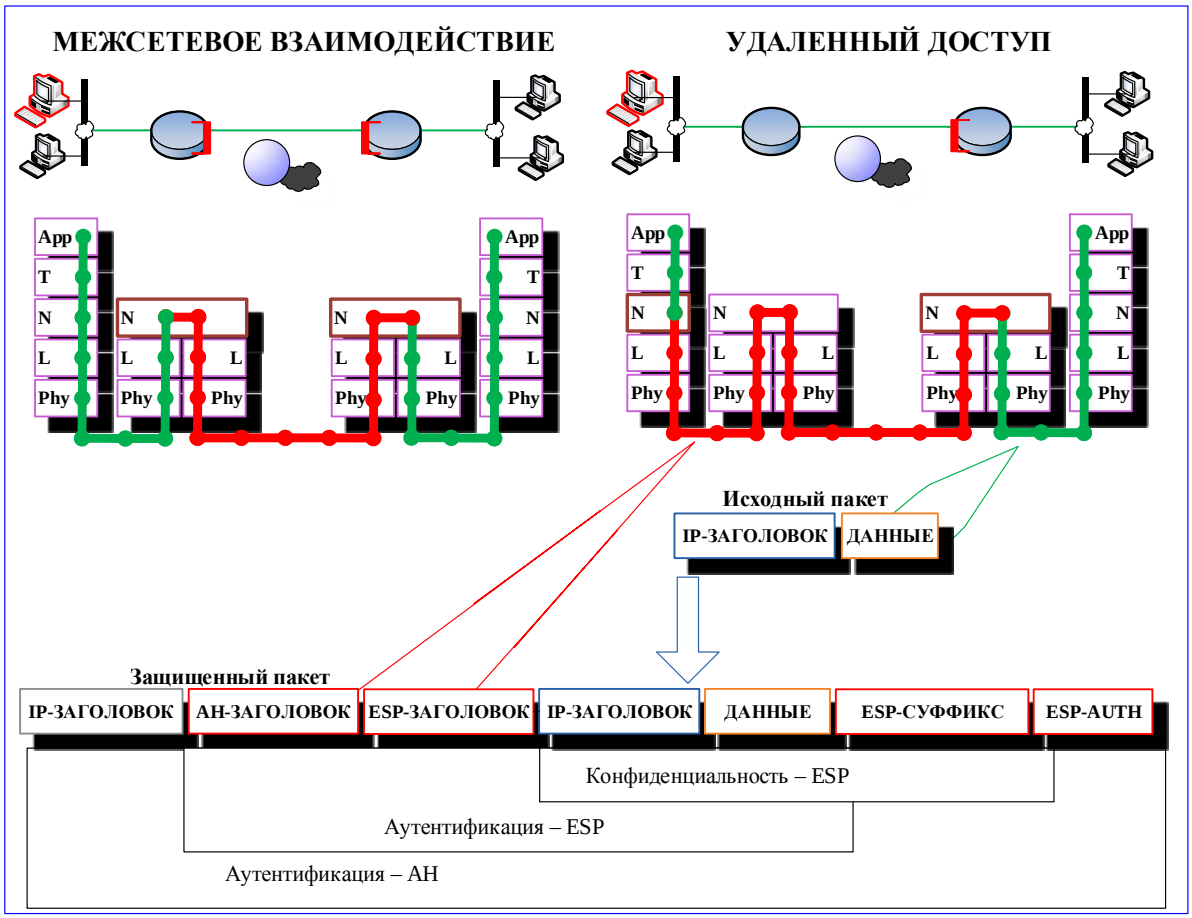

Рис. 16.11. Передача IP-пакета в туннельном режиме

В первой схеме защищенный канал (безопасная ассоциация, SA), устанавливается между двумя конечными узлами телекоммуникационной сети (см. рис. 16.12). Протокол IPSec в этом случае работает на конечном узле и защищает данные, поступающие на него. Для схемы “хост-хост” чаще всего используется транспортный режим защиты, хотя разрешается и туннельный.

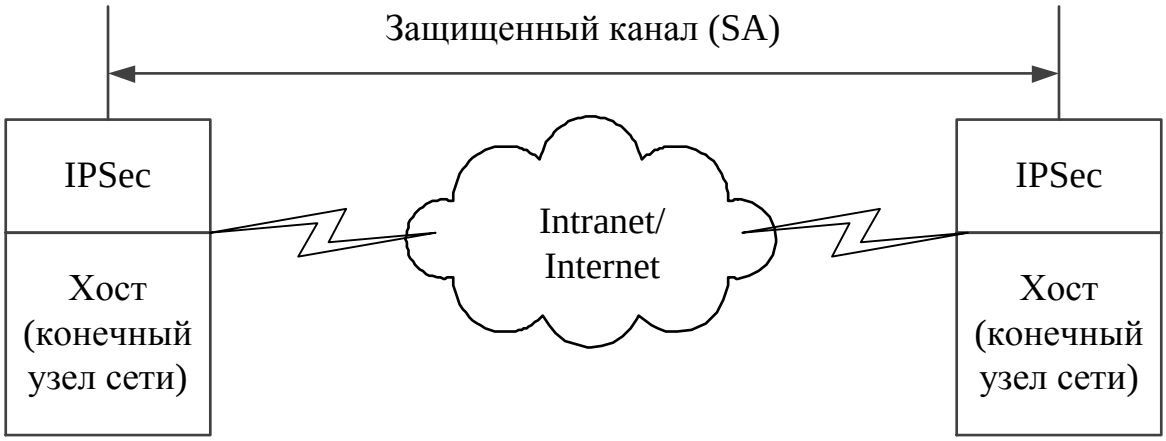

Рис. 16.12. Схема организации защищенного канала “хост-хост”

