УДК 621.391

Х.Н. Рзаев[1], Ф.Г. Самедов[2], З.Б. Иманова[1], Ж.С. Джамалова [1]

[1] *Азербайджанский Государственный Университет Нефти и Промышленности, Баку*
[2] *Азербайджанский Технический Университет, Баку*

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В СИСТЕМЕ УПРАВЛЕНИЯ БУРЕНИЕМ МОРСКИХ НЕФТЕГАЗОДОБЫВАЮЩИХ СООРУЖЕНИЙ

Рассматривается система управления бурением морских нефтедобывающих сооружений, проводится анализ основных требований к качеству обслуживания на основе протоколов, обеспечивающих обмен данными в сети управления бурением, анализируются угрозы информационной безопасности циркулирующих потоков данных. Рассматриваются основные протоколы обеспечения достоверности безопасности в перспективных системах предоставления услуг связи сети NGN.

Ключевые слова: *информационно-телекоммуникационная система, безопасность, достоверность, морские нефтегазовые сооружения.*

Введение

Морские нефтегазовые сооружения является опасными производственными объектами и характеризуются высокой аварийностью. По данным [1 – 4] на континентальном шельфе за период с 1990 по 2013 только на стационарных платформах произошло 63938 несчастных случаев. В США [6] 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 [7], 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 [5]. По оценкам зарубежных специалистов [6] 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” [6]. 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 [7].

В настоящее время возрастают требования охраны окружающей среды к производствам нефтегазовой отрасли, так как они представляют повышенную опасность природе и человеку. Для достижения соответствия современным нормам экологической безопасности проводится постоянная модернизация и внедрение современных технологий [8]. Таким образом, актуальной проблемой нефтегазовой отрасли является обеспечение безопасности и надежности систем управления бурения, многопотоковых каналов передачи данных для систем экологического мониторинга.

Целью статьи является анализ перспективных систем управления бурением морских нефтедобывающих сооружений, основных требований к качеству обслуживания на основе протоколов, обеспечивающих обмен данными в сети управления бурени-

ем, угроз информационной безопасности циркулирующих потоков данных, рассмотрение основных протоколов обеспечения достоверности и безопасности в перспективных системах предоставления услуг связи сети NGN.

Изложение основного материала

1. Анализ основных систем управления бурением морских нефтедобывающих сооружений.

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 [8]. 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. 1 приведена структурная схема СКАДА СОПТ WaveControl [8].

