УДК 004.056

Иванов И.П., Хасанов Р.Р., Ишмаков Т.М.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Статья посвящена современным технологиям информационной безопасности (ИБ), которые помогают защищать данные

и системы от киберугроз. Рассматриваются системы обнаружения и предотвращения вторжений, анализ больших данных, машинное обучение, блокчейн и квантовая криптография. Особое внимание уделяется их роли в противодействии актуальным угрозам, а также примерам из практики, иллюстрирующим их эффективность и ограничения.

Ключевые слова: информационная безопасность, кибербезопасность, системы обнаружения вторжений, анализ больших данных, машинное обучение, блокчейн, квантовая криптография.

Информационная безопасность (ИБ) – это комплекс мер и технологий, направленных на защиту данных, систем и сетей от несанкционированного доступа, утечек и атак. В условиях цифровизации, когда объемы данных стремительно растут, а киберугрозы становятся все более изощренными, традиционные методы защиты, такие как пароли или антивирусы, теряют свою эффективность. Современные технологии, включая машинное обучение, анализ больших данных, блокчейн и квантовую криптографию, открывают новые горизонты для обеспечения ИБ. Эта статья раскрывает суть этих технологий, их преимущества и вызовы, а также демонстрирует, как они применяются для защиты информации.

Системы обнаружения и предотвращения вторжений (IDS/IPS) – это ключевые инструменты для защиты сетей. Они отслеживают сетевой трафик и выявляют подозрительную активность. Традиционные системы опираются на сигнатурный анализ, сравнивая данные с известными шаблонами атак. Однако такие методы не справляются с новыми или сложными угрозами, такими как целевые атаки (APT).

Современные системы, или NGIPS (Next-Generation IPS), используют более продвинутые подходы. Они анализируют поведение пользователей и устройств, выявляя аномалии с помощью машинного обучения. Например, российская компания Positive Technologies разработала PT Network Attack Discovery (PT NAD). Эта система анализирует сетевой трафик в реальном времени, обнаруживает скрытые угрозы и автоматически блокирует подозрительные действия, минимизируя ущерб. Такие решения особенно важны, учитывая, что большинство атак начинается с кражи учетных данных.

IDS/IPS нового поколения демонстрируют, как ИБ переходит от реактивной защиты к проактивной, способной предугадывать и предотвращать угрозы до их реализации.

Большие данные – это огромные объемы информации, генерируемые сетями, устройствами и пользователями. В контексте ИБ они становятся ценным ресурсом для выявления угроз. Технологии анализа больших данных позволяют обрабатывать логи, трафик и другие данные в реальном времени, находя скрытые закономерности и аномалии.

Примером является платформа InfoWatch Traffic Monitor от российской компании InfoWatch. Она собирает данные с серверов, рабочих станций и

сетевых устройств, анализируя поведение пользователей и приложений. Это помогает выявить подозрительные действия, такие как несанкционированный доступ, и предсказать возможные атаки. Гибкость платформы позволяет настраивать алгоритмы под конкретные угрозы, что делает ее эффективной против новых видов атак.

Машинное обучение – это технология, которая позволяет системам обучаться на данных и улучшать свои способности без явного программирования. В ИБ машинное обучение используется для выявления аномалий, предсказания атак и автоматизации реагирования.

Российская компания Group-IB создала систему Threat Intelligence & Attribution, которая применяет машинное обучение и глубокое обучение для анализа киберугроз. Система распознает паттерны, характерные для атак, включая угрозы нулевого дня, которые неизвестны традиционным антивирусам. Она адаптируется к новым видам атак, обеспечивая защиту в реальном времени. Например, система может автоматически изолировать зараженное устройство, предотвращая распространение угрозы.

Машинное обучение делает ИБ более интеллектуальной, позволяя системам не только реагировать на известные угрозы, но и предвидеть новые, что особенно важно в условиях стремительно эволюционирующих кибератак.

Блокчейн – это технология, основанная на децентрализованной базе данных, где информация хранится в виде цепочки блоков, защищенных криптографией. В ИБ блокчейн применяется для обеспечения целостности данных, управления идентификацией и защиты транзакций.

