ИННОВАЦИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ

Герман А.А., студент

Белорусский государственный университет информатики и радиоэлектроники,
Институт информационных технологий,
г. Минск, Республика Беларусь

Савенко А.Г. – маг. техн. наук, ст. препод. каф. ИСиТ

Данная работа посвящена исследованию и анализу технологий криптографии. В работе рассмотрены основные угрозы безопасности данных, ключевые методы шифрования такие как RSA и SSH, а также новые перспективные направления такие как квантовая криптография и биометрические криптографические системы. Кроме этого, рассмотрены инновационные подходы к защите данных, а именно использование искусственного интеллекта.

Всю историю человек стремился создать наиболее надёжный способ сохранения данных. Хищение информации всегда являлось важной проблемой. В настоящее время эра цифровых технологий принесла новый уровень сложности в защиту данных.

Кибератаки – это попытки злоумышленника получить доступ к данным, украсть, изменить или уничтожить их. На данный момент существуют десятки видов кибератак. Только за последний год (2023) их число увеличилось на 11% по сравнению с предыдущим годом. Наиболее распространёнными являются следующие кибератаки: фишинг, DDos-атаки, использование вредоносного ПО [1].

Фишинг – мошенничество, направленное на получение секретной информации путём обмана владельца, с использованием цифровых средств.

Наиболее известными фишинг атаками является мошенничество с Bank Crelan и с Facebook и Google. В результате первой атаки были украдены 78 миллионов долларов, а во время второй более 120 миллионов.

DDoS-атаки направлены на то, чтобы сделать цифровой ресурс недоступным для обычных пользователей. Злоумышленники направляют на сайт огромное количество запросов, в результате чего те не выдерживают нагрузки и перестают отвечать. Одна из самых мощных атак за последнее время была организована на Google в августе 2023 года. Число запросов составило 398 в секунду.

Вредоносное ПО – это любое программное обеспечение, цель которого заразить ваше устройство вирусом. При помощи него возможно провести огромное количество видов кибератак. Одной из таких является Ransomware. Самая мощная атака данного типа – «WannaCry», была проведена в 2017 году. В результате неё было заражено 300 тысяч компьютеров в 150 странах мира.

Необходимость в сокрытии и защите информации приводит к созданию различных методов шифрования. Криптографическая история прошла длинный путь от шифра цезаря и квадрата Полибия, до современных методов шифрования таких как AES, RSA, SHA.

AES – один из самых популярных алгоритмов шифрования. Он является стандартом для государственных организаций в США и рекомендуется во всём мире. Такое внимание обусловлено его высокой криптостойкостью. Шифр был продемонстрировал высокую устойчивость к атакам.

Шифр RSA также является одним из самых надёжных на данный момент. Это ассиметричный алгоритм шифрования, разработанный в 1976 году. Принцип работы основывается на использовании двух ключей, один из которых предназначен для шифрования, другой для дешифрования.

SHA – это алгоритм, предназначенный для создания уникальных хеш-функций, неподлежащих расшифровки. Наиболее распространённым и криптостойким является алгоритм SHA-256. И хотя на данный момент был разработан SHA-3, предпочтение отдаётся более устаревшим алгоритмам, поскольку использование новых требует серьёзной модернизации в существующих системах.

Помимо классических способов шифрования существенно начали развиваться и исследоваться новые области защиты данных, а именно квантовая криптография и биометрические криптографические системы.

На данный момент квантовая криптография один из самых перспективных способов защиты данных. В своей работе данный метод использует основы квантовой физики и является более надёжным, чем классическая криптография.

Одним из ключевых принципов квантовой криптографии является невозможность перехвата данных без уведомления об этом. При попытке хищения данных они будут изменяться, что, в свою очередь, будет заметно при получении. Данное правило основано на принципе неопределённости Гейзенберга. Он состоит в том, что невозможно одновременно точно измерить импульс и положение частицы, точно так же, как нельзя перехватить данные без их изменения.

