АНАЛИЗ СОВРЕМЕННЫХ ФИШИНГОВЫХ АТАК И МЕТОДОВ ЗАЩИТЫ ОТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В. Д. Барковский, В. А. Федоренко

Белорусский государственный университет информатики и радиоэлектроники, г. Минск

Основной целью данной статьи является анализ принципов квантовой криптографии, ее преимуществ и перспектив внедрения в сферу кибербезопасности.

Ключевые слова: квантовая криптография, квантовое распределение ключей, фотон, кубит, протокол BB84.

ANALYSIS OF MODERN PHISHING ATTACKS AND METHODS OF PROTECTION AGAINST SOCIAL ENGINEERING

V. D. Barkovsky, V. A. Fedorenko

Belarusian state university of informatics and radioelectronics, Minsk

The main objective of this article is to analyze the principles of quantum cryptography, its advantages, and the prospects for its implementation in the field of cybersecurity.

Keywords: quantum cryptography, quantum key distribution, photon, qubit, BB84 protocol.

В отличие от традиционной криптографии, основанной на математике, квантовая криптография полагается на физику и использует свойства квантовых частиц, таких как фотоны, для обмена ключами и защиты передачи данных от подслушивания или подделки. Фотоны представляют собой двоичные кубиты [2].

Квантовая криптография основывается на фундаментальных принципах квантовой физики, таких как:

– принцип неопределенности Гейзенберга – любое измерение состояния квантовой системы приводит к ее изменению. Это позволяет мгновенно обнаружить попытку перехвата данных;

– принцип суперпозиции – квантовые частицы могут находиться в нескольких состояниях одновременно, что усложняет задачу взлома;

– эффект запутанности – изменение состояния одной частицы моментально отражается на другой, независимо от расстояния между ними.

Одним из основных элементов квантовой криптографии является квантовый канал связи, который обеспечивает надежную передачу квантового состояния между двумя сторонами.

Квантовая криптография предлагает несколько преимуществ по сравнению с традиционными криптографическими методами:

– обеспечивает безопасность, поскольку опирается на фундаментальные принципы квантовой механики, обеспечивающие безопасность. Это гарантирует, что ни один злоумышленник не сможет перехватить или изменить зашифрованные данные, не будучи обнаруженным;

– позволяет безопасно распространять ключи шифрования с помощью КРК, гарантирующее, безопасный обмен ключами и не может быть перехвачен третьей стороной. Это устраняет риск перехвата или угадывания ключей, существующий в традиционных методах;

– считается ориентированной на будущее, поскольку неуязвима перед потенциальными достижениями в области квантовых вычислений, которые могут нарушить традиционные методы шифрования;

– используя квантовые ключи, гарантирует, что отправитель и получатель, а также любые посредники могут безопасно аутентифицировать друг друга. Это помогает предотвратить несанкционированный доступ и защищает от атак типа «человек посередине».

В целом, преимущества квантовой криптографии заключаются в ее способности обеспечивать надежную защиту, безопасное распределение ключей, защиту от достижений квантовых вычислений в будущем и надежные механизмы аутентификации [2].

Потенциальные недостатки и ограничения, связанные с квантовой криптографией, включают следующее:

– протоколы КРК ограничены максимальным расстоянием, на котором они могут быть реализованы. Это связано с потерей квантовых состояний через передающую среду;

– скорость распространения ключей значительно медленнее, чем в классической криптографии;

– стоимость систем квантовой криптографии может быть значительно выше по сравнению с традиционными криптографическими методами. Ожидается, что по мере развития технологии и ее более широкого использования стоимость будет снижаться.

Современные исследования в области квантовой криптографии сосредоточены на развитии квантовых сетей и улучшении протоколов распределения квантовых ключей (QKD). Наиболее известные протоколы, такие как BB84 и E91, уже проде-

монстрировали свою эффективность в лабораторных условиях и в ограниченных коммерческих проектах.

Недавние прорывы в области квантовых ретрансляторов позволяют расширить дальность передачи квантовых сигналов, что является важным шагом к созданию глобальных квантовых сетей. Такие сети обещают стать основой для безопасной передачи данных на большие расстояния без риска перехвата. Кроме того, ведутся работы по созданию спутниковых квантовых сетей, которые смогут обеспечить безопасную связь на уровне целых континентов.

Квантовая криптография представляет собой одно из самых перспективных направлений в области кибербезопасности.

Литература

1. Основы квантовой криптографии. – URL: https://na-journal.ru/62023-informacionnye-tekhnologii/5918-osnovy-kvantovoj-kriptografii (дата обращения: 13.10.2025).
2. Роль квантовой криптографии в будущем кибербезопасности. – URL: https://cyber-leninka.ru/article/n/rol-kvantovoy-kriptografii-v-buduschem-kiberbezopasnosti/viewer (дата обращения: 13.10.2025).