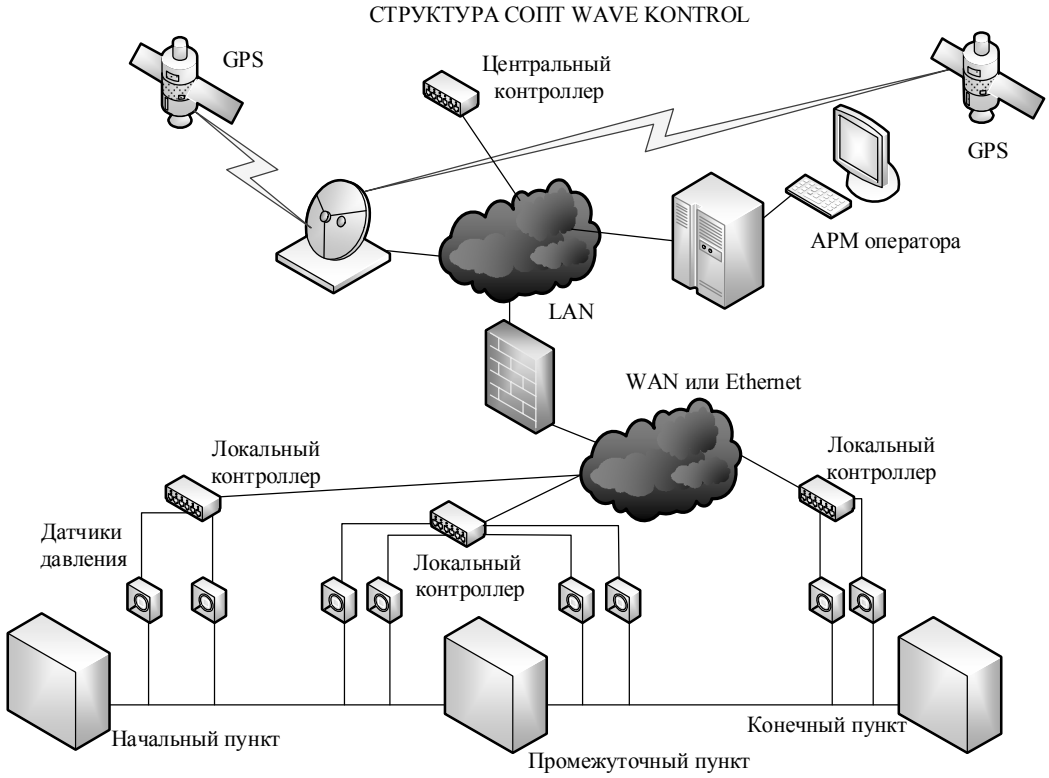

Рис. 1. Структурная схема СКАДА СОПТ WaveControl

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. 2.

