УДК 004.056

Ганиев М.Р., Ефимов И.О., Каримуллин Т.Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

СОВРЕМЕННЫЕ МЕТОДЫ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Современные методы повышения уровня информационной безопасности играют важную роль в обеспечении защиты данных и ресурсов на всех уровнях информационной системы. В статье рассматриваются актуальные подходы и технологии, используемые для защиты информации в условиях постоянно растущих угроз и уязвимостей.

Ключевые слова: управление доступом, системы обнаружения и предотвращения вторжений, облачные вычисления, искусственный интеллект и машинное обучение.

Информационная безопасность (ИБ) одна важнейшей составляющей функционирования организаций, различных государственных структур и отдельных пользователей. Сложность современных информационных систем с требует применения новых методов и технологий для защиты от разнообразных угроз. Эти угрозы могут исходить как от внешних злоумышленников, так и от внутренних нарушителей безопасности [1]. Рассмотрим далее комплексный обзор современных подходов, используемых в ИБ. Как известно, основные задачи ИБ – это обеспечение защиты данных и ресурсов от различных угроз, включая внешние и внутренние, которые базируются на базовых элементах: конфиденциальности, т.е. защите информации от несанкционированного доступа; обеспечение целостности, т.е. обеспечение неизменности и сохранности даны; обеспечение доступности, т.е. обеспечение доступа к информации и ресурсам.

Рассмотрим далее основные методы ИБ.

Криптография. Используется для защиты данных с помощью шифрования данных, цифровых подписей и хеширования.

Управление доступом. Контролирует доступ к информации на основе принятых в организации политик безопасности, включая мандатное, дискреционное и ролевое управление.

Системы обнаружения и предотвращения вторжений. Мониторинг и блокировка угроз в режиме реального времени.

Безопасность в облачных вычислениях. Защита данных в облаке с помощью шифрования и методов многофакторной аутентификации.

Искусственный интеллект и машинное обучение. Используются для обнаружения аномалий, прогнозирования атак и автоматического реагирования на различные угрозы.

Системы обнаружения и предотвращения вторжений являются важнейшими инструментами для мониторинга и защиты информационных систем от внешних и внутренних угроз и включают следующие подсистемы:

– система обнаружения вторжений анализирует сетевой трафик и действия пользователей, чтобы выявить подозрительную активность;

– система предотвращения вторжений не только обнаруживают угрозы, но и может предпринимать активные действия для их блокировки, например блокировать атакующие IP-адреса или прерывать подозрительные соединения.

Эти системы являются важными элементами комплексной системы защиты и используются в режиме реального времени для предотвращения кибератак.

С переходом многих компаний и организаций на использование облачных сервисов возникает необходимость защиты данных в облаке. Современные методы обеспечения безопасности в облачных вычислениях включают:

– шифрование данных: защита данных как при хранении в облаке, так и при их передаче;

– многофакторная аутентификация: для повышения уровня защиты от несанкционированного доступа;

– контроль доступа и управление пользователями: использование ролевого и многоуровневого контроля для минимизации рисков.

Современные методы защиты информации активно используют технологии искусственного интеллекта (ИИ) и машинного обучения (МО) [2]. Эти технологии помогают:

– обнаружение аномалий: анализируя большие объемы данных, системы могут выявить необычное поведение, которое может указывать на угрозу;

– прогнозирование атак: используя алгоритмы МО, системы могут предсказывать возможные атаки на основе предыдущих инцидентов;

– автоматическое реагирование на угрозы: ИИ может автоматически принимать меры для предотвращения атак, например блокировать подозрительные IP-адреса или отключать вредоносный трафик.

Рассмотрим далее пути совершенствования методов ИБ. Современные методы обеспечения ИБ требуют комплексного подхода, включающего обновление и адаптацию стратегий защиты [3]. Важна интеграция

различных методов, таких как многофакторная аутентификация, блокчейн-технологии, машинное обучение и искусственный интеллект для обнаружения аномалий и предотвращения атак. Кроме того, важным элементом обеспечения ИБ является обучение и повышение осведомленности пользователей о потенциальных угрозах, что помогает снизить риски, связанные с человеческим фактором. В условиях растущей зависимости от облачных вычислений и мобильных устройств особое внимание следует уделять защите данных в распределенных системах и обеспечению конфиденциальности пользователей [4].

Таким образом, успешная реализация стратегии информационной безопасности требует взаимодействия технологий, процессов и людей, а также постоянного мониторинга и улучшения защиты на всех уровнях.

Список использованных источников:

1. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Мельников А.В. Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия // vestnik-rosnou.ru – 2023. URL: https://vestnik-rosnou.ru/sites/default/files/136_Сложные %20системы %20№ %203 %20ПРОСМОТРОВЫЙ.pdf (дата обращения: 30.04.2025).

2. Исмагилова А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. 2024. № 1(109). С. 178–188.

3. Валеев С.С., Кондратьева Н.В. Особенности проектирования систем безопасности на базе архитектуры нулевого доверия // ivdon.ru – 2023. URL: http://www.ivdon.ru/uploads/article/pdf/IVD_68__8_valeev_kondratyeva_v2.pdf_72458b243f.pdf (дата обращения: 30.04.2025).

4. Валеев С.С., Кондратьева Н.В., Мельников А.В. Архитектура предприятия и архитектура нулевого доверия. // info-secur.ru – 2023. URL: https://www.info-secur.ru/index.php/ojs/article/download/413/371/ (дата обращения: 30.04.2025).

Ganiev M.R., Karimullin T.F., Efimov I.O.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

MODERN METHODS OF IMPROVING INFORMATION SECURITY

Abstract. Modern methods of increasing the level of information security play an important role in ensuring the protection of data and resources at all

levels of the information system. The article discusses current approaches and technologies used to protect information in the face of ever-growing threats and vulnerabilities.

Keywords: access control, intrusion detection and prevention systems, cloud computing, artificial intelligence and machine learning.