УДК 004.056:004.738.5

ПРОЕКТИРОВАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ НА ПРИМЕРЕ SAAS-ПРИЛОЖЕНИЯ

Кабильдина А.Ж., Калынюк С.С., Шавкунов Р.
студенты, Факультет Инновационных Технологий, Кафедра кибербезопасности и искуственного интеллекта, Карагандинский технический университет имени Абылкаса Сагинова, г.Караганда, Казахстан

В статье рассматриваются особенности проектирования комплексной системы информационной безопасности предприятия на примере SaaS-приложения. Анализируются угрозы конфиденциальности, целостности и доступности корпоративных данных, возникающие в условиях использования облачных сервисов и удалённого доступа. Представлен сравнительный анализ подходов к построению защиты данных, выявлены преимущества и ограничения современных методов, а также предложены направления оптимизации системы информационной безопасности для SaaS-среды.

Ключевые слова: информационная безопасность, SaaS-приложение, корпоративные данные, управление доступом, защита данных, конфиденциальность, целостность информации, доступность информации, киберугрозы, утечка данных, аутентификация, шифрование, облачные сервисы, контроль инцидентов, мониторинг безопасности, мультифакторная аутентификация, DevSecOps.

Введение

Современные предприятия активно используют SaaS-приложения для автоматизации бизнес-процессов, управления клиентской базой и обработки финансовой информации. Облачные сервисы обеспечивают удобство и масштабируемость, однако создают дополнительные риски для информационной безопасности: утечка данных, несанкционированный доступ, взлом учетных записей и сбои в работе сервисов.

Комплексная защита SaaS-среды требует интеграции технических, организационных и процедурных мер. Стандарты ISO/IEC 27001 и ISO/IEC 27701, а также подходы DevSecOps, обеспечивают управление рисками, контроль доступа, шифрование данных и мониторинг инцидентов. Цель данной статьи заключается в анализе проектирования комплексной системы информационной безопасности для SaaS-приложений и разработке рекомендаций по её совершенствованию.

Основная часть

Информационная безопасность SaaS-приложений - это комплексная задача, включающая защиту корпоративных данных, пользовательской информации и бизнес-процессов от внешних и внутренних угроз. Основные направления защиты включают управление доступом, шифрование, мониторинг инцидентов и интеграцию DevSecOps [1,5].

Многоуровневая аутентификация (MFA), ролевой доступ (RBAC) и принцип наименьших привилегий являются ключевыми инструментами предотвращения несанкционированного доступа [1,4,7]. Например, Atlassian внедрила MFA для всех сотрудников, что позволило снизить число инцидентов безопасности на 60 % [1]. Применение RBAC в SaaS-платформах минимизирует риск случайного или злонамеренного доступа к критическим данным [2].

SaaS-приложения должны использовать шифрование данных как при хранении, так и при передаче (TLS 1.3, AES-256) [5,6,10]. Slack и другие корпоративные платформы реализуют сквозное шифрование сообщений и файлов, обеспечивая соответствие стандартам GDPR и SOC 2 [3,4]. Кроме того, шифрование API-ключей и резервных копий данных снижает риск утечек при нарушении безопасности облачного сервиса [10,11].

Использование SIEM-систем, логирования действий пользователей и регулярного аудита позволяет выявлять подозрительную активность и реагировать на инциденты в кратчайшие сроки [9,11]. В 2023 году исследование Microsoft Azure показало, что централизованный мониторинг снижает время реагирования на инциденты с 48 до 6 часов [3].

Анализ логов и событий в реальном времени позволяет предотвратить распространение угроз и минимизировать ущерб[8,9].Встраивание механизмов безопасности на стадии разработки и CI/CD позволяет выявлять уязвимости ещё до развертывания приложения [12]. Автоматизированное тестирование на SQL-инъекции, XSS и утечки API-ключей помогает минимизировать риски и обеспечивает принцип «безопасность по дизайну» [12].