В соответствии со второй схемой (рис. 16.13), защищенный канал устанавливается между двумя промежуточными узлами, так называемыми шлюзами безопасности (Security Gateway, SG), на каждом из которых работает протокол IPSec. Защищенный обмен данными может происходить между любыми двумя конечными узлами, подключенными к сетям, которые расположены позади шлюзов безопасности. От конечных узлов поддержка протокола IPSec не требуется, они передают свой трафик в незащищенном виде через заслуживающих доверие сети Intranet предприятий. Трафик, направляемый в общедоступную сеть, проходит через шлюз безопасности, который и обеспечивает его защиту с помощью IPSec, действуя от своего имени. Шлюзы могут использовать только туннельный режим работы.

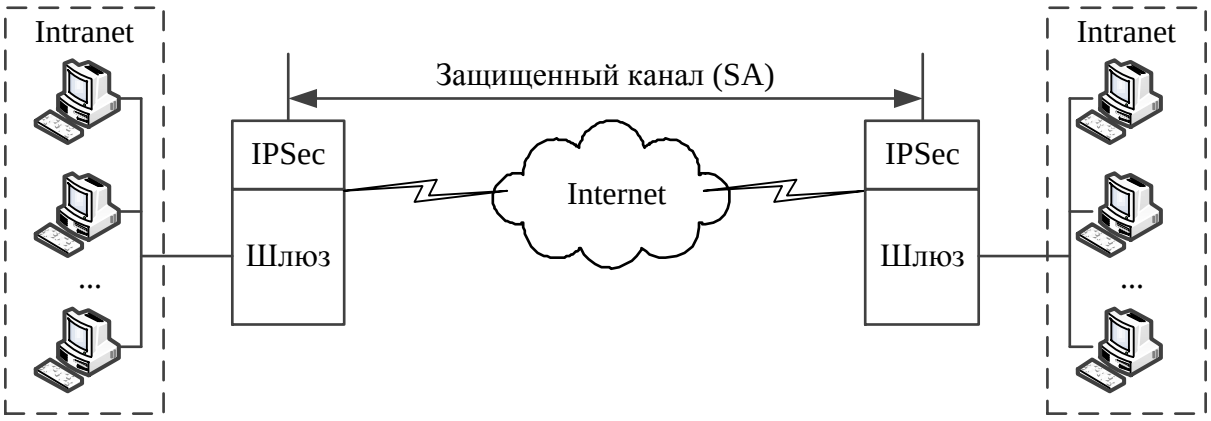

Рис. 16.13. Схема организации защищенного канала “шлюз-шлюз”

Схема “хост-шлюз” (см. рис. 16.14) часто применяется при удаленном доступе. Здесь защищенный канал организуется между удаленным хостом, на котором работает IPSec, и шлюзом, защищающим трафик для всех хостов, входящих в сеть Intranet организации. Эту схему можно усложнить, создав

параллельно еще один защищенный канал – между удаленным хостом и каким-либо хостом, принадлежащим внутренней сети, защищаемой шлюзом. Такое комбинированное использование двух SA позволяет надежно защитить трафик и во внутренней сети.

Для обеспечения конфиденциальности и целостности данных между сервисными протоколами (такими как HTTP, NNTP, FTP и т.д.) и транспортными протоколами (TCP/IP) используются протоколы SSL (Secure Socket Layer) и его новая версия TLS (Transport Layer Security). Часто для него используется аббревиатура HTTPS. Для обеспечения безопасности протокол формирует “безопасный канал” в котором шифруются на основе алгоритмов симметричной криптографии все сообщения, при этом обеспечивается проверка на целостность передаваемых данных на основе MAC-кодов.

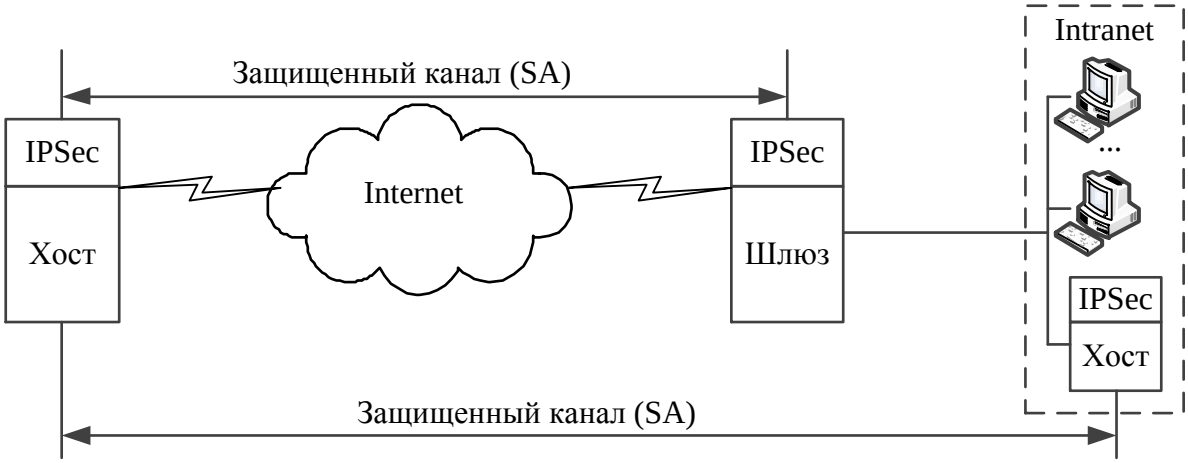

Рис. 16.14. Схема организации защищенного канала “хост-шлюз” с дополнительным каналом “хост-хост”

“Безопасный канал” протокола SSL имеет три основные свойства:

– канал является частным. Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа;

– канал обеспечивает подлинность. Серверная сторона диалога всегда проводит проверку подлинности, в то время как клиентская – осуществляет проверку подлинности опционально;

канал надежный. Транспортировка сообщений включает в себя проверку целостности (с привлечением MAC-кодов). Анализ протокола показал, что SSL можно условно разделить на несколько модулей (подпротоколов) по цели их использования (рис. 16.15):

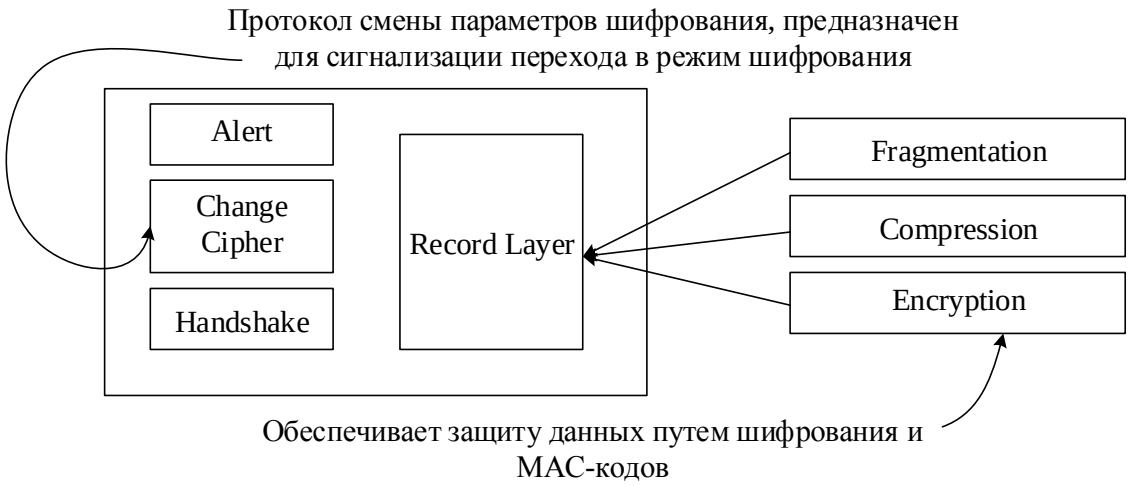

Рис. 16.15. Структура протокола SSL

Протокол SSL работает на двух уровнях: на первом уровне – протокол подтверждения подключения (Handshake Protocol Layer). Он состоит из трех подпротоколов: протокол подтверждения подключения (Handshake Protocol), протокол изменения параметров шифра (Change Cipher Spec Protocol) и предупредительный протокол (Alert protocol), на втором уровне – протокол записи. Структурная схема работы протокола TLS изображена на рис. 16.16.

