Введение

Одной из актуальнейших задач в современных телекоммуникационных системах и сетях (телекоммуникация — от греч. tele — вдаль, далеко и лат. communicatio — общение, т. е. дословно — связь на расстоянии), которые являются синтезом развития двух исходно независимых сетей — электросвязи (телеграфной, телефонной, телетайпной и радиосвязи) и вычислительных, стала задача обеспечения защиты информации.

Под защитой информации обычно понимают деятельность, направленную на недопущение утечки информации, несанкционированного и непреднамеренного воздействия на информацию. Предотвращение утечки информации в телекоммуникационных системах направлено на предупреждение разглашения конфиденциальной информации и несанкционированного доступа к ним. Защита информации также направлена на защиту 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.

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 целях ее защиты.

В последние годы ведутся активные исследования квантовых компьютеров — вычислительных устройств, основанных на законах квантовой физики. Важно понимать, что квантовый компьютер неправильно рассматривать как «классический компьютер с огромной мощностью». Отличие между классическими компьютерами и квантовыми фундаментальное, оно лежит в плоскости принципов работы устройства. Из-за этого классические и квантовые алгоритмы отличаются друг от друга.

Под методом, или алгоритмом, Шора понимают квантовый алгоритм, позволяющий решить задачи факторизации числа и дискретного логарифмирования, на которых основана основная часть современных методов асимметричной криптографии, за полиномиальное время. Впервые этот метод был предложен американским ученым Питером Шором в 1994 году [104]. Алгоритм Шора уже был продемонстрирован на практике для малых чисел. Так, еще в 2001 году группа исследователей из IBM при помощи квантового компьютера с 7 кубитами показала разложение числа 15 с помощью алгоритма Шора. Существуют и другие квантовые алгоритмы, которые могут быть опасны для существующих в настоящее время криптографических методов защиты информации. Сложившаяся ситуация получила название «квантовой угрозы».

Конечно, на сегодняшний день не существует такого квантового компьютера, который способен оперировать числами, использующимися в криптосистемах на практике. Однако число кубитов, с которыми мы можем оперировать, растет. В июле 2021 года в известном журнале Nature была опубликована работа [105], в которой был представлен программируемый квантовый симулятор на 256 кубитов. Таким образом, безопасность таких асимметричных систем шифрования, как, например, RSA, находится под угрозой. То же самое можно сказать и по поводу протокола Диффи–Хеллмана, активно используемого в телекоммуникационных системах.

Существуют две основные линии защиты от квантовой угрозы. Первая линия защиты предполагает использование квантовых технологий для изменения способа защиты на физическом уровне. К таким технологиям относится, например, квантовое распределение ключей, позволяющее безопасно обмениваться ключами благодаря законам квантовой физики. С его основами можно ознакомиться, к примеру, в [5]. Вторая линия защиты предполагает использование криптосистем, безопасность которых основывается на задачах, для которых в настоящее время не существует эффективных квантовых и классических алгоритмов решения. Такие криптографические схемы принято называть постквантовыми.

Данное пособие посвящено изложению различных аспектов постквантовой (или квантово-устойчивой) криптографии, являющейся одним из эффективных методов обеспечения безопасности телекоммуникационных сетей при широком внедрении перспективных квантовых компьютеров.

Первый раздел данного пособия посвящен описанию классической криптографии с открытым ключом и специфике ее использования в Российской Федерации. Второй раздел пособия посвящен оценке квантовой устойчивости криптографических алгоритмов, используемых в современной телекоммуникационной инфраструктуре. Третий раздел описывает основные подходы к построению квантово-устойчивых алгоритмов и описывает основные вехи конкурса NIST PQC по их стандартизации.

Большая часть пособия посвящена описанию принципов построения и описанию наиболее распространенных реализаций алгоритмов электронной подписи и распределения ключа или шифрования постквантовой криптографии, основанных на пяти наиболее распространенных подходах — с использованием алгебраических решеток, систем квадратных уравнений над конечными полями, кодов, корректирующих ошибок, хеш-функций и изогений суперсингулярных эллиптических кривых. Учебные пособия, посвященные данной тематике, на русском языке до настоящего времени неизвестны широкому кругу читателей.

Пособие написано в основном в рамках программы дисциплины «Постквантовая криптография», которая читается на втором курсе магистратуры Московского технического университета связи и информатики по направлению подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи» по программе «Квантовые коммуникации» на основе материалов, полученных авторами в рамках научно-исследовательской работы [88]. В конце издания наряду с приложением, в котором вкратце рассмотрены математические основы современной криптографии, приведен список учебной литературы, которая может быть полезна для изучения различных аспектов криптографии, в том числе и постквантовой, а также список из более чем 80 научных работ, связанных с

тематикой, охватываемой пособием, и предназначенных 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 защиты информации.