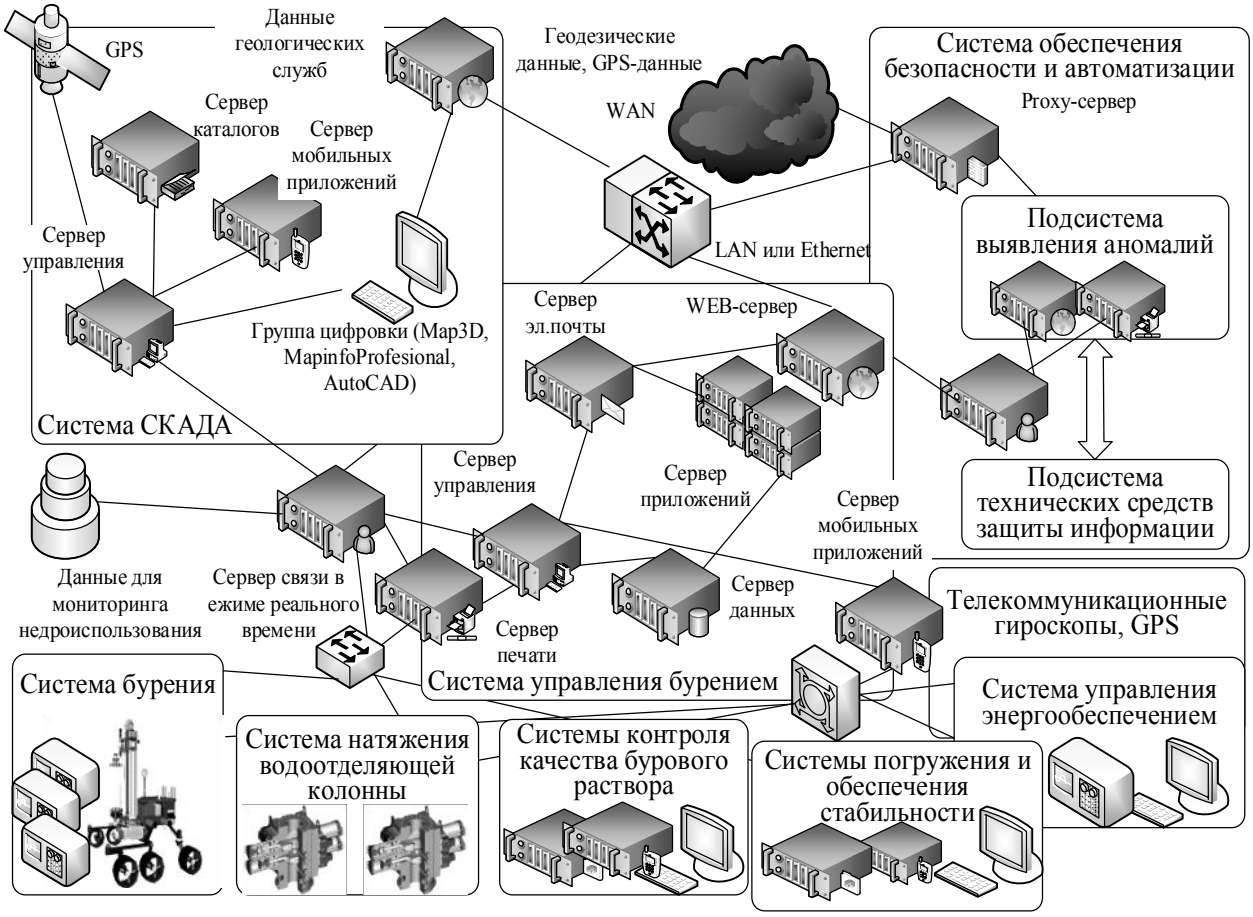

Рис. 2. Структурная схема сети управления бурением

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.

Таким образом, 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.

2. Анализ основных требований, предъявляемых к современным телекоммуникационным системам и сетям.

Среди стандартов, посвященных качеству обслуживания в электросвязи, одно из центральных мест занимает Рекомендация МСЭ Е.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 Е.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 струк-

туру 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 [12].

На основании проведенного анализа в работе [11] в табл. 1 представлены основные критерии и показатели качества передачи информации в телекоммуникационных IP сетях, в соответствии с функциями, реализуемыми операторами информационно-телекоммуникационных услуг [10, 11].

Таблица 1

Требования и показатели качества функционирования информационных систем

Показатель	Определение, раскрывающее смысл наименования	Показатели качества обслуживания
Достоверность информации		
Безошибочность информации	Свойство информации не иметь явных или скрытых ошибок и/или искажений	$P_{иск} \le 10^{-5} - 10^{-7}$ – 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	$P_{хран.} \le 0,95$ – при угрозах проникновения в систему случайных источников опасности; $P_{хран.} \le 0,9$ – 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	$T_{авт.вв} \le 10$ 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 $P_{пп} \ge 0,95$ $T_{отобр} \le 10$ с – время представления на экран монитора поступивших в ИС команд, приказов и срочных сигналов с $P_{пп} \ge 0,9$
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	$T_{без} \ge 200$ лет
Целостность информации	Состояние информации, при котором обеспечивается достижение целей её функционального применения в системе.	$T_{без.} \ge 200$ лет ,с $P_{мод} \ge 0,9$
Доступность информации	Состояние информации, её носителей и технологий обработки, при котором обеспечивается санкционированный доступ к ней и надёжность представления требуемой информации	$T_{без.} \ge 30$ лет , с $P_{НСД} \ge 0,9$
Актуальность безошибочной информации	Свойство безошибочной информации 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	$T_{стар} \le 2,5$ 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	$T_{вв} \le 40$ с в БД другой оперативной исходной информации от источников с $P_{пп} \ge 0,8$; $T_{вв} \le 180$ с $P_{пп} \ge 0,8$.

Окончание табл. 1

Показатель	Определение, раскрывающее смысл наименования	Показатели качества обслуживания
Оперативность информации		
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. 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. 2.

Проведенный анализ [13] 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 [14] 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.

Таким образом, сеть системы управления бурением морских нефтегазодобывающих сооружений может быть подвержена атакам на основании угроз локальных и глобальных вычислительных систем.

Таблица 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.		

3. Анализ угроз безопасности информации в современных телекоммуникационных системах и сетях. 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. 1, 2):

– 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.

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 [14]. 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. 3.