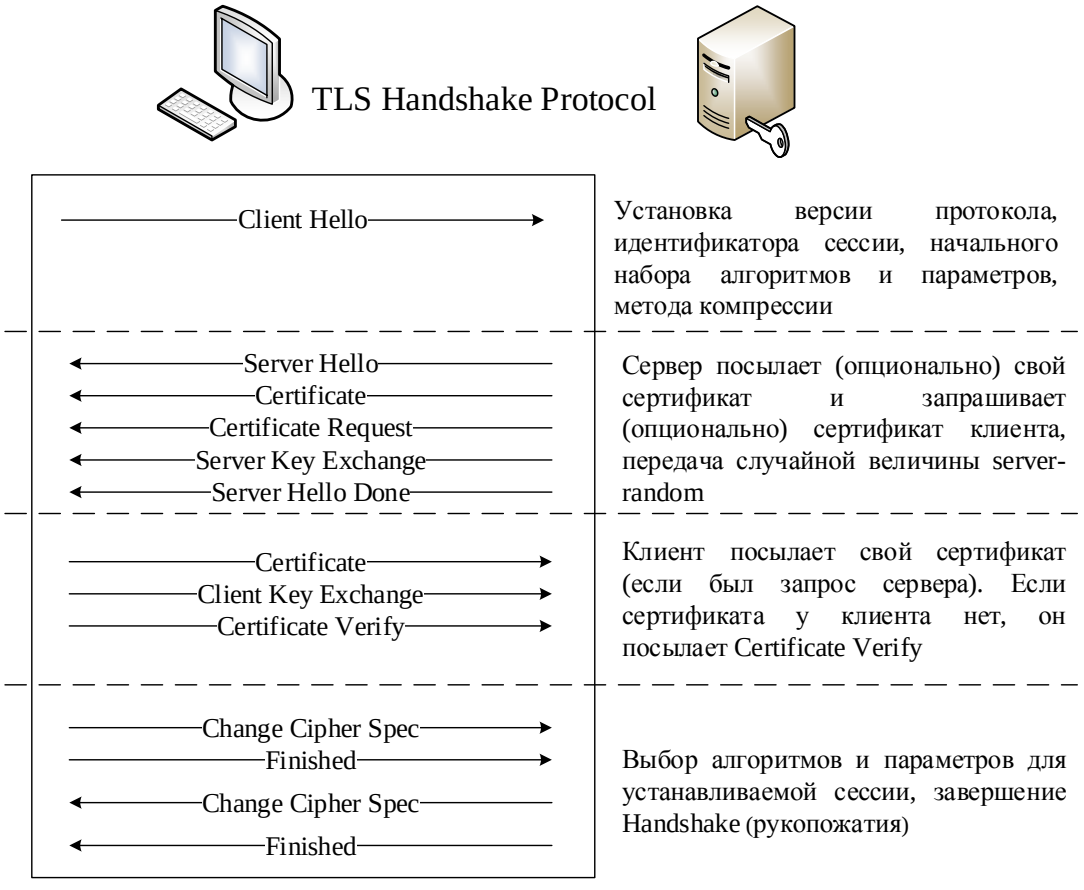

Рис. 16.16. Структурная схема работы протокола TLS

TLS Handshake Protocol обеспечивает инициализацию сессии (соединения) выполнением операций:

– клиент и сервер договариваются об используемых в сессии алгоритмах и параметрах защиты, обмениваются случайными величинами client_random, server_random, договариваются, будут или нет новые соединения;

– производится обмен сертификатами для аутентификации клиента и сервера (по заданным опциям);

– клиент генерирует случайную величину pre_master secret, шифрует ее и передает серверу.

Клиент и сервер по pre_master secret, client_random и server_random формируют master secret (набор необходимой ключевой информации) сессии.

В текущей версии протокола доступны следующие алгоритмы:

для обмена ключами и проверки их подлинности используют комбинации алгоритмов: RSA (асимметричный шифр), Diffie-Hellman (безопасный обмен ключами), DSA (алгоритм цифровой подписи) и алгоритмы технологии Fortezza;

для симметричного шифрования: RC2, RC4, IDEA, DES, Triple DES или AES;

для хеш-функций: MD5 или SHA.

Модульная структура протоколов SSL и TLS позволяет менять алгоритмы шифрования данных.

Проведенный анализ криптоалгоритмов, используемых в протоколе SSL/TLS показал, что вопрос криптоанализа алгоритмов упирается только в мощности системы, используемой для взлома, а при стремительном развитии компьютерных систем это лишь вопрос времени. Чаще всего, клиент ограничен в мощности системы, но никак не злоумышленник.

Проведем анализ протоколов безопасности в перспективных телекоммуникационных системах и сетях (IP-сетях нового поколения (NGN), исследуем особенности их реализации на различных уровнях модели OSI. Поскольку подавляющее большинство территориально распределенных телекоммуникационных систем и сетей, в том числе, специального назначения (например, система управления бурением морских нефтедобывающих сооружений), используют коммуникационные протоколы технологии IP, анализ методов и механизмов обеспечения безопасной передачи данных будем проводить в контексте совершенствования протоколов сетевой безопасности IP-сетей.

Анализ перспективных направлений развития цифровых информационно-телекоммуникационных систем и сетей

Проведенный в работе [**Ошибка! Источник ссылки не найден.**] анализ тенденции в развитии информационно-телекоммуникационных сетей

(ИТКС) показал, что цифровые каналы имеют значительно меньшую вероятность ошибки (10^{-6}) по сравнению с аналоговыми каналами (10^{-4}) и их производительность в 5 – 7 раз выше аналоговых. В конце 90-х годов прошлого столетия международным союзом электросвязи (МСЭ) была предложена концепция мультисервисных сетей следующего поколения NGN (Next Generation Network). Сравнительная характеристика возможностей обеспечения различных информационно-телекоммуникационных услуг цифровыми сетями представлена в табл. 16.3.

