ВВЕДЕНИЕ

Современное состояние и развитие телекоммуникационных систем как в России, так и за рубежом, характеризуется стремлением производителей и провайдеров услуг к предоставлению пользователям (через единую точку доступа) неограниченного спектра приложений с гарантированным качеством обслуживания (Quality of Service, QoS).

Необходимо отметить, что решение проблемы доступа пользователей к информации имеет свою историю. В середине XX столетия А.А. Харкевичем была высказана идея создания единой автоматизированной сети связи (ЕАСС) страны для «...удовлетворения потребностей в доставке различных видов информации для народного хозяйства и населения» [110]. Цель ЕАСС — максимально объединить, унифицировать и автоматизировать все средства связи СССР, что позволило бы значительно сократить финансовые и организационные ресурсы страны на подготовку кадров, проектирование, строительство и обслуживание телекоммуникационных систем. Однако реализация данной программы изначально была затруднена из-за использования аналоговых форм представления информации при ее передаче через ЕАСС.

В конце двадцатого столетия, с появлением новых форм представления информации и методов управления в телекоммуникационных системах, идея объединения и унификации различных служб электросвязи нашла свое отражение в создании цифровых сетей интегрального обслуживания (ЦСИО).

Первоначально предполагалось, что ЦСИО будет предоставлять пользователю возможность передачи информации в цифровом формате со скоростью $N \times 64$ кбит/с. В результате такие сети получили название узкополосные ЦСИО. Однако данное решение оказалось не способным поддерживать высокоскоростные службы электросвязи, функционирующие в реальном времени.

С появлением технологии асинхронного метода передачи (Asynchronous Transfer Mode, ATM) [127], фундаментально отличающейся от других телекоммуникационных технологий, появилась возможность создания транспортного механизма для передачи всех видов информации с QoS. В результате такие телекоммуникационные системы получили название широкополосных ЦСИО (рекомендации

МСЭ-Т, серия I.700–799).

Конкуренция производителей, провайдеров услуг в борьбе за пользователей телекоммуникаций активизировала дальнейшее развитие интернет-протокол (Internet Protocol, IP) технологии. Как следствие, рабочей группой, проектировавшей IP (Internet Engineering Task Force, IETF), были разработаны технологии MPLS [161] (Multiprotocol Label Switching — мультипротокольная коммутация по меткам) и IP v.6.0 [160], позволяющие предоставить пользователю неограниченный спектр приложений и QoS.

В результате IP/MPLS и ATM стали базовыми технологиями для мультисервисных сетей связи (МСС) [38], которые имеют отличия, но имеют и много общего:

- любая пользовательская и служебная информация преобразуется в единую форму — цифровые блоки определенной длины (пакеты);
- к каждому цифровому блоку добавляется заголовок с данными о маршруте, который предварительно определен и гарантирует поддержание требуемых вероятностно-временных характеристик (скорость передачи информации, задержка во времени, временной джиттер, вероятность неправильного приема на сообщение/пакет/символ, вероятность отказа в обслуживании) передаваемой информации;
- передача пользовательских и служебных пакетов осуществляется путем асинхронного мультиплексирования в соответствующие пользовательские и служебные цифровые тракты и каналы;
- в пункте назначения пакеты объединяются, преобразуются в первоначальную форму и передаются пользователю для дальнейшей обработки.

Таким образом, представление всех видов информации в едином цифровом формате и выделение требуемых ресурсов сети, гарантирующих QoS, перед началом передачи пользовательской информации являются обязательными компонентами технологий IP/MPLS и ATM.

Естественно, что при уникальной возможности мультисервисных сетей связи предоставлять пользователям неограниченный спектр приложений в реальном времени возникает проблема защиты пользовательской информации. В этой связи исследовательской комиссией МСЭ-Т в 2003 г. были разработаны рекомендации X.805 «Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами» [174]. Значимость данного документа в том, что впервые определена методология организации информационной безопасности телекоммуникационных систем. Архитектура

безопасности разделяет все ресурсы телекоммуникационных систем (каналы связи, программно-аппаратные комплексы, приложения и так далее) на независимые модули защиты информации. Каждый модуль характеризуется параметрами информационной безопасности, поддержание которых в актуальном (обновленном) состоянии является сложной организационной, технической и финансовой проблемой.

Значительный вклад в решение вопросов, связанных с созданием теоретического и практического задела построения защищенных, телекоммуникационных систем, внесли известные работы ученых А.П. Алферова, Д.П. Зегжда, А.С. Кузьмина, А.А. Молдовяна, А.Н. Молдовяна, Б.Я. Рябко, А.А. Шелупанова, В.В. Ященко, W. Diffie, V. Stollings, M. Hellman, C. Shannon, B. Schneier и многих других ученых.

В последнее десятилетие, начиная с публикации W. Lou и Y. Fang [143], ведутся активные исследования возможности обеспечения конфиденциальности информации в мобильных сетях за счет механизмов сетевого уровня модели взаимосвязи открытых систем [43, 54, 123, 125, 143, 156, 167]. Данный подход имеет ряд преимуществ. Во-первых, чем масштабней сеть связи, тем больше ее ресурсов можно задействовать для обеспечения конфиденциальности пользовательской информации. Во-вторых, пользователь не обязательно должен иметь дополнительное специальное программно-аппаратное обеспечение.

По мнению автора, использование территориально-распределенных ресурсов в мультисервисных сетях связи (каналов связи, криптографических программно-аппаратных комплексов, баз данных и так далее) является одним из путей решения комплексной защиты пользовательской информации. В этом случае пользователю достаточно определить свой профиль защиты информации — количественные или качественные оценки параметров информационной безопасности. Система управления, проведя мониторинг свободных ресурсов мультисервисной сети связи, реализует не только соединение, поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль в виде структуры соединений защиты информации [128].

Реализация данного подхода возможна за счет механизмов сетевого уровня модели взаимосвязи открытых систем (протоколов маршрутизации и сигнализации), в основу которых легли результаты научных исследований ученых Г.П. Башарина, В.А. Богатырева, А.В. Бутрименко, В.М. Вишневского, С.Л. Гинзбурга, В.С. Гладкого, Б.С. Гольдштейна, И.М. Гуревича, А.В. Ершова, Г.П. Заха-

рова, А.Е. Кучерявого, В.Г. Лазарева, А.Н. Назарова, М. Шварца, М.А. Шнепс-Шнеппе, Г.Г. Яновского, D. Barber, D. Bertsekas, D. Davies, R. Gallager, M. Gerla, L. Kleinrock, W. Price, C. Solomonides и многих других ученых.

В монографии предлагаются теоретико-методологические основы комплексной защиты пользовательской информации (обеспечение конфиденциальности, целостности и доступности) на базе технологий сетевого уровня (протоколов маршрутизации и сигнализации) мультисервисных сетей связи.

Материал книги состоит из результатов, в которых автору принадлежит основная роль в постановке, решении задач и в обобщении полученных результатов. Некоторые результаты получены в соавторстве с аспирантами научной группы автора (А.С. Буров, В.О. Жарикова, А.А. Киселев, О.И. Солонская).

Автор выражает глубокую признательность своей супруге Л.Т. Новиковой за поддержку, оказанную мне на протяжении ряда лет при написании монографии; д.т.н., профессору В.П. Шувалову за ценные советы при подготовке настоящей монографии к изданию.

Существенная помощь, способствующая улучшению содержанию книги, была оказана доктором физ.-мат. наук, профессором С.В. Белим, доктором техн. наук В.Е. Митрохиным и доктором физ.-мат. наук, профессором В.К. Попковым, взявшим на себя труд по ее рецензированию, за что автор им чрезвычайно благодарен.