Российская платформа Waves Enterprise использует блокчейн для защиты данных от изменений и утечек. Каждый блок содержит информацию о предыдущем, а криптографические подписи гарантируют неизменность записей. Это делает технологию идеальной для управления цепочками поставок, финансовых транзакций или персональных данных. Например, блокчейн может создать систему, где пользователи сами контролируют доступ к своим данным, снижая риск компрометации.

Блокчейн повышает доверие к системам, устраняя необходимость в посредниках и обеспечивая прозрачность, что делает его перспективным инструментом ИБ.

Квантовая криптография использует законы квантовой физики для создания сверхнадежных систем шифрования. Основной метод – квантовое распределение ключей (QKD), которое позволяет двум сторонам безопасно обмениваться ключами. Любая попытка перехвата ключа нарушает квантовое состояние, что мгновенно обнаруживается.

В России компания QRate разрабатывают компактные QKD-системы, которые можно интегрировать с традиционными методами шифрования. Такие решения устойчивы даже к атакам с использованием квантовых компьютеров, которые могут взломать классические алгоритмы. Исследователи также работают над увеличением дальности передачи

данных и снижением помех, чтобы сделать технологию доступной для массового использования.

Квантовая криптография представляет собой будущее ИБ, обещающее беспрецедентный уровень защиты данных в эпоху квантовых технологий.

Несмотря на прогресс, технологии ИБ сталкиваются с рядом трудностей:

- нехватка специалистов: квалифицированных экспертов по кибербезопасности недостаточно для удовлетворения спроса;
- сложность интеграции: новые технологии требуют адаптации к существующим системам, что может быть дорого и трудоемко;
- эволюция угроз: киберпреступники постоянно разрабатывают новые методы атак, требующие регулярного обновления защитных систем;
- высокая стоимость: внедрение передовых решений, таких как QKD, требует значительных инвестиций.

Эти вызовы подчеркивают необходимость комплексного подхода, сочетающего технологии, обучение персонала и организационные меры.

Информационная безопасность – это не просто набор технологий, а динамично развивающаяся область, требующая постоянной адаптации к новым вызовам. Системы IDS/IPS, анализ больших данных, машинное обучение, блокчейн и квантовая криптография формируют современный арсенал защиты данных и систем. Они позволяют не только реагировать на угрозы, но и предвидеть их, минимизируя риски. Однако ни одна технология не может обеспечить абсолютную безопасность в одиночку. Эффективная защита требует сочетания инноваций, квалифицированных специалистов и осведомленности пользователей. В эпоху цифровизации ИБ становится основой устойчивого развития организаций и общества в целом.

Список использованных источников:

1. Positive Technologies. PT Network Attack Discovery. URL: https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/ (дата обращения 10.04.2025).

2. InfoWatch. InfoWatch Traffic Monitor. URL: https://www.infowatch.ru/products/dlp-sistema-traffic-monitor (дата обращения 10.04.2025).

3. Group-IB. Threat Intelligence & Attribution. URL: https://www.group-ib.com/products/threat-intelligence/ (дата обращения 10.04.2025).

4. Waves Enterprise. URL: https://doc.web3tech.ru/ru/latest/index.html (дата обращения 10.04.2025).

5. QRate. Аппаратно-программный комплекс квантового распределения ключей (КРК). URL: https://goqrate.com/projects/qrate_qkd312/S (дата обращения 10.04.2025).

Ivanov I. P., Khasanov R. R., Ishmakov T. M.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

INFORMATION SECURITY TECHNOLOGIES

Abstract. The article is devoted to modern information security (IS) technologies that help protect data and systems from cyber threats. Intrusion detection and prevention systems, big data analysis, machine learning, blockchain and quantum cryptography are considered. Special attention is paid to their role in countering current threats, as well as practical examples illustrating their effectiveness and limitations.

Keywords: information security, cybersecurity, intrusion detection systems, big data analysis, machine learning, blockchain, quantum cryptography.