Таблица 16.3

Сравнительная характеристика возможностей обеспечения различных

Информационно-телекоммуникационные услуги	Вид информационно-телекоммуникационной сети				
	PDH	IDN	N-ISDN	B-ISDN	NGN
Телефония	+	+	+	+	+
IP-телефония	–	–	–	+ –	+ –
Видеоконференцсвязь, видеонаблюдение	–	–	–	+ –	+ –
Передача служебной информации	–	+	+	+	+
Высокоскоростная передача массивов данных	–	–	–	+ –	+
Краткосрочный обмен данными (БД, дистанционное обучение и т.д.)	–	–	+	+	+
Информационный поиск	–	–	+	+	+

Анализ табл. 16.3 показывает, что для обеспечения возросших потребностей необходим комплексный (интегрированный) подход к обеспечению качества обслуживания и эффективности функционирования ИТКС в соответствии с международными рекомендациями (ITU-T, ETSI, IETF, TL 9000, E.800).

Концепция NGN, в первую очередь, характеризуется четким разделением трех уровней соединения – доступа, транспорта и услуг (рис. 16.17) в соответствии с их функциональными задачами (для маршрутизации, коммутации и передачи данных используется транспортный функциональный уровень, для передачи информации сигнализации – уровень доступа, а за управление логикой услуг и приложений, создание, внедрение и взаимодействие различных услуг отвечает уровень услуг).

Особенностью технологии NGN являются открытые интерфейсы между транспортным уровнем и уровнем управления коммутацией.

Основными используемыми технологиями являются ATM и IP.

Как правило, в основу транспортного уровня мультисервисной сети ложатся существующие сети ATM или IP, т.е. сеть NGN может создаваться как наложенная на существующие транспортные пакетные сети. Сети, базирующиеся на технологии ATM, имеющей встроенные средства

обеспечения качества обслуживания, могут использоваться при создании NGN практически без изменений.

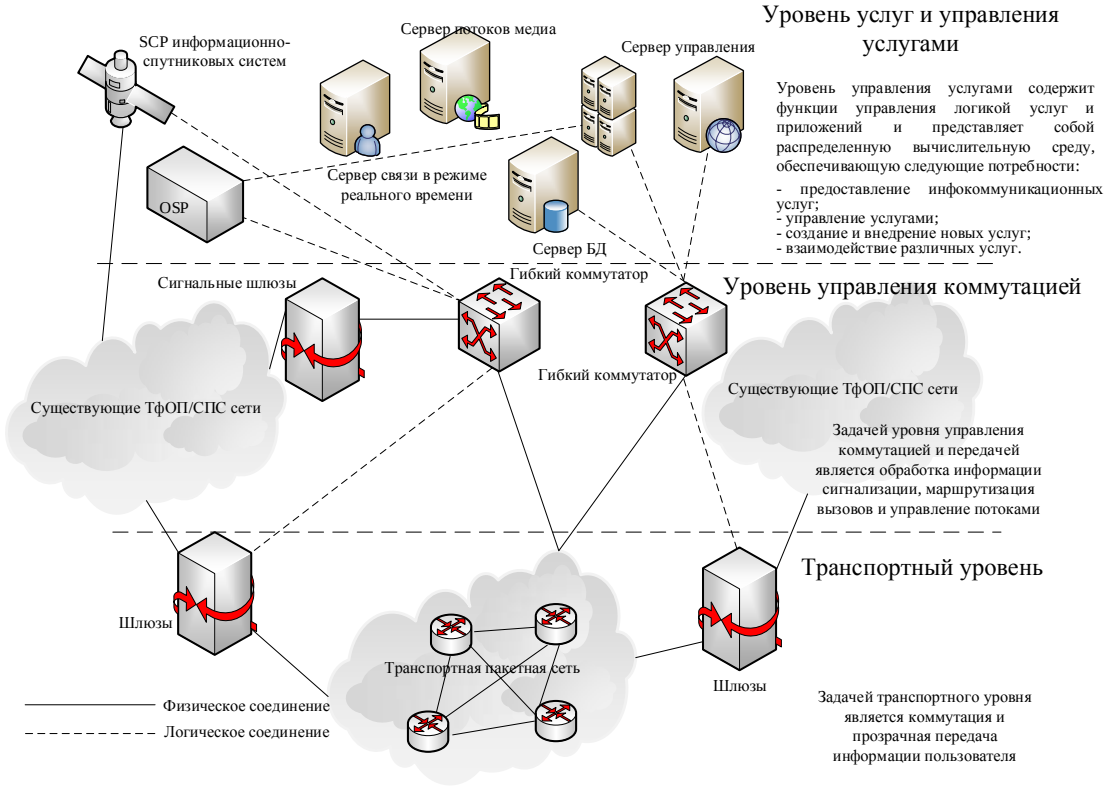

Рис. 16.17. Обобщенная схема построения сети NGN

Использование в качестве транспортного уровня NGN существующих сетей IP потребует реализации в них дополнительной функции обеспечения качества обслуживания, структурная схема сети NGN приведена на рис. 16.18.

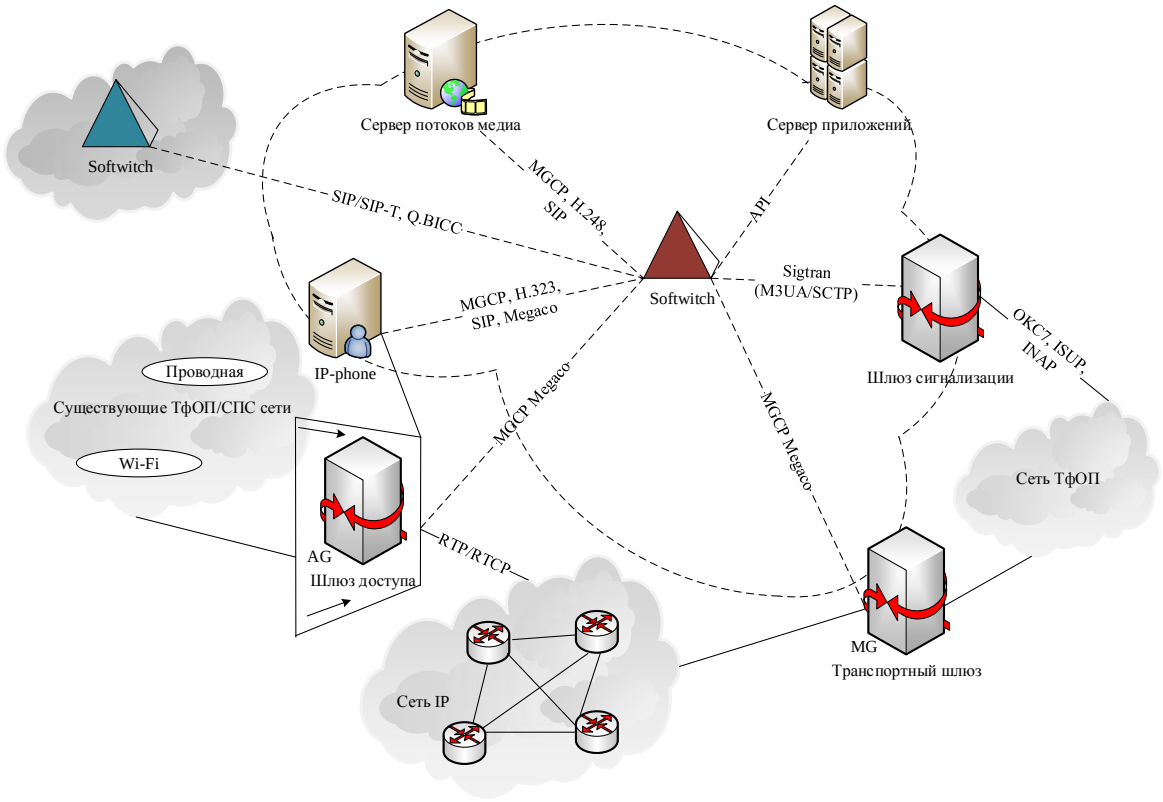

Рис. 16.18. Структурная схема сети NGN

В случае, если на маршрутизаторе/коммутаторе ATM/IP реализуется функция коммутации под внешним управлением, то в них должна быть реализована функция управления со стороны гибкого коммутатора с реализацией протоколов H.248/MGCP (для IP) или BICC (для ATM). Для передачи информации сигнализации сети ТфОП через пакетную сеть используются специальные протоколы. Так, для передачи информации сигнализации ОКС7. поступающей через сигнальные шлюзы от ТфОП к оборудованию гибкого коммутатора, используется протокол MxUA технологии SIGTRAN (в то же время в ряде реализаций гибкого коммутатора предусмотрен непосредственный ввод сигнализации ОКС7).

Проведенный анализ рис. 16.18 показал, что сети следующего поколения имеют две парадигмы построения: с использованием либо программных коммутаторов (Softswitch, оборудование конвергентных сетей) и медиашлюзов (MGW), либо программно-аппаратного комплекса – IMS (IP Multimedia Subsystem) – мультимедийная IP-подсистема). Основная задача Softswitch – согласовывать разные протоколы сигнализации как сетей одного типа, например, при сопряжении сетей H.323 и SIP, так и при взаимодействии сетей коммутации каналов с IP-сетями.

Основная задача IMS передавать сигнальный трафик и трафик в канале через IP-уровень, а также выполнять функции маршрутизатора или механизма управления сессиями абонентов с использованием информации об их состоянии.

Базовыми элементами опорной сети архитектуры IMS являются:

– CSCF (Call Session Control Function) – элемент с функциями управления сеансами и маршрутизацией, состоит из трех функциональных блоков:

– P-CSCF (Proxy CSCF) – посредник для взаимодействия с абонентскими терминалами. Основные задачи – аутентификация абонента и формирование учётной записи;

– I-CSCF (Interrogating CSCF) – посредник для взаимодействия с внешними сетями. Основные задачи – определение привилегий внешнего абонента по доступу к услугам, выбор соответствующего сервера приложений и обеспечение доступа к нему;

– S-CSCF (Serving CSCF) – центральный узел сети IMS, обрабатывает все SIP-сообщения, которыми обмениваются оконечные устройства.

– HSS (Home Subscriber Server) – сервер домашних абонентов, является базой пользовательских данных и обеспечивает доступ к индивидуальным данным пользователя, связанными с услугами. В случае если в сети IMS используется несколько серверов HSS, необходимо добавление SLF (Subscriber Locator Function) который занимается поиском HSS с данными конкретного пользователя.