Сравнительный анализ показывает, что международные компании, применяющие комплексные меры информационной безопасности и соблюдающие стандарты ISO/IEC 27001, ISO/IEC 27002 и CSA Cloud Controls Matrix [5,9], обладают более высокой устойчивостью к кибератакам по сравнению с организациями, ограничивающимися локальными регламентами и минимальными требованиями безопасности [2,4,7].

Для повышения безопасности SaaS-приложений рекомендуется внедрять мультимодальную аутентификацию, объединяющую биометрические методы, токены доступа и поведенческую аналитику, а также использовать технологии искусственного интеллекта для выявления аномальной активности [11,12]. Инструменты TensorFlow, OpenCV и SIEM-платформы позволяют автоматизировать процесс обнаружения угроз и снизить влияние человеческого фактора на безопасность данных [1,10,12]. Комплексная система

информационной безопасности начинается с оценки рисков и выявления уязвимых мест [1,9]. CSA Cloud Controls Matrix позволяет классифицировать угрозы для SaaS, включая SQL-инъекции, XSS, DDoS, компрометацию токенов доступа и утечки данных [9]. Методики риск-менеджмента на основе ISO/IEC 27005 позволяют прогнозировать вероятность инцидентов и оценивать их влияние на бизнес-процессы [5,6].

Аудит и соответствие международным требованиям Регулярный аудит и соответствие стандартам ISO/IEC 27001, ISO/IEC 27002 и SOC 2 обеспечивают контроль за соблюдением корпоративных политик безопасности [5,6,9]. Для SaaS-компаний, работающих с пользователями из ЕС и других стран с строгими правилами защиты данных, критично соблюдение GDPR и локальных законов о персональных данных [5,7]. Это включает права пользователей на удаление и ограничение обработки данных, а также обязательную прозрачность процессов [5].

Кейсы SaaS-платформ и уроки безопасности

- Slack: внедрение сквозного шифрования, баг-баунти и регулярные аудиты позволили минимизировать риск утечек корпоративной переписки [3,4].
- Atlassian: применение MFA и RBAC снизило число инцидентов безопасности на 60 % [1].
- Salesforce: централизованное управление доступом, интеграция DevSecOps и регулярный аудит обеспечивают защиту данных миллионов пользователей [10].

Рекомендации по усилению защиты SaaS

- Внедрение мультимодальной аутентификации, объединяющей биометрию, токены доступа и поведенческую аналитику [11,12];
- Использование искусственного интеллекта и машинного обучения для выявления аномальной активности [1,10];
- Интеграция автоматизированного аудита и SIEM для быстрого реагирования на инциденты [3,9];
- Внедрение DevSecOps и принципа «безопасность по дизайну» на этапе разработки [12].

Применение этих подходов позволяет значительно снизить вероятность утечек, повысить устойчивость SaaS-приложений к современным киберугрозам и укрепить доверие пользователей к корпоративной информационной среде [1,5,9,11].

Заключение

Проектирование комплексной системы информационной безопасности для SaaS-приложений требует сочетания технических решений, организационных мер и постоянного мониторинга. Ключевые угрозы - утечка данных, несанкционированный доступ и технические сбои - требуют проактивного подхода [1,4,5].

Сравнение подходов международных компаний и предприятий СНГ показывает, что высокий уровень защиты достигается через строгие стандарты, многоуровневую аутентификацию и интеграцию DevSecOps, тогда как ограниченные меры повышают риск инцидентов [2,7,9].

Внедрение мультимодальной аутентификации и автоматизированного мониторинга позволит повысить уровень безопасности SaaS-приложений, снизить вероятность утечек и укрепить доверие клиентов к корпоративной информационной среде [11,12].

Список использованной литературы

1. Offering security diagnosis as a service for cloud SaaS applications, Journal of Information Security and Applications, Vol. 44. ScienceDirect
2. Айтхожаева Е., Алимсейтова Ж., Акатаев Н. «Информационная безопасность облачных сервисов», Вестник КазАТК. vestnik.alt.edu.kz
3. Айтхожаева Е., Ким Э. «Стандартизация информационной безопасности облачных сервисов», Вестник КазАТК. vestnik.alt.edu.kz
4. Rohatgi G., Ensuring Secure SaaS: Best Practices and Approaches for Integrating Security to Cloud-Based Applications. jtipublishing.com
5. ISO/IEC 27001-международный стандарт по менеджменту информационной безопасности. ru.wikipedia.org
6. ISO 27000 - серия стандартов по информационной безопасности. ru.wikipedia.org
7. Yandex Cloud. «Информационная безопасность в облачных системах: принципы и методы». yandex.cloud
8. Yandex Cloud. «Безопасность в облаках: исследование и прогнозы». yandex.cloud
9. Документ CSA «Top threats of Cloud Computing v1.0»: анализ модели угроз облачных моделей (SaaS, PaaS, IaaS). scientificjournal.ru
10. Chouhan P.K., Yao F., Yerima S.Y., Sezer S. Software as a Service: Analyzing Security Issues. arxiv.org
11. Hannousse A., Yahiouche S. Securing Microservices and Microservice Architectures: A Systematic Mapping Study. arxiv.org
12. Rexhepi O. Cybersecurity of SaaS Products: Secure-by-Design Engineering and Continuous Assurance. tacje.net

SAAS-ҚОСЫМШАСЫ МЫСАЛЫНДА КӘСІПОРЫННЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІНІҢ КЕШЕНДІ ЖҮЙЕСІН ЖОБАЛАУ.

Мақалада SaaS-қосымша мысалында кәсіпорынның кешенді ақпараттық қауіпсіздік жүйесін жобалау ерекшеліктері қарастырылады. Бұлтты сервистер мен қашықтан қатынауды пайдалану жағдайында туындайтын

корпоративтік деректердің құпиялылығына, тұтастығына және қолжетімділігіне төнетін қауіптерге талдау жасалады. Деректерді қорғауды құру тәсілдеріне салыстырмалы талдау ұсынылып, заманауи әдістердің артықшылықтары мен шектеулері айқындалады, сондай-ақ SaaS ортасы үшін ақпараттық қауіпсіздік жүйесін оңтайландыру бағыттары ұсынылады.

Кілт сөздер: ақпараттық қауіпсіздік, SaaS-қосымша, корпоративтік деректер, қатынауды басқару, деректерді қорғау, құпиялылық, ақпарат тұтастығы, ақпараттың қолжетімділігі, киберқауіптер, деректердің ағып кетуі, аутентификация, шифрлау, бұлтты сервистер, инциденттерді бақылау, қауіпсіздік мониторингі, мультифакторлық аутентификация, DevSecOps.

DESIGNING A COMPREHENSIVE INFORMATION SECURITY SYSTEM FOR AN ENTERPRISE USING A SAAS APPLICATION AS AN EXAMPLE

The article examines the features of designing a comprehensive enterprise information security system using the example of a SaaS application. It analyzes threats to the confidentiality, integrity, and availability of corporate data arising from the use of cloud services and remote access. A comparative analysis of approaches to building data protection is presented, the advantages and limitations of modern methods are identified, and directions for optimizing the information security system for the SaaS environment are proposed.

Keywords: information security, SaaS application, corporate data, access control, data protection, confidentiality, data integrity, information availability, cyber threats, data leakage, authentication, encryption, cloud services, incident management, security monitoring, multi-factor authentication, DevSecOps.

REFERENCES

1. *Offering Security Diagnosis as a Service for Cloud SaaS Applications. Journal of Information Security and Applications*, Vol. 44. ScienceDirect.
2. Aitkhozhaeva, E., Alimseitova, Zh., & Akataev, N. Information security of cloud services. *Bulletin of KazATC*. Available at: vestnik.alt.edu.kz.
3. Aitkhozhaeva, E., & Kim, E. Standardization of information security of cloud services. *Bulletin of KazATC*. Available at: vestnik.alt.edu.kz.
4. Rohatgi, G. *Ensuