СТАТЬИ

УДК 004.056.53

КВАНТОВЫЙ ХАКИНГ: АТАКИ НА ЛИНИИ СВЯЗИ

Белера Р.А., Деев Д.Д., Смирнов И.А., Короченцев Д.А., Черкесова Л.В.

ГОУ ВПО «Донской государственный технический университет», Ростов-на-Дону, e-mail: chia2002@inbox.ru

В статье рассмотрены вопросы надежности квантовой криптографии, необходимость её использования в современных линиях связи, её преимущества и недостатки при практическом применении. Проанализированы аппаратные возможности современных квантовых линий связи, вопросы их технических характеристик, видов применяемых квантовых протоколов и эффективности систем защиты информации. С развитием информационных технологий и вычислительных способностей техники новых поколений (квантовых компьютеров) математические криптографические алгоритмы с течением времени устаревают. Утверждения, что тот или иной канал связи полностью безопасен, как представляется авторам, несостоятельны – рано или поздно он будет взломан. Исследована сама возможность кибератак на квантовые линии связи, и выявлено не менее 20 видов возможных атак, основанных на несовершенстве аппаратуры. Несомненно, что сегодня не существует абсолютно надёжной и защищённой криптосистемы и/или линии связи, как неквантовой, так и квантовой, и пока не представляется возможным реализовать её на практике из-за существования многочисленных уязвимостей. Достаточно квалифицированный хакер сможет использовать эти уязвимости для осуществления своих целей с помощью квантового хакинга – взлома, похищения и/или уничтожения информации, передаваемой в квантовых линиях связи. Количество возможных квантовых атак с течением времени будет только увеличиваться. При разработке системы сертификации для квантовой криптографии проблемой является тот факт, что в теории – квантовая криптография является надёжной и принципиально невзламываемой, но на практике квантовые системы связи далеко не идеальны. Любые системы делают люди – обычные работники, которые должны выполнить свой план, и при этом уложиться в установленные сроки. И это создает огромное количество дыр и уязвимостей в реализации, отличий между задуманной идеальной системой и её несовершенной в техническом отношении практической реализацией. Всё это вместе и является питательной средой для злоумышленника – для осуществления квантового хакинга.

Ключевые слова: квантовые линии связи, неопределенности Гейзенберга, квантовые протоколы, аппаратура квантовой связи, квантовый хакинг, аппаратные атаки, уязвимости линии связи

QUANTUM HACKING: ATTACKS ON COMMUNICATION LINES

Belera R.A., Deev D.D., Smirnov I.A., Korochentsev D.A., Cherckesova L.V.

Don State Technical University, Rostov-on-Don, e-mail: chia2002@inbox.ru

The article discusses the reliability of quantum cryptography, the need for its use in modern communication lines, its benefits and downsides in the application in practice. The hardware capabilities of modern quantum communication lines, their technical characteristics, types of quantum protocols used, and the effectiveness of information security systems are analyzed. With development of information technologies and computing capabilities of new technology generations (quantum computers), mathematical cryptographic algorithms, over time, become obsolete. Claims that a particular communication channel is completely secure, as it seems to the authors, are untenable – sooner or later it will be hacked. The possibility of cyberattacks on quantum communication lines has been investigated, and at least 20 types of possible attacks based on hardware imperfections have been detected. Apparently, that today there is no absolutely reliable and secure cryptosystem and/or communication line, both non–quantum and quantum, and it is not yet possible to implement it in practice because of presence of many vulnerabilities. Sufficiently skilled hacker will be able to use these vulnerabilities to achieve their goals through quantum hacking – stealing and/or destroying information transmitted in quantum communication lines. The number of possible quantum attacks will only increase over time. When developing certification system for quantum cryptography, the problem is that in theory quantum cryptography is reliable and unbreakable in principle, but in practice, quantum communication systems are far from ideal. Any systems are made by people – the ordinary workers who must fulfill their plan, and at the same time meet the deadlines. It creates a huge number of holes and vulnerabilities in the implementation, differences between the conceived ideal system and its technically imperfect practical implementation. All this together is breeding ground for an attacker – for quantum hacking.

Keywords: quantum communication lines, Heisenberg uncertainties, quantum protocols, quantum communication equipment, quantum hacking, hardware attacks, communication line vulnerabilities

Развитие квантовых технологий является одним из основных направлений в современном IT–мире. Исследователи всего мира тестируют системы квантовой связи, использующие протоколы квантовой криптографии. Их особенность заключается в том, что в идеале невозможно перехватить информацию, передаваемую через квантовый канал связи. Главная идея квантовой криптографии – передавать информацию так, чтобы ее нельзя было перехватить, даже в принципе. И сразу появляются резонные вопросы: какими характеристиками должна обладать квантовая линия связи, какие квантовые протоколы будут применяться, насколько они эффективны для защиты информации, какова скорость передачи данных, каково максимальное расстояние при передаче информации, каков должен быть уровень защищенности и безопасности ка-

нала связи, какой должен применяться алгоритм шифрования?

Сегодня можно сказать, что квантовые криптографические протоколы не будут слишком сложными, т.к. злоумышленник всё равно не сможет их расшифровать, не обладая достаточно высокими вычислительными мощностями. Современные классические суперкомпьютеры имеют вычислительные мощности, несопоставимые с квантовыми, не говоря уже о персональных гаджетах. Постоянно разрабатываются и совершенствуются новые квантовые вычислительные системы, протоколы и алгоритмы передачи данных, практически не подверженные криптоанализу.

Цель исследования: главный вопрос состоит в том, как передавать информацию уже сейчас, применяя не пока ещё не разработанную идеальную систему квантовой связи, а реально существующие физические линии – т.е. чем идеальная теория отличается от реальной практики? В настоящее время для передачи данных используются беспроводные и волоконно–оптические линии связи (ВОЛС). По дороге к адресату фотон может подвергнуться воздействию многих факторов, способных его уничтожить. Вопрос о надежности квантовой криптографии и о реальной возможности квантового хакинга очень актуален и является целью нашего исследования.

Материалы и методы исследования

Хакинг связан с внесением изменений в программное обеспечение для достижения целей, отличающихся от целей создателей программ. Такие изменения являются вредоносными. Злоумышленником, занимающимся хакингом, может быть кто угодно, но зачастую хакеры – это весьма квалифицированные программисты и тестировщики программного и аппаратного обеспечения, способные применить свои профессиональные навыки для добычи или перехвата интересующей их информации. Утверждения, что тот или иной канал связи или метод шифрования данных полностью безопасен, безосновательны, всё равно он рано или поздно будет взломан. Развиваются информационные технологии, растут вычислительные способности, а математические криптографические алгоритмы с течением времени устаревают. Информацию, зашифрованную алгоритмами классической криптографии, всегда можно скопировать и сохранить на будущее, а когда система шифрования будет взломана, ранее сохранённую информацию можно будет прочитать «задним числом» [1].

Это нежелательно для многих категорий тайн – государственных, правительственных, военных, коммерческих, медицинских, банковских, конфиденциальных, – разоблачение которых может привести к нежелательному резонансу и катастрофическим последствиям.

Надежность алгоритмов квантовой криптографии обеспечена действием принципа неопределенности Гейзенберга. Этот принцип гласит, что в одно и то же время с большой точностью определить координаты и скорость квантовой частицы нельзя [2]. Определение принципа неопределенности таково:

$$\Delta x \Delta p \geq \frac{\hbar}{2},$$

где Δx – это среднеквадратичное отклонение координаты, Δp – среднеквадратичное отклонение импульса; $\hbar$ – приведённая постоянная Планка, которая равна 1,054571800 (13)$\times$ $\times 10^{-34}$ Дж·с = 6,582119514 (40)$\times 10^{-16}$ эВ·с.

В нерелятивистской физике это неравенство показывает, квантовая частица может иметь такое состояние, что значение x можно измерить с какой угодно высокой точностью, но в этом случае значение p будет известно приблизительно, или наоборот. Во всех иных состояниях x и p можно измерить с вполне приемлемой точностью. Если неравенство рассматривать со стороны релятивистской физики, то в системе отсчёта, созданной применительно к самому микрообъекту, для нахождения его координат имеется наименьшая элементарная погрешность: $\Delta q \sim \frac{\hbar}{mc}$. Ей соответствует неопределённость, связанная с импульсом $\Delta q \sim mc$, отвечающая наименьшей пороговой энергии, необходимой для образования *пары частица – античастица*. В итоге всех этих действий обнаруживается, что проведённые измерения потеряли всякий смысл [3].

В той системе координат, в которой рассматриваемый микрообъект движется с пороговым значением энергии $\Delta q \sim mc$, наименьшая погрешность измерения его координат равна: $\Delta q \sim \frac{\hbar c}{\in}$. В случае ультрарелятивистских энергий, в пределе, импульс соотносится с энергией квантовой частицы выражениями $\varepsilon = cp$ и $\Delta q \sim \frac{\hbar}{p}$. Это значит, что погрешность (ошибка) измерения координат оказывается близкой к величине длины волны микрообъекта, описанной Де Бройлем [3]. В выражениях для неопределённостей равенство получается в том случае, если «форма представления вектора состояния системы в координатном пред-

ставлении совпадает с формой его представления в импульсном представлении» [2; 3].

Данная неопределенность применима к квантовым технологиям так: если есть движущаяся частица, то можно измерить положение этой частицы в пространстве, но при этом теряется информация о её скорости. Однако можно вычислить положение частицы в пространстве и после измерения её скорости, но при этом возможно будет получить только случайное значение. На такие пары квантовых свойств, которые невозможно измерить одновременно, и кодируются биты в квантовой криптографии. Для этого случайным образом выбирается, какое из свойств использовать для кодирования информации. Выбор неизвестен злоумышленнику, и он, в идеале, не сможет прочитать информацию, а если, гипотетически, сможет, то только с ошибками, делающими невозможным понимание смысла информации.

Надежность квантового шифрования на данный момент считается очень высокой. Сегодня в мире широко применяются симметричные и асимметричные криптографические алгоритмы. Практически на все виды алгоритмов существуют атаки, и одним из основательных решений для сохранения устойчивости информации является увеличение размерности ключа.

Сегодня считается, что размерности ключа от 128 бит считаются надежными, однако для информации, содержащей государственную тайну, требуются ключи 192 и 256 бит, как в американском шифре AES или российском «Кузнечике». Это связано с тем фактом, что у злоумышленников не хватит вычислительных мощностей для перебора всех вариантов для взлома информации. С развитием технологий это кажется *сомнительным* и не даёт 100 % гарантии, что эта информация сохранится в тайне и будет надежно защищена [4]. К примеру, шифр RSA в 1976 г. с кодированием в 425 бит считался абсолютно надежным, и для его расшифрования, по мнению авторов, понадобилось бы 40 квадриллионов лет. Но спустя 15 лет, в 1993 г., был запущен проект распределённых вычислений, который координировался через электронную почту, связанный с нахождением сомножителей числа RSA–129. Чтобы решить эту головоломную задачу, почти 600 волонтёров из двадцати стран всего земного шара более чем полгода отдавали своё машинное время 1600 компьютеров, но расшифровали сообщение, за которое авторы 15 лет назад объявили награду в 100$ [5].

Сегодня ключи RSA имеют размерности более 2048 бит, и это, скорее всего, не предел.

Квантовая криптография и квантовые линии связи сегодня являются ответом на многие вызовы, стоящие перед современной кибербезопасностью информационных систем.

Этапы передачи сигнала в квантовой криптографии представлены на рис. 1. С помощью лазерного диода генерируются импульсы света, которые впоследствии затухают на уровне фотонов. Затем они через атмосферную оптическую линию связи (АОЛС) передаются получателю, где идентифицируются в течение заданных промежутков времени. Передатчик генерирует синхроимпульсы с периодом времени T; импульсы света уменьшаются на уровне фотонов; затем однофотонный детектор активируется электрическими импульсами, которые и появляются на выходе такого однофотонного детектора [6].