– BGCF – элемент управляющий пересылкой вызовов между доменом коммутации каналов и сетью IMS. Осуществляет маршрутизацию на основе телефонных номеров и выбирает шлюз в домене коммутации каналов, через который сеть IMS будет взаимодействовать с ТфОП или GSM.

– MGCF – управляет транспортными шлюзами.

– MRFC – управляет процессором мультимедиа ресурсов, обеспечивая реализацию таких услуг, как конференцсвязь, оповещение, перекодирование передаваемого сигнала.

Протоколы, используемые в сетях NGN, можно разделить на несколько классов (рис. 16.19) [**Ошибка! Источник ссылки не найден.**]:

– протоколы передачи пользовательской (мультимедийной) информации – пакетные протоколы стека TCP/IP;

– протоколы сигнализации, используемые для управления и взаимодействия различных узлов сети NGN в процессе обслуживания вызовов;

– служебные протоколы, используемые для различных вспомогательных целей (аутентификации и авторизации пользователей, технического обслуживания и др.).

Проведенный анализ протоколов сети NGN показал, что для обеспечения достоверности и безопасности данных будут использоваться процедуры протоколов IP-сетей. Для обеспечения безопасности в перспективных сетях предлагается использовать комплексный подходов к решению задач обеспечения информационной безопасности, в основе которого лежит

необходимость согласования методов обеспечения информационной безопасности для разных компонентов сети NGN, включая данные, услуги и телекоммуникационные протоколы [**Ошибка! Источник ссылки не найден.**]. Специалисты компании Cisco рассматривают безопасность как основной опорный элемент архитектуры IP NGN и одно из наиболее важных требований для надежного предоставления сервисов и обеспечения непрерывности деловой активности.

В маршрутизаторах и коммутаторах Cisco предусмотрены встроенные средства обеспечения безопасности, позволяющие защитить и обеспечить надежное функционирование сети провайдера услуг на сетевом уровне. Эти средства – Cisco NetFlow и система обеспечения безопасности сети Cisco Network Foundation Protection – работают совместно с целью нейтрализации самых распространенных угроз, отражения распространенных атак и обеспечения основных функций безопасности (рис. 16.20).

