ВВЕДЕНИЕ

Современные телекоммуникационные системы (телекоммуникация — от греч. tele — вдаль, далеко и лат. communicatio — общение, т. е. дословно — связь на расстоянии) и сети являются синтезом развития двух исходно независимых сетей — сетей электросвязи (телеграфной, телефонной, телетайпной и радиосвязи) и вычислительных сетей.

Логика развития систем связи требовала применения цифровых систем передачи данных, а также вычислительных средств для решения задач маршрутизации, управления трафиком, сигнализации. В свою очередь, логика развития вычислительной техники требовала все большего применения средств связи между периферийными устройствами и отдельными ЭВМ. Достигнутое в результате этих двух встречных движений совмещение техники связи с вычислительной техникой позволило усовершенствовать технологию обслуживания телефонной инфраструктуры и повысить эффективность отрасли связи, а также полнее использовать ресурсы вычислительных центров, вычислительных систем и сетей путем перераспределения этих ресурсов и решаемых задач.

Под защитой информации обычно понимают деятельность, направленную на недопущение утечки информации, несанкционированного и непреднамеренного воздействия на информацию, в частности, содержащуюся в телекоммуникационных системах.

Предотвращение утечки информации в телекоммуникационных системах направлено на предупреждение разглашения конфиденциальной информации, несанкционированного доступа к ним. Защита информации также направлена на за-

щиту от искажения конфиденциальной информации, ее уничтожения, блокирования доступа и аналогичных действий с носителем информации. Разрушительные действия с информацией в телекоммуникационных системах могут осуществляться со злым умыслом или без него.

Многообразие информации (знания) об окружающем мире в научной литературе разделяется на две категории. Первая категория знаний связывается с наблюдениями и ощущениями, получаемыми человеком из окружающего мира, и называется *сведениями.* Вторая категория относится к отображению человеком полученных сведений на материальных носителях в виде рисунков, текстов, таблиц, диаграмм, звуков, фильмов и др. Знания второй категории называются *сообщениями*, будучи созданными человеком или техническим устройством, они могут быть доступными широкому кругу лиц. В связи с этим перед обладателем (создателем и/или законным пользователем) сообщений возникают по отношению к ценным сообщениям следующие основные задачи, составляющие предмет теории защиты информации:

- обеспечение надежного хранения сообщений и управление доступом к информации со стороны различных категорий пользователей, в том числе блокирование доступа к информации со стороны нарушителя (защита от несанкционированного доступа);
- при передаче информации между законными пользователями обеспечение надежной защиты от искажения сообщений и от ознакомления с ними посторонних лиц или нарушителя;
- регулирование права, связанного с обладанием и пользованием информацией.

Объекты добычи информации для нарушителя — это информационные системы законных пользователей и сообщения, передаваемые по телекоммуникационным системам.

На протяжении всей истории человечества наблюдалось противодействие защиты и нападения по отношению к ценной информации. Это противодействие явилось основным движущим фактором развития методов и средств как защиты информации, так и ее добычи. Оба направления информацион-

ной деятельности (защита и добыча) взаимно стимулировали совершенствование методов и средств, являясь, по существу, двумя сторонами медали.

Современные методы защиты информации классифицируются по решаемым задачам:

- организационно-административные методы направлены на обеспечение режима секретности на предприятиях, фирмах, учреждениях, располагающих ценной информацией, на противодействие нарушителю с помощью доверенных зон, сейфов, хранилищ и т. д.;
- правовые методы предназначены для юридической защиты информации, регулирующей права на собственность, на использование информации и др.;
- инженерно-физические методы обеспечивают защиту информации в определенной территориальной зоне или в рабочем помещении от утечки по акустическим и электромагнитным каналам, в том числе при обработке информации различными техническими устройствами. Инженерные методы направлены также на разработку устройств-контейнеров для хранения данных, защищенных от несанкционированного проникновения, и на разработку технических средств передачи информации, затрудняющих нарушителю съем данных с линии связи;
- стеганографические методы предназначены для сокрытия секретного сообщения (в том числе зашифрованного) «внутри» несекретного сообщения. При этом форма несекретного сообщения за счет избыточности не претерпевает явных изменений, т. е. скрывается сам факт вложения секретного сообщения. К примерам методов стеганографии относятся:
  - запись симпатическими чернилами секретного текста между строк обычного письма;
  - «встраивание» секретного сообщения в рисунок (телекадр, файл) с помощью изменения относительно небольшого числа его элементов (точек, пикселей), при этом параметры измененных элементов несекретного сообщения кодируют символы секретного сообщения;