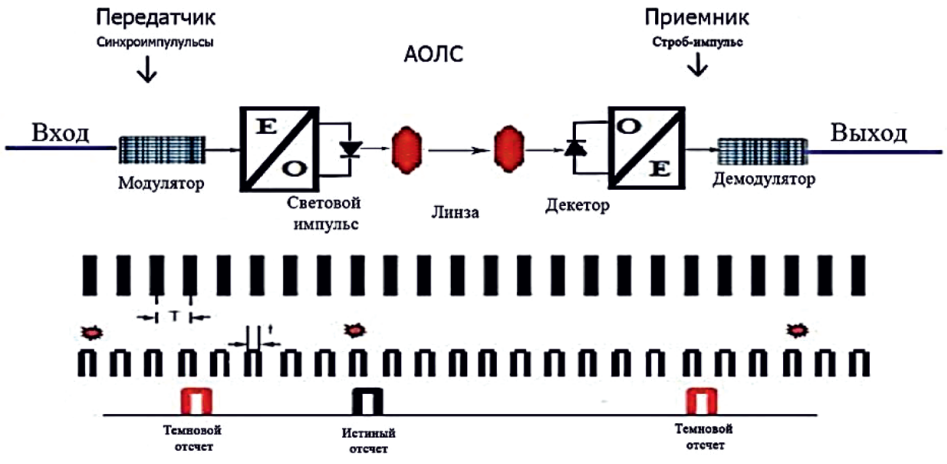

Рис. 1. Этапы передачи сигнала в квантовой криптографии

Отсчёты однофотонного детектора (темновые показания) возникают самопроизвольно и являются, по существу, паразитным сигналом. Однако его нужно принимать в расчёт при работе с системами квантовой криптографии, так как эти сигналы могут послужить причиной значительного искажения сигнала. Исследования проводятся в области разработки новых алгоритмов и протоколов квантовой криптографии, обладающих устойчивостью к квантовым алгоритмам. Такие протоколы можно разделить на две категории, показанные на рис. 2 [6].

Первая категория содержит квантово-криптографические протоколы, которые основаны на кодировании квантового состояния одиночной частицы. Они опираются на принцип невозможности различить два неортогональных квантовых состояния.

Вторая категория протоколов базируется на *перепутанных квантовых состояниях.* При этом контролируется, выполняется ли неравенство Белла и другие основные квантовые соотношения.

Известен квантовый протокол на перепутанных квантовых состояниях (на эффекте запутывания) А. Экерта EPR (в честь А. Эйнштейна, Б. Подольского и Н. Розена) E91.

Особая категория протоколов базируется на кодировании данных в квадратурных амплитудах, в состоянии квантованного электромагнитного поля.

Базовый протокол квантовой криптографии, основанный на состояниях одной частицы – BB84 (в честь Ч. Беннета и Ж. Брассара), использует два или три независимых базиса, состоящих из парных ортогональных состояний, выполняющих условие: квадрат модуля скалярного произведения состояний из разных базисов равен обратной размерности гильбертова пространства:

$$|\langle\omega_i|\varphi_i\rangle|^2 = 1/D,$$

для состояний из одного базиса скалярное произведение равно нулю:

$$\langle\omega_i|\omega_i\rangle = 0 \ (i, j = 1,2).$$

Можно составить независимые базисы, образованные парами ортогональных векторов поляризации, кодируя в поляризационных степенях свободы электромагнитного поля:

$$\left(|\updownarrow\rangle \equiv |V\rangle, |\leftrightarrow\rangle \equiv |H\rangle\right) \text{ вычислительный,}$$

$$|L\rangle B\frac{1}{\sqrt{2}}\left\{|H\rangle B|V\rangle\right\}, |R\rangle B\frac{1}{\sqrt{2}}\left\{|H\rangle B|V\rangle\right\} \text{ диагональный,}$$

$$|L\rangle \equiv \frac{1}{\sqrt{2}}\left\{|H\rangle + i|V\rangle\right\}, |R\rangle \equiv \frac{1}{\sqrt{2}}\left\{|H\rangle - i|V\rangle\right\} \text{ циркулярный [6].}$$

Использование квантового криптографического протокола распределения ключей BB84 или B92 (в честь Ч. Беннета) способно надежно защитить информацию.

Схема его работы представлен на рис. 3.

Рис. 2. Классификация протоколов квантовой криптографии

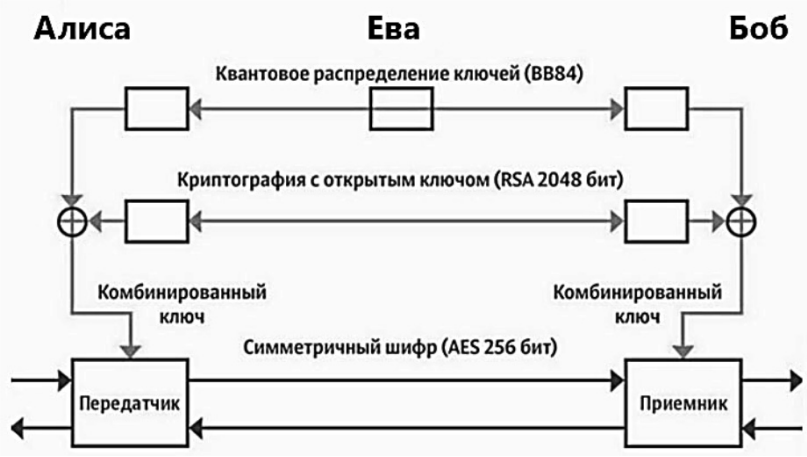

Рис. 3. Схема применения квантового алгоритма распределения ключей

Однако нельзя быть уверенными в том, что протоколы квантовой криптографии абсолютно безопасны и не могут быть подвержены кибератакам. К настоящему времени известны возможные атаки на квантовый протокол BB84 [6; 7]: для случая однофотонных сигналов (некогерентные, когерентные атаки); разделения числа фотонов. Криптографическая стойкость квантового протокола B92 основана на том факте, что при попытке измерить состояние фотона с помощью Евы возникает ошибка в другом, неортогональном состоянии. Однако существует идея атаки PNS (Photon–Number–Splitting Attack, атака разделения числа фотонов), основанной на том факте, что квантовый протокол может быть реализован на неуникальных фотонах. Возможность передачи ключа несколькими, а не только одним, фотонами открывает перспективу взлома квантовых сетей с помощью этой атаки, так как в этом случае становится возможным выбрать часть квантов из квантового канала связи, достаточную для измерения поляризации этого луча Евой. Одним из методов борьбы с этой пока неактуальной, но очевидной угрозой является снижение до возможного минимума мощности излучения, что, в свою очередь, затрудняет передачу данных на большие расстояния из–за ослабления сигнала в оптоволокне. Для борьбы с этой угрозой разработан новый трёхуровневый протокол (Decoy State Protocol), использующий малошумящий детектор, разработанный NIST [4].

Создаются и совершенствуются квантовые системы шифрования и протоколы, которые являются самыми мощными на сегодняшний день, однако есть проблема с безопасностью квантовых линий связи. Сегодня выявлено около 20 видов атак на квантовые каналы связи, проблема так и не решена. При атаке на конкретный канал используются несовершенства, огрехи и неидеальности в оптических аппаратных компонентах. Любая квантовая атака требует подключения к оптической линии связи, где перегоняются фотоны. Рассмотрим некоторые виды квантовых атак.

1. Атака с помощью светоделителя – основана на методе сканирования и разделения импульсов на две составляющие, и анализе каждой из частей в одном из двух базисов [7].