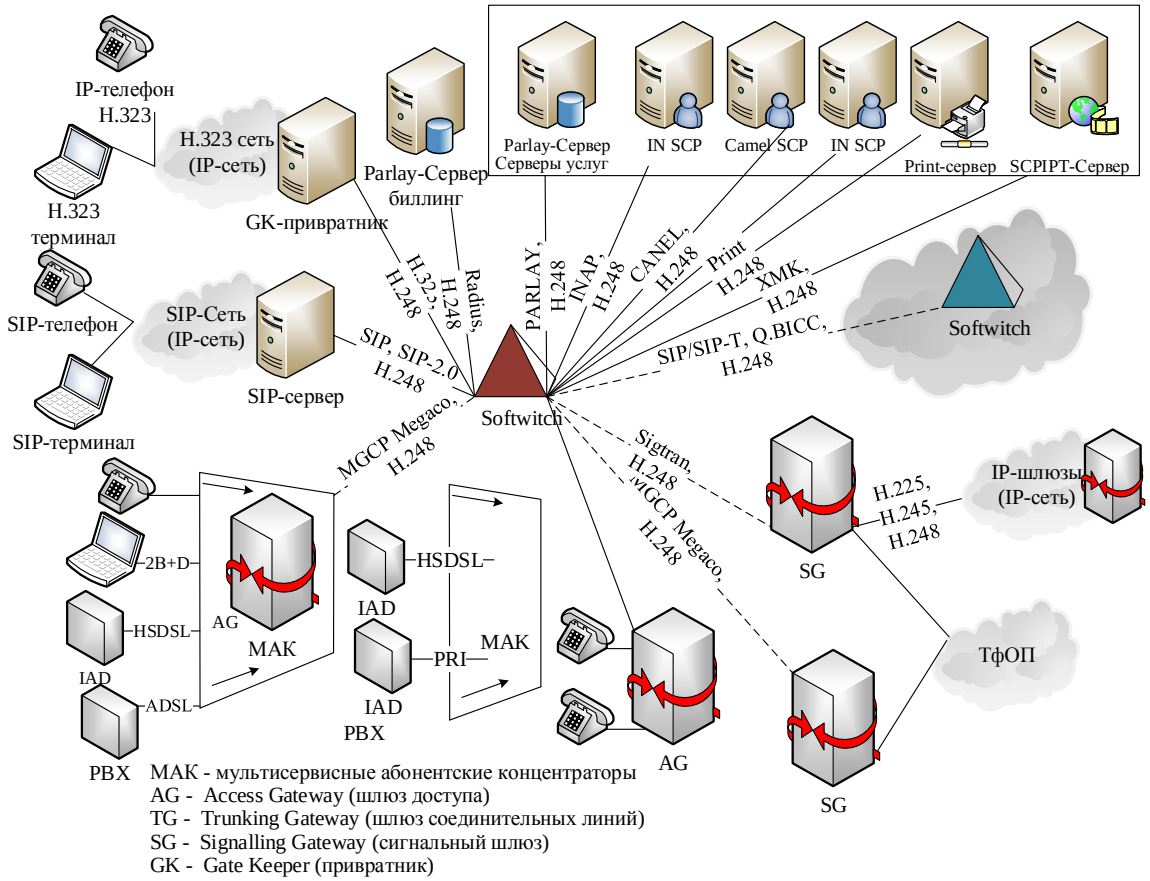

Рис. 16.19. Основные протоколы, используемые в сетях NGN

Рис. 16.20.Принципы работы Cisco NetFlow

Система Cisco Network Foundation Protection (NFP) входящая в состав программного обеспечения Cisco IOS, обеспечивает защиту сетевых устройств, механизмов маршрутизации и передачи управляющей информации, а также управление трафиком, поступающим на сетевые устройства.

Таким образом, проведенный анализ протоколов IP-сетей и перспективных сетей IP-сетей нового поколения NGN для обеспечения достоверности и безопасности при передачи данных, позволяет сделать следующие выводы:

IP-сети и сети нового поколения NGN являются открытыми системами и для обеспечения достоверности в них, как правило, используются протоколы HDLC, обеспечивающие повторную передачу пакетов (кадров) с ошибками, либо помехоустойчивые коды для прямого исправления ошибок.

протоколы сетевой безопасности IPSec, функционирующие на сетевом уровне, с одной стороны “прозрачны” для приложений, а с другой – могут работать практически во всех сетях, так как основаны на широко распространенном протоколе IP. Протоколы IPSec доминируют на сегодняшний день в большинстве реализаций WAN-сетей и реализовываются как программном виде (например, протоколы реализованы в операционной системе Windows компании Microsoft), так и в виде программно-аппаратных реализаций (решения Cisco, Nokia). Несмотря на большое число различных решений, все реализации обладают высокой совместимостью друг с другом [**Ошибка! Источник ссылки не найден.**];

для обеспечения безопасности используются криптографические процедуры протоколов IPSec, либо протоколов транспортного уровня SSL (TLS). По мнению специалистов Cisco для обеспечения информационной безопасности при работе в сетевой среде, в которой присутствуют разноплановые и смешанные угрозы безопасности, необходимо использовать комплексный подход для согласования методов обеспечения информационной безопасности для разных компонентов сети NGN, включая данные, услуги и телекоммуникационные протоколы. Однако применение криптографических средств защиты данных могут приводить к снижению уровня оперативности, что снижает обобщенный показатель качества обслуживания.

Выводы

1. Проведенный анализ и исследования показали, что современные телекоммуникационные системы и сети, используя последние достижения в развитии электронных коммуникаций и IT-технологий, постоянно расширяют спектр предоставляемых услуг, в том числе по обслуживанию субъектов автоматизированного информационного взаимодействия, обеспечению доступа к различным мультимедийным сервисам и технологиям, поддержке удаленных пользователей и т.д. В тоже время быстрый рост объемов, обрабатываемых данных приводит к ужесточению вероятностно-временных требований, предъявляемых к основным компонентам телекоммуникационных систем и сетей на всех этапах информационного обмена данными.

2. Появление новых форм и способов предоставления коммуникационных услуг, стремительное развитие вычислительной техники выдвигают новые требования к надежности (достоверности) и обеспечению безопасности телекоммуникационных сетей. Особенно остро эти вопросы стоят в телекоммуникационных сетях специального назначения, в которых отказ в обслуживании или выход конкретных параметров качества за установленные пределы может привести к катастрофическим последствиям в финансовом секторе, промышленности, энергетическом комплексе и пр. В качестве примера такой системы можно привести систему управления бурением морских нефтедобывающих сооружений, представляющую собой большую территориально распределенную мультисервисную телекоммуникационную систему специального назначения, использующую высокопроизводительные вычислительные комплексы и сложные механизмы комплексной защиты информационных технологий.

3. Проведенный анализ показал, что подавляющее большинство нарушений безопасности (65% и более) относятся к нарушению конфиденциальности, целостности и аутентичности данных. Лидирующую позицию по реализации угроз сетевой безопасности занимают нарушения, приводящие как к утечке закрытой информации, так и к навязыванию ложной

информации или неправильной работе компонентов телекоммуникационной системы.

4. Таким образом, наибольшую опасность информационным ресурсам в современных телекоммуникационных системах и сетях представляют угрозы несанкционированного доступа к ресурсам сети. Это обусловлено тем, что нарушение подлинности обрабатываемых и передаваемых данных, неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи наносят существенный материальный и моральный ущерб различным субъектам (государству, юридическим и физическим лицам), участвующим в процессах информационного взаимодействия.

5. Возникает противоречие между резко возросшими вероятностно-временными требованиями к перспективным механизмам достоверности и безопасности информации в условиях непрерывного совершенствования угроз информационной безопасности и реальным состоянием существующих моделей, методов и вычислительных алгоритмов, применяемых в протоколах сетевой безопасности, используемого научно-методического аппарата для построения эффективных механизмов противодействию угроз безопасности телекоммуникационных систем и сетей.