- и, наконец, криптографические методы, которые являются в настоящее время основными методами защиты информации в телекоммуникационных системах и которые связаны с поиском и исследованием математических методов преобразования информации.

В последние десятилетия в криптографических методах защиты информации активную роль стали играть квантовые методы, дополнившие и обогатившие их.

Квантовая теория, пришедшая в первые десятилетия XX века на смену классическим представлениям о мире, принесла с собой целый ряд контринтуитивных, странных с точки зрения здравого смысла ограничений на возможность манипуляции физическими объектами. Знаменитый принцип неопределенности Гейзенберга провозглашает невозможность одновременного измерения координаты и импульса частицы с произвольной точностью. Постулат редукции волновой функции, выдвинутый фон Нейманом, указывает на невозможность в общем случае измерения квантовой системы без разрушения ее состояния. Открытый в 1982 году принцип квантовой неклонируемости утверждает невозможность создания копии (клона) квантовой системы, сколь угодно близкого к оригиналу. С практической точки зрения эти и подобные им ограничения долгое время носили только отрицательный характер, показывая, что при достижении определенной точности в работе телекоммуникационных систем возникают дополнительные трудности, связанные с квантовой природой физических объектов, такие как «квантовый шум» оптического канала связи, «квантовый шум» фотодетектора, стандартный квантовый предел в прецизионных измерениях и др. Замечательным нововведением стала идея применения квантовых методов в таких приложениях, которые нуждаются в защите от действий противника или нарушителя (которых вместе можно именовать злоумышленниками) и ограничения возможностей последнего на основе фундаментальных квантовых законов. Таким образом, «отрицательные» свойства квантовых систем, такие как «хрупкость» для измерения, становятся «положительными», коль скоро с этой «хрупкостью» сталкивается злоумышленник.

Исторически первой задачей такого типа [8] была идея создания «квантовых денег», защищенных от подделки при помощи специальных некопируемых маркеров, над которой американский ученый Визнер размышлял в 70-е годы XX века [65]. Работы Визнера были опубликованы только в 1983 году, поэтому рождение нового направления обычно связывают с предложением американца Ч. Беннета и канадца Ж. Брассара по использованию двухуровневых квантовых систем для распределения между двумя пользователями секретного ключа, не доступного злоумышленнику, прослушивающему канал связи. Однако в 1980-е годы этой проблемой занимался очень узкий круг людей, так как основная идея Беннета и Брассара (протокол BB84) была опубликована в 1984 году в трудах малоизвестной индийской конференции, после чего все работы в США по этой теме были засекречены. Широкая известность в научных кругах к данному направлению исследований пришла только в 1991 году, когда английский ученый А. Экерт опубликовал совершенно иной метод решения той же самой проблемы защищенного от перехвата распределения ключей. Метод, предложенный Экертом, опирался не только на использование двухуровневых квантовых систем, но и на использование сильных квантовых корреляций (перепутывания) между ними, т. е. был, так сказать, «дважды квантовым». В скором времени были опубликованы рассекреченные результаты группы Ч. Беннета по успешной экспериментальной реализации квантового распределения ключей на одиночных фотонах в открытом пространстве.

С этого момента новое научное направление, получившее название квантовой криптографии, стоящее на стыке криптографических и инженерно-физических методов защиты информации, стало интенсивно развиваться, привлекая специалистов из совершенно разных областей знания — математической теории информации, квантовой оптики, физики твердого тела, обоснования квантовой теории и др. За прошедшие три десятилетия было предложено множество новых протоколов и опробованы различные методы их реализации, выполнена важная работа по доказательству безусловной защищенности квантовых протоколов от перехвата и разработаны

первые коммерческие и государственные квантовые криптосистемы.

Современные стандартные криптографические линии еще далеки от совершенства, к примеру, канал со скоростью генерации ключа 50 кбит/с обладает дальностью действия обычно не более 100 км. Однако этот канал имеет одно важное преимущество перед популярными классическими асимметричными криптосистемами — он является безусловно защищенным. Безусловность в данном случае означает отсутствие предположений о возможностях злоумышленника — за пределами передающей и принимающей станций он может делать все, что не противоречит законам природы. В то же время классические асимметричные системы распределения ключей, например алгоритм RSA, используемый для шифрования данных, всегда защищены только от злоумышленника, обладающего ограниченными вычислительными ресурсами. Например, пароль, посылаемый через телекоммуникационную сеть Интернет, защищен от обладателя персонального компьютера (рядового хакера), но не защищен от обладателя суперкомпьютера (правительства развитой страны). Именно поэтому квантовая криптография уже сегодня находит спрос в крупном бизнесе и правительственной связи. К примеру, уже в начале 2021 года в Китае под руководством учёных из Университета науки и технологий была развёрнута первая в мире интегрированная сеть квантовой связи общей протяжённостью сети в 4600 км. И это не просто оптический кабель от точки до точки, а полностью рабочая сеть из более чем 700 оптических сегментов и двумя станциями космической связи с передачей данных по спутниковым каналам. К интегрированной сети квантовой связи было подключено свыше 150 абонентов: банков, предприятий, госучреждений и других служб, которым нужна сверхзащищённая связь. Также в 2021 году китайским ученым, используя спутник связи, удалось произвести квантовый обмен ключами между двумя наземными станциями, расположенными на расстоянии 1120 км друг от друга.

Постоянный рост скорости передачи и снижение себестоимости позволяют надеяться на более широкое распростра-

нение квантовых криптосистем уже в ближайшем будущем. Опытная квантовая сеть с открытым доступом введена в тестовую эксплуатацию, к примеру, и в Москве. Она соединяет университеты МИСиС и МТУСИ и доступна для внешних подключений. На очереди стоят разработка глобальной спутниковой криптографической сети и расширение наземных сетей на трансатлантические расстояния при помощи квантовых повторителей.

Основная часть пособия посвящена протоколам квантового распределения ключей и физическим основам их функционирования. С задачей квантового распределения ключей связана и задача их генерации, которая также может быть решена квантовыми методами, обзор математических основ которых будет рассмотрен в пособии. Существуют и менее распространенные способы использования квантовых методов в задачах защиты информации в телекоммуникационных системах, к которым относятся построение квантовых аналогов традиционных криптографических систем и механизмов обеспечения конфиденциальности, целостности и аутентификации. Один из разделов пособия посвящен и данной теме. Подобный широкий охват отличает это издание от основного ряда работ, посвященной данной тематике.

Пособие построено в основном на основе материалов [8, 69], которые использовались при чтении лекций в магистратуре Московского технического университета связи и информатики по направлению подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи» по программе «Квантовые коммуникации» весной 2022 года. В конце издания наряду с приложениями, в которых вкратце рассмотрены основы квантовой механики и математические основы современных квантовых методов, приведен список учебной литературы, которая может быть полезна для изучения различных аспектов криптографии и квантовых коммуникаций, а также список из более чем 60 научных работ, связанных с тематикой, охватываемой пособием, предназначенный для общего ознакомления.

Учебное пособие предназначено для студентов высших учебных заведений, обучающихся по направлению бакалавриата 11.03.02 «Инфокоммуникационные технологии и системы

связи», по направлению специалитета 10.05.02 «Информационная безопасность телекоммуникационных систем», по направлениям магистратуры 09.04.01 «Информатика и вычислительная техника», 11.04.02 «Инфокоммуникационные технологии и системы связи», а также может быть полезно специалистам в области квантовых коммуникаций и защиты информации.