

УДК 004.056

БУДУЩЕЕ БЕЗОПАСНОСТИ И УСТОЙЧИВОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Эргашев Д. Х., студент гр. МИЦЭ-21, 2 курс СЭИ,
Научный руководитель: Щепеткин Е. Н., к.т.н., доцент
Уральский государственный лесотехнический университет,
г. Екатеринбург

Аннотация: Несмотря на наличие продвинутых программ и механизмов безопасности современное развитие технологий нуждается в повышении мер безопасности и устойчивости информационных систем. В данной статье будет рассмотрены ключевые тенденции в области защиты данных, перспективы использования квантовой криптографии, автоматизация и улучшения кибербезопасности с применением искусственного интеллекта и машинного обучения, а также биометрические методы аутентификации и уязвимости.

Ключевые слова: Квантовая криптография, защита данных, информационные системы.

Криптография является основным математическим методом и инструментом обеспечения конфиденциальности, целостности и защиты данных в современных информационных системах. В современной криптографии используются открытые алгоритмы шифрования. Самые распространённые алгоритмы – это симметричные и ассиметричные (AES, RSA) и хеш-функции, которые основаны на математических вычислениях, сложность которых определяет их стойкость. Однако развитие квантовых компьютеров, так как квантовые вычисления могут разложить большие числа на множители значительно быстрее, чем классические методы, что делает существующие алгоритмы уязвимыми [1].

В квантовой криптографии используются основные свойства квантовой механики, такие как суперпозиция и квантовая запутанность, для создания безопасных систем передачи информации. Одним из ключевых методов квантовой криптографии является неопределённость поведения квантовой системы, выраженная в принципе неопределённости Гейзенберга, то есть невозможно одновременно измерить один параметр фотона, не изменив другой. В протоколе BB84, предложенном Чарльзом Беннетом и Жилем Брассаром в 1984 году, две стороны передают фотоны в случайных поляризациях.

Одним из главных преимуществ квантовой криптографии является то, что её свойство принципиально неуязвимость к взлому. Традиционные алгоритмы криптографии могут быть скомпрометированы с развитием квантовых

компьютеров. Но несмотря на высокую степень защиты у квантовой криптографии есть технические ограничения и одним из ограничений является высокая стоимость оборудования, которая необходима для передачи квантовых ключей. Кроме того, современные квантовые сети пока только способны передачи фотонов на ограниченные расстояния.

В последние годы компании вкладывают в развитие квантовых сетей огромные средства, потому что квантовая криптография может стать основной для создания глобального квантового интернета, которого практически невозможно будет взломать. Уже сегодня Китай успешно протестировал квантовую передачи данных через спутник Micius [2].

Развитие искусственного интеллекта (ИИ) и машинного обучения (МО) существенно влияет на будущее в сфере кибербезопасности информационных систем и подходы к их защите. ИИ активно используется для разработки систем способных, а режиме реальном времени идентифицировать мошеннические схемы фильтровать спам сообщения и нейтрализовать киберугрозы. Алгоритмы машинного обучения анализирует огромные объемы данных и основной особенностей машинного обучения при предотвращении киберугроз является использование алгоритмов, которые способны обучаться на исторических данных и делать прогнозы на основе текущих данных, которые превосходит традиционные методы предотвращения киберугроз.

Машинное обучение также применяется для мониторинга и анализа поведения пользователей в информационных системах. Такие алгоритмы как Random Forest и Gradient Boosting способны классифицировать данные обнаруживать аномалии на основе активности и сетевого трафика или на основе активности пользователя. Глубокое обучение нейронные сети такие как рекуррентные нейронные сети (RNN) и сверточные нейронные сети (CNN) применяется для анализа сложных паттернов в данных в режиме реального времени.

Автоматизация обнаружения процессов киберугроз с использованием ИИ и МО представляет значительные преимущества включая высокая точность обнаружения, высокая скорость реакции на угрозы и снижение нагрузки на специалистов. Однако существуют ряд рисков ошибки в алгоритмах некачественное обучение моделей ложные срабатывание что требует тщательного подхода к внедрению этих технологий. Биологические методы аутентификации предлагают революционный подход к защите и доступ информации используя уникальные физиологические характеристики для идентификации личности.

Биологические методы аутентификации используют распознавание лиц, отпечатки пальцев, голосовую идентификацию. Они представляют удобные и эффективные способы подтверждения личности что значительно повышает уровень безопасности по сравнению с традиционными паролями и пин кодами. Все биометрические системы работают по одному и тому же принципу первым

этапе они регистрирует биометрические данные пользователей вносят шаблон в базу и при аутентификации проверяется данные с базой. Несмотря на уникальность биометрических методов аутентификации они [3].

имеют уязвимости. К ним относятся ошибки первого рода атаки подделки и второго рода утечки биометрических шаблонов из баз данных.

Известные случаи утечки биометрических данных:

В 2025 году произошла утечка данных в США в Управление по кадровым вопросам из-за чего было скомпрометировано отпечатки пальцев миллионов сотрудников.

В 2019 году исследователи обнаружили уязвимости в системе биометрической безопасности, используемой в Великобритании что дала доступ к данным отпечатков пальцев и распознавания лиц [4].

Эти случаи утечек подчеркивает необходимость разработки более надежных методов защиты биометрических данных и постоянного совершенствования технологий аутентификации.

Рассмотренные технологии – квантовая криптография, искусственный интеллект и биометрические методы аутентификации оказывают значительное влияние на будущее безопасности информационных систем. Квантовая криптография предлагает новый уровень защиты данных используя принципы квантовой механики что особенно актуально в эпоху развития квантовых вычислений. Использование и интеграция систем искусственного интеллекта при выявлении угроз в информационных системах позволяет не только анализировать и предсказывать угрозы, но и разрабатывать новые методы шифрования повышая общую устойчивость инструкторы. Биометрические методы аутентификации, основанные на уникальных характеристиках пользователей, обеспечивают более надежные способы идентификации снижая риски, связанные с паролями.

Для повышения устойчивости и безопасности информационных систем рекомендуется принимать слабеющие шаги:

Внедрения квантово-устойчивых алгоритмов шифрования. Подготовка к возможным угрозам со стороны квантовых компьютеров требует разработки и применение алгоритмов устойчивых к их вычислительным мощностям [5].

Использование искусственного интеллекта для мониторинга и реагирования на угрозы. ИИ способен анализировать большие объемы данных в реальном времени выявляя аномалии предсказывая потенциальные атаки, что повышает оперативность и эффективность мер безопасности.

Обеспечение защиты биометрических данных:

Необходимо внедрять меры по защите биометрической информации от утечки включая шифрование и безопасное хранение чтобы предотвратить несанкционированный доступ и использование.

Комплексный подход, объединяющий эти рекомендации позволить создать более надежные и устойчивые информационные системы, способные эффективно противостоять современным и будущим киберугрозам [6].

Список литературы:

1.Использование машинного обучения для обнаружения киберугроз в реальном времени [Электронный ресурс] // CISOCLUB.

2.Принципы работы и уязвимости биометрических систем аутентификации / И. П. Пересыпкин, Л. Е. Мартынова, К. Е. Назарова [и др.]. – Текст : непосредственный // Молодой ученый. – 2016.

3.Биометрические системы аутентификации: вызовы конфиденциальности и безопасности данных [Электронный ресурс] // Научная аналитика. – URL: <https://na-journal.ru/4-2024-informacionnye-tekhnologii/10818-biometricheskie-sistemy-autentifikacii-vyzovy-konfidencialnosti-i-bezopasnosti-dannyh>