Несмотря на высокую надёжность квантовых систем безопасности, использование их на данный момент ограниченно. Это связано в первую очередь со всё ещё продолжающимися

исследованиями. В мире существует несколько организаций, которые занимаются активным изучением данной области. Среди них IBM, Mitsubishi, Toshiba, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт. Более того, применение квантовых технологии требует больших затрат и специального оборудования [2].

Тем не менее, квантовая криптография не теряет своих перспектив на будущее. Сегодня уже существует опыт по созданию компьютерной сети, защищенной методами квантовой криптографии. Это единственная сеть в мире, которую невозможно взломать. Кроме этого, в условиях постоянно развивающихся цифровых технологий в будущем классические методы шифрования такие как AES и RSA потеряют свою неуязвимость перед квантовыми системами взлома.

Не менее инновационным и молодым направлением можно назвать биометрические криптографические системы. Данный метод в своей работе использует биометрические данные такие как: голос, отпечаток пальцев, ДНК. Принцип основан на индивидуальности биологического кода, что позволяет создавать уникальные ключи шифрования, которые невозможно подделать или воспроизвести. Данный методы аутентификации имеет преимущество перед другими системами, поскольку биометрические признаки трудно фальсифицировать, а также для аутентификации требуется присутствие владельца [3].

Помимо защиты от несанкционированного доступа биометрия стала применяться в качестве источника материала для создания ключей. В зависимости от цели криптозащиты можно выделить несколько направление биометрических криптографических систем: системы с освобождением ключа, системы со связыванием ключа, системы с генерацией ключа. Последняя является наиболее перспективной.

Несмотря на высокую надёжность в биометрических системах присутствуют свои сложности. За последние несколько лет было разработано множество методов генерации ключей. Однако, как показала практика, длина ключа очень мала в силу ограниченности уникальных биометрических признаков. Кроме этого, криптография требует точного знания ключа, а биометрические данные в свою очередь всегда имеют погрешность при воспроизведении в цифровом виде.

Тем не менее биометрические криптографические системы продолжают развиваться и совершенствоваться.

Активное развитие искусственного интеллекта расширило его применение в различных областях, в том числе и в криптографии. Он играет значительную роль в усовершенствовании, анализе и разработке криптосистем. Способность искусственного интеллекта обрабатывать большие объёмы данных и обучаться на ошибках делает его идеальным инструментом.

Одной из основных областей применения искусственного интеллекта являются анализ алгоритма шифрования. Помимо этого, искусственный интеллекта используют в создании криптографических алгоритмов.

Интеграция искусственного интеллекта в существующие системы безопасности может значительно повысить защиту данных.

Многообещающим направлением является сочетание искусственного интеллекта и квантовой криптографии.

Несмотря на то, что эти новые области ещё не изучены достаточно хорошо, многие компании начинают активно испытывать и внедрять инновационные технологии в нашу жизнь. Стартап «Deep Instinct» использует машинное обучение для предотвращения кибератак. Проекты «Google's Project Quantum» и «IBM Q» разрабатывают алгоритм PQC, который сможет выстоять против атак квантового компьютера. Компания BioCatch при помощи искусственного интеллекта проводит анализ поведенческих биометрических данных, таких как способ взаимодействия пользователя с устройством, для идентификации и предотвращения мошенничества.

Информационная безопасность продолжает оставаться одной из главных проблем нашего времени. Развитие методов защиты данных приводит к созданию новых способов её хищения. В современном цифровом мире квантовые технологии и искусственный интеллект выводят кибератаки на новый уровень опасности. Возрастает необходимость не просто улучшать существующие методы защиты данных, но также создавать новые.

Список использованных источников:

1. Наиболее распространенные типы кибератак // [Электронный ресурс] – Режим доступа: https://www.keepersecurity.com/blog/ru/2023/08/30/the-most-common-types-of-cyberattacks/ – Дата доступа: 17.03.2024.

2. Квантовая криптография / шифрование // [Электронный ресурс] – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_(%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)– Дата доступа: 22.03.2024.

3. Биометрические методы в криптографии: проблемы и перспективы // [Электронный ресурс] – Режим доступа: https://www.lastmile.su/journal/article/4013 – Дата доступа: 22.03.2024.