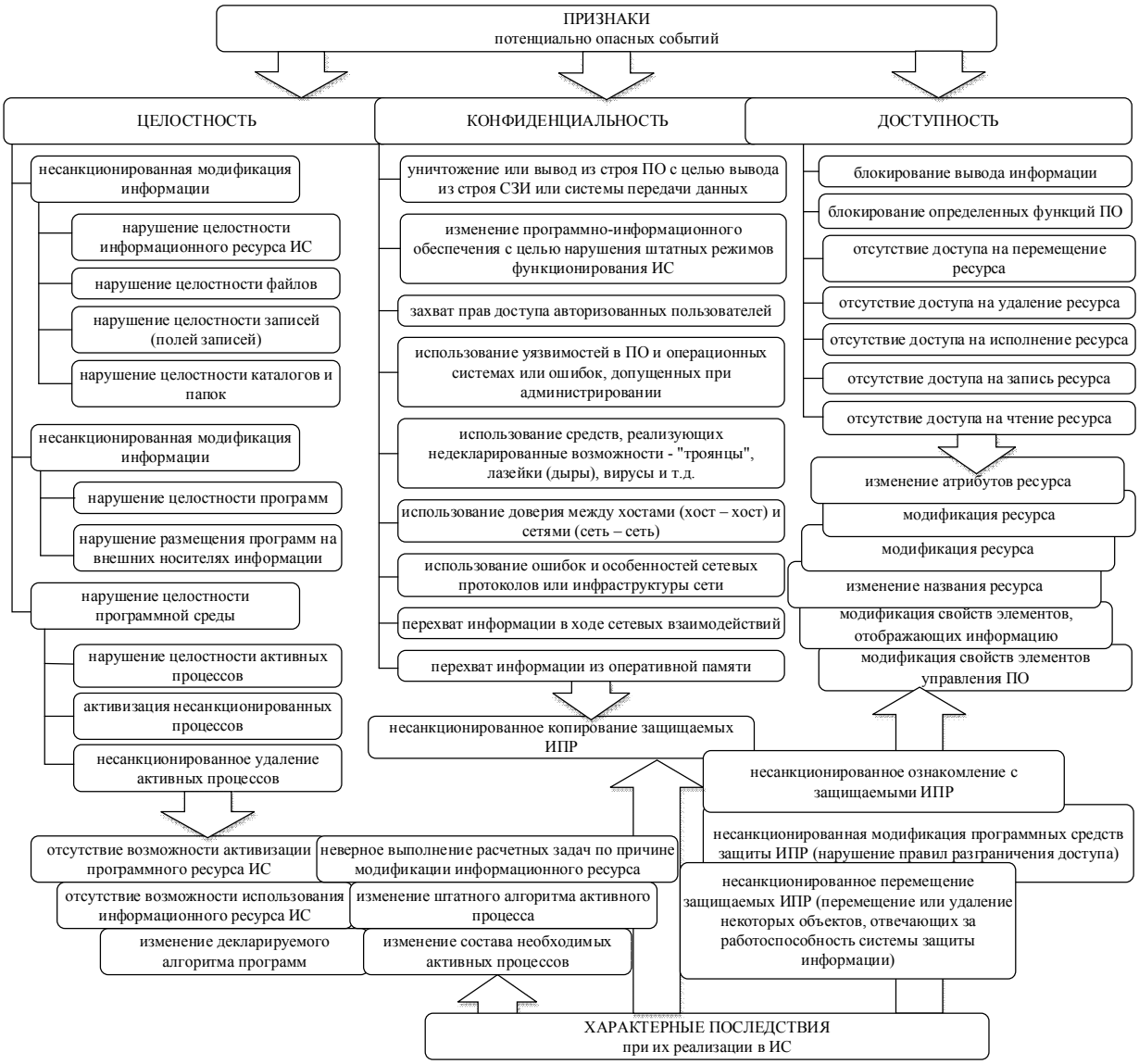

Рис. 3. Классификационные ПОС при функционировании ПО и характерные последствия при их реализации в ИС

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.

Опыт эксплуатации показывает, что около 80% попыток НСД к конкретной ИС осуществляют лица, работающие или работавшие с данной системой. Поэтому будем считать, что потенциальный нарушитель имеет достаточно высокую квалификацию и ему известны принципы функционирования ИС [15, 16].

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 [17].

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.

4. Анализ протоколов обеспечения достоверности и безопасности данных в современных телекоммуникационных системах. 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.

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 [10]:

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.

На прикладном уровне модели ISO/OSI используются программные средства защиты и выявления аномалий: брандмауэры, firewall-ы, антивирусные программы, NAT-ы, алгоритмы шифрования полей БД.

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. 3.