2. Атака «Квантовый троян» – основана на сканировании импульса с помощью оптического мультиплексора по направлению к отправителю или получателю. Импульс разделяется на две составляющие, для синхронизации детектирования, и передаётся на схему декодирования. Искажения пересылаемых фотонов при этом не наблюдается. Ева испускает сигналы, которые поступают на станции Алисы и Боба через квантовый канал. Она может послать лазерные импульсы в оптоволокно, которое соединяет станции А и Б, и проанализировать отраженный свет. Можно узнать, как и когда стрелял настоящий лазер, когда открывался счётчик фотонов, как настроены фазовые модуляторы или светоделители, и пр. Поэтому любые неоднородности в оптических трактах передатчика и приёмника должны быть сведены к минимуму [7].

3. Когерентные атаки, которые базируются на тактике ретрансляции. Предполагается, что Ева производит измерение после полного завершения открытого сеанса связи между Алисой и Бобом. Этот сеанс включает не только обсуждение базисов, но и выполнение протоколов коррекции ошибок и усиления секретности. При более

реалистичных индивидуальных атаках считается, что Ева ждет только окончания процедуры сравнения базисов. После проведения всех измерений Ева сможет отправлять Бобу «псевдофотоны в уже измеренных состояниях» [4].

4. Некогерентные атаки, принцип которых заключается в перехватывании и перепутывании фотонов отправителя с набором пересылаемых отдельных фотонов. Состояние группы измеряется, и изменённые данные пересылаются получателю [8]. Ева создает вспомогательные частицы (образцы, пробы) и выполняет взаимодействие созданных проб со всеми кубитами, пересылаемыми от Алисы к Бобу, после чего последовательно измеряет все свои пробы. В этом виде некогерентных атак предполагается, что Ева ждет только окончания процедуры сравнения базисов и не дожидается окончания процедур коррекции ошибок и усиления секретности. Индивидуальные атаки имеют важную особенность – они могут быть рассмотрены классическими методами. Это означает, что Алиса, Боб и Ева обладают некой классической информацией в виде случайных величин α, β, ε, и что законы квантовой механики позволяют рассматривать совместное распределение вероятностей $P(\alpha, \beta, \varepsilon)$ [8].

5. Атака с ослеплением лавинных фотодетекторов, разработанная В. Макаровым, позволяет хакеру добыть секретный ключ таким образом, что этого перехвата получатель даже не заметит. Для получения ключа однофотонный детектор адресата–получателя ослепляется (засвечивается) лазерным лучом. В этот момент хакер осуществляет перехват сигнала, посланного отправителем. Квантовый детектор получателя, ослеплённый лазером, переходит в режим работы обычного детектора, и при этом даёт «1» под влиянием мощного светового импульса, независимо от квантовых свойств самого импульса. В такой ситуации хакер, получив «1», может послать на детектор получателя–адресата импульс света. Тот посчитает, что получил этот сигнал от своего адресата. Так, злоумышленник может послать получателю обычный сигнал вместо квантового и, таким образом, перехватить полученные от отправителя данные, оставаясь незамеченным [4].

6. Атака с разделением фотонов состоит в том, что в импульсе выявляется не один фотон, а несколько. Затем происходит перемещение одного фотона и его перепутывание с пробой (рис. 4). Неповреждённая часть данных пересылается получателю, а хакер находит значение пересланного кубита и при этом не вносит ошибок в «просеянный ключ» [8].

7. Спектральная атака. В том случае, когда испускаемые фотоны созданы четырьмя различными фотодиодами, у них будут наблюдаться различные спектральные характеристики. Хакер может измерить цвет фотона, но не его поляризацию [4].

8. Атака на псевдослучайные числа. Если отправитель использует квантовый генератор псевдослучайных чисел, то хакер может подобрать и применить тот же алгоритм формирования последовательности ПСЧ и получить настоящую последовательность битов [8].

Результаты исследования и их обсуждение

Возникают новые идеи и воплощаются новые алгоритмы и детекторы, стойкие ко многим видам атак. Взломать квантовую криптографию «задним числом» невозможно, и найденные дыры в реализациях не влияют на защищенность уже переданных данных. Зависит ли взломоустойчивость квантовой криптосистемы от её реализации? Скорее да, так как разработаны взломоустойчивые устройство-независимые системы [1].

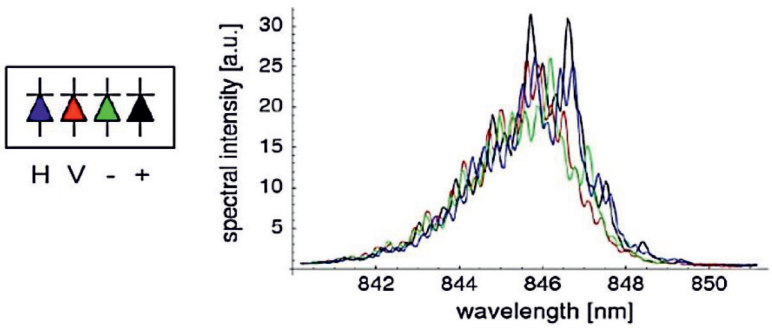

Рис. 4. Схема применения квантового алгоритма распределения ключей

Заключение

Сегодня не существует абсолютно надёжной и защищенной криптосистемы и/или линии связи, как неквантовой, так и квантовой, и пока не представляется возможным реализовать её на практике из–за существования многочисленных уязвимостей [9]. Любая новая технология, в том числе и квантовая криптография, имеет как свои преимущества, так и свои недочёты – уязвимости, которые квалифицированный хакер сможет использовать в своих целях.

Список литературы

1. Макаров В.В. Все важные секреты перестанут быть секретами в будущем // Российский Квантовый Центр // Хайтек. 2019. [Электронный ресурс]. URL: https://yandex.ru/news/story/Vse_vazhnye_sekrety_perestanut_byt_sekretami_v_budushhem_Vadim_Makarov_RKC__o_kvantovoj_kriptografii_dyrakh_v_sistemakh_i_atakakh_na_sputniki--a4f5008ffb5a29670102fba192f72517?lang=ru (дата обращения: 09.05.2020).

2. Принцип неопределённости Гейзенберга // Элементы. Физика. 200 законов мироздания. 2020. [Электронный ресурс]. URL: https://elementy.ru/trefil/21096/Printsip_neopredelennosti_Geyzenberga (дата обращения: 09.05.2020).

3. Принцип неопределённости // Википедия. Свободная энциклопедия. 2020. [Электронный ресурс]. URL:https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF_%D0%BD%D0%B5%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%91%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D0%B8 (дата обращения: 09.05.2020).

4. Действительно ли надёжна квантовая криптография? // Хабр. Блог компании Toshiba. 2020. [Электронный ресурс]. URL: https://habr.com/ru/company/toshibarus/blog/444502/ (дата обращения: 09.05.2020).

5. RSA // Википедия. Свободная энциклопедия. 2020. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/RSA (дата обращения: 09.05.2020).

6. Актаева А.У., Байкенов А.А., Галиева Н.Г., Асанова К., Байман Г., Шатенова Г. Квантовая информация: методы защиты информации // Современные информационные технологии и ИТ–образование. 2016. Т. 12. №2. [Электронный ресурс]. URL: http://sitito.cs.msu.ru/index.php/SITITO/article/view/21/32 (дата обращения: 09.05.2020).

7. Серикова Ю.И., Малыгина Е.А. Уязвимости криптографических систем с различными протоколами квантового распределения ключа и ключевая роль биометрии в квантовой криптографии // Universum: технические науки. 2017. № 11 (44). [Электронный ресурс]. URL: https://docs.google.com/viewer?url=http://7universum.com/pdf/tech/11(44)/Serikova.pdf (дата обращения: 09.05.2020).

8. Филяк П.Ю., Ермолин А.Н. Квантовые технологии в обеспечении информационной безопасности // Информация и безопасность. 2019. Т. 22. № 4 (4). С. 507–516.

9. Глейм А. Абсолютная защита: что такое квантовые коммуникации и как они работают // ITMO.NEWS. 2015. [Элетронный ресурс] URL: https://news.itmo.ru/ru/archive/archive2/news/5070/ (дата обращения: 09.05.2020).