Таблица 3

Основные протоколы обеспечения достоверности и безопасности в IP-сетях

Приложение	Протоколы обеспечения достоверности	Протоколы обеспечения безопасности
Факсимильная связь	T.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. 3 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 [14]. С одной стороны, они прозрачны для приложений, а с другой – могут работать практически во всех сетях, так как основаны на широко распространенном протоколе IP [14]. 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 [19]. Основное назначение протоколов IPSec – обеспечение безопасной передачи данных по IP-сетям.

Их применение обеспечивает [19]: 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. 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.

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

5. Анализ перспективных направлений развития цифровых информационно-телекоммуникационных систем и сетей. Проведенный в работе [5] 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 ИТК услуг цифровыми сетями представлена в табл. 4.

Таблица 4

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. 4 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. 4) 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).

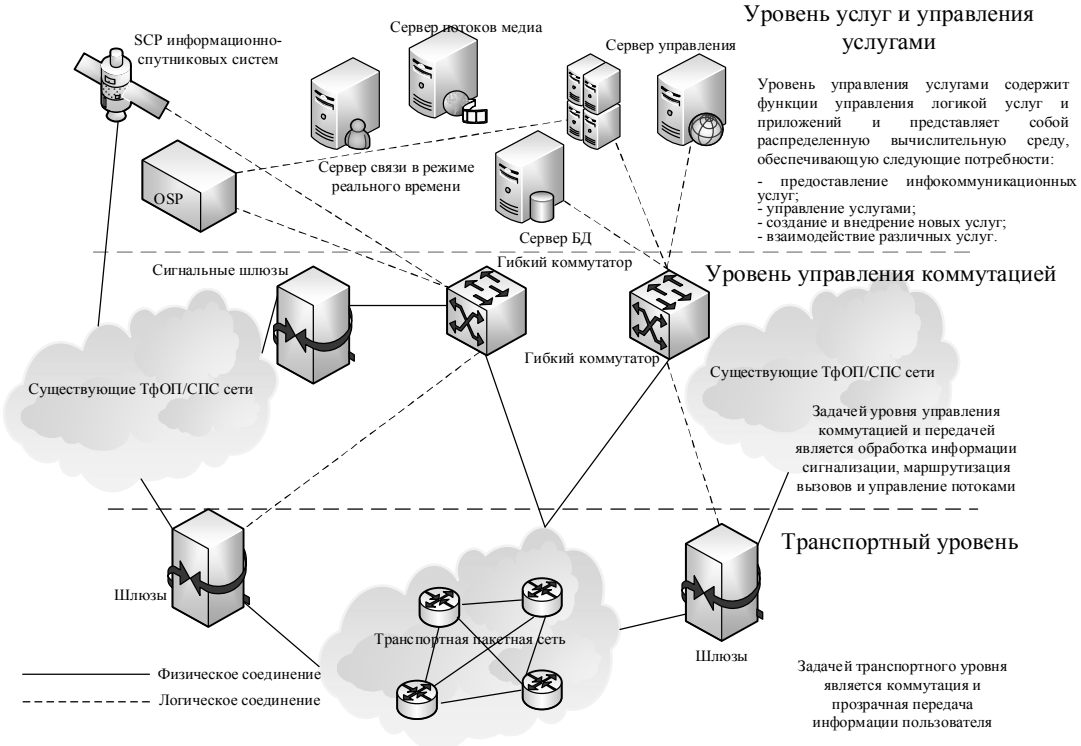

Рис. 4. Обобщенная схема построения сети NGN

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. Использование в качестве транспортного уровня NGN существующих сетей IP потребует реализации в них дополнительной функции обеспечения качества обслуживания, струк-

турная схема сети NGN приведена на рис. 5. 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. 5 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:

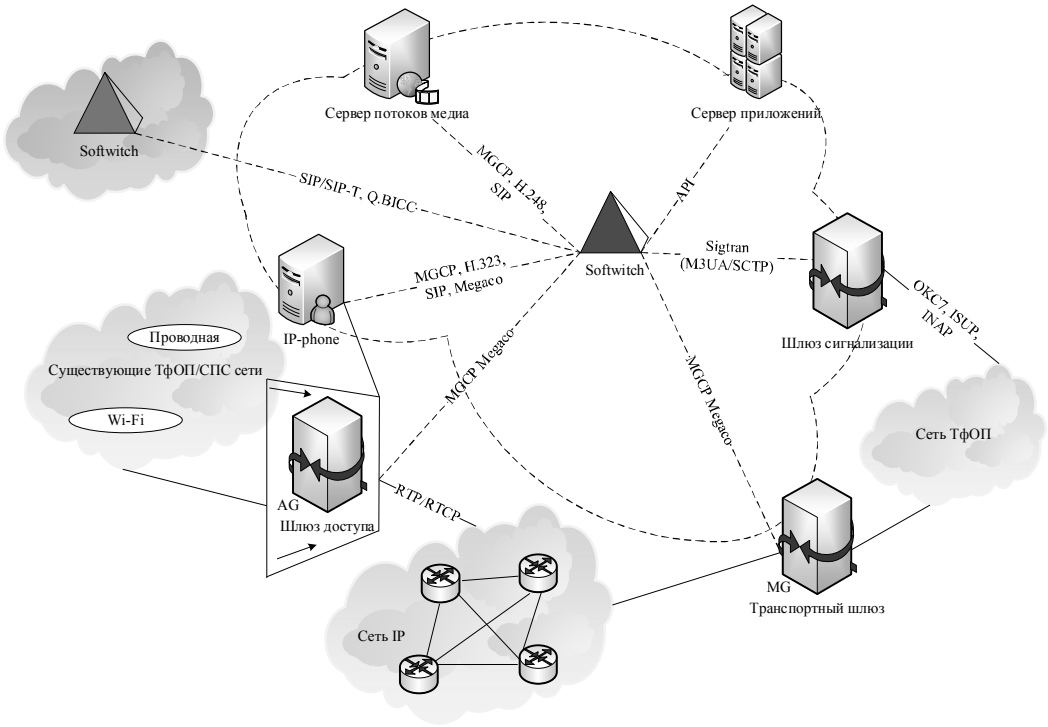

Рис. 5. Структурная схема сети NGN

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

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

o 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;

o 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.

6. Основные протоколы обеспечения достоверности и безопасности в сетях NGN. Протоколы, используемые в сетях NGN, можно разделить на несколько классов (рис. 6):

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 [18].

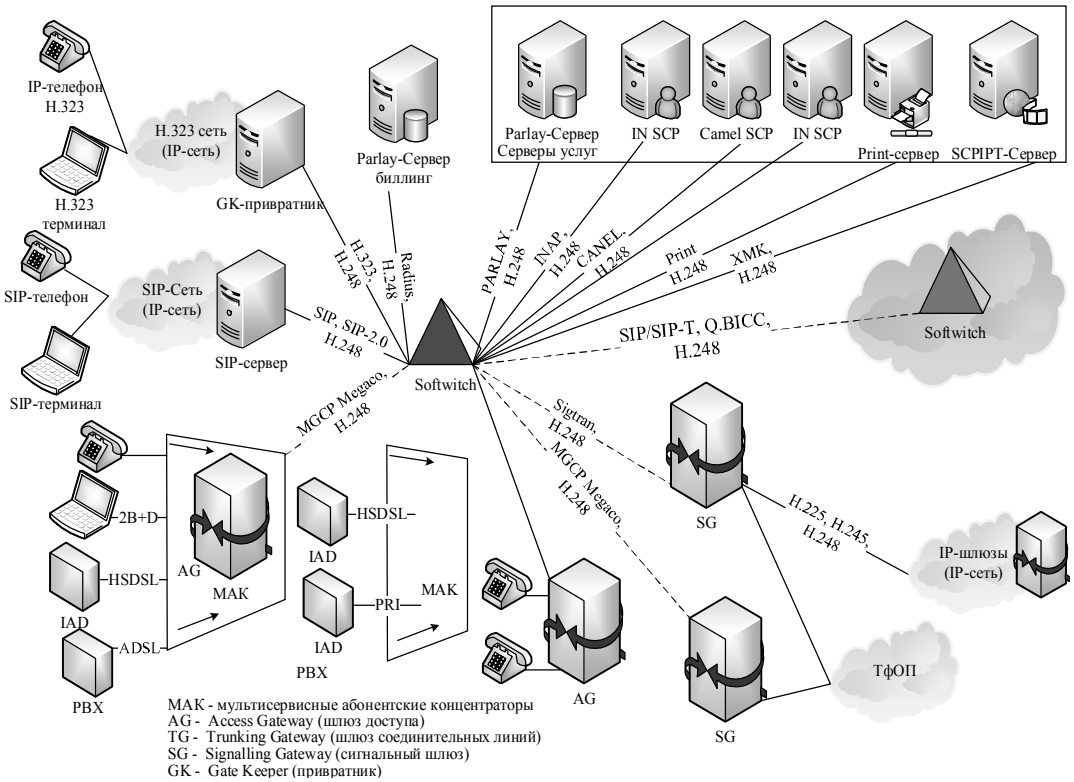

Рис. 6. Основные протоколы, используемые в сетях NGN

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 [17].

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. 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 [17].

Выводы

Проведенный анализ сети системы бурения морских нефтедобывающих сооружений показал, что она относится к многоуровневым системам критического управления. Для ее построения используются протоколы и программно-аппаратные средства, используемые в глобальных сетях Ethernet, основанные на протоколах IP-сетей. Исследования IP-сетей и перспективных сетей IP-сетей нового поколения NGN, показали, что они являются открытыми системами и для обеспечения достоверности, как правило, используются протоколы HDLC, обес-

печивающие повторную передачу пакетов (кадров) с ошибками. Для обеспечения безопасности используются криптографические процедуры протоколов IPSec, либо протоколов транспортного уровня SSL (TLS). Однако применение криптографических средств защиты данных могут приводить к снижению уровня оперативности, что снижает обобщенный показатель качества обслуживания.

Таким образом, перспективным направлением дальнейших исследований является разработка интегрированных механизмов, одновременно обеспечивающих требуемые показатели достоверности и безопасности данных в системах управления бурением морских нефтегазодобывающих сооружений.

Список литературы

1. Рзаев Х.Н. Комплексна система контролю морських нафтогазовидобувних споруд / Х.Н. Рзаев // Системи обробки інформації. – Х.: ХУ ПС, 2015. – Вип. 4(129). – С. 59-63.

2. Рзаев Х.Н. Обоснование эффективности морской добычи жидких углеводов / Х.Н. Рзаев // Известия высших техн. учебн. завед. Азербайджана. – 2015. – № 3. – С. 21-30.

3. Рзаев Х.Н. Отечественный опыт развития конструктивных форм морских стационарных платформ / Х.Н. Рзаев // Системи обробки інформації. – Х.: ХУ ПС, 2015. – Вип. 11(136). – С. 59-62.

4. Рзаев Х.Н. Зарубежный опыт строительства морских стационарных платформ / Х.Н. Рзаев // Azərbaycan mühəndislik akademiyasinin xəbərləri. – 2015. – № 7,3. – С. 104-111.

5. Дашевская О.В. Нефтяные кризисы в мировой экономике / О.В. Дашевская, Т.Р. Бабалов // Вісник Східноєвропейського університету економіки і менеджменту. – 2012. – 3 (13). – С. 40-47.

6. Бялый Ю. Мировая энергетика и перспективы "энергетических" войн [Электронный ресурс]: – Режим доступа к ресурсу: http://www.kurginyan.ru/ clubs.shtml?cat=53&id=318.

7. Айдын Гаджиев Современные тенденции мировой нефтяной политики и Азербайджан [Электронный ресурс]: – Режим доступа к ресурсу: http://ru.sputnik.az/ expert/20080522/42310117.html.

8. Джамбеков А.М. Перспективы использования космических систем экологического мониторинга в нефтегазовой отрасли на примере предприятия ГПЗ ООО «Газпром добыча Астрахань» / А.М. Джамбеков, А.А. Марков // Современные наукоемкие технологии. – 2013. – № 8-2. – С. 327-329.

9. Семенов С.Г. Модели и методы управления сетевыми ресурсами в информационно-телекоммуникационных системах: монография / С.Г. Семенов, А.А. Смирнов, Е.В. Мелешко. – Х.: НТУ "ХПИ", 2011. – 212 с.

10. Стандарт ГОСТ РВ 51987 «Информационная технология, комплекс стандартов на АС. Требования и показатели качества функционирования информационных систем» [Электронный ресурс]: – Режим доступа к ресурсу: http://gearletitbit.weebly.com/blog/gost-rv-51987-2002.

11. Бойко А.А. Система показателей качества баз данных автоматизированных систем / А.А. Бойко, С.А. Гриценко, В.Ю. Храмов // Вестник ВГУ, серия: Системный анализ и информационные технологии. – 2010. – № 1. – С. 39-45.

12. Яновский Г.Г. Качество обслуживания в сетях IP / Г.Г. Яновский // Журнал «Вестник связи». – 2008. – №1. – С. 1-16.

13. Телекоммуникационные услуги в мировой экономике [Электронный ресурс]: – Режим доступа к ресурсу: http:// www.gumer.info/bibliotek_Buks/Econom/world_econom/30.php.

14. Король О.Г. Протоколы безопасности телекоммуникационных сетей / О. Г. Король // Системи обробки інформації. – Х.: ХУ ПС, 2012. – Вип. 6 (104). – С. 113-120.

15. Жидков И.В. О признаках потенциально опасных событий в информационных системах [Электронный ресурс] / И.В. Жидков, И.В. Кадушкин. – Режим доступа к ресурсу: http://cyberleninka.ru/article/n/o-priznakah-potentsialno-opasnyh-sobytiy-v-informatsionnyh-sistemah.

16. Прохоров С.А. Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения [Электронный ресурс] / С.А. Прохоров, А.А. Федосеев, В.Ф. Денисов, А.В. Иващенко. – Режим доступа: http://www.ssau.ru/files/resources/ sotrudniki/13_isokbp.pdf.

17. Безопасность IP-сетей нового поколения для провайдеров услуг [Электронный ресурс]: – Режим доступа к ресурсу: http://www.eureca.ru/edu/study/cisco/ library/download.php?type=pdf&att=IP_NGN.pd.

18. Защита в сетях NGN. [Электронный ресурс]: – Режим доступа к ресурсу: https://www.google.ru/ url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjavtXptJDKAhUGl3IKHZf7CG8QFggbMAA&url=http%3A%2F%2Fwww.eureca.ru.

19. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс. – М.: Издательский дом «Вильямс», 2001. – 672 с.

Поступила в редколлегию 22 03.2016

Рецензент: д-р техн. наук, проф., чл.-кор. НАН Азербайджана Р.Ш. Курбанов, Баку.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМІ УПРАВЛІННЯ БУРІННЯ МОРСЬКИХ НАФТОГАЗОВИДОБУВНИХ СПОРУД

Х.Н. Рзаєв, Ф.Г. Самедов, З.Б. Іманова, Ж.С. Джамалова

Розглядається система управління бурінням морських нафтовидобувних споруд, проводиться аналіз основних вимог до якості обслуговування на основі протоколів, які забезпечують обмін даними в мережі управління бурінням, аналізуються загрози інформаційної безпеки циркулюючих потоків даних. Розглядаються основні протоколи забезпечення достовірності безпеки в перспективних системах надання послуг зв'язку мережі NGN.

Ключові слова: *інформаційно-телекомунікаційна система, безпека, вірогідність, морські нафтогазові споруди.*

PROVIDING INFORMATION SAFETY IN THE CONTROL SYSTEM FOR DRILLING MARINE OIL AND GAS FACILITIES

H.N. Rzaev, F.G. Samedov, Z.B. İmanova, J.S. Jamalova

The paper considers the control system for drilling marine oil and gas facilities performs analysis of basic requirements to service quality based on protocols that ensure communication in management drilling network, analyzes information security threats of circulating data flows. The main protocols that ensure reliability and safety in advanced systems for providing connection services in NGN network.

Keywords: *information-telecommunication system, safety, reliability, marine oil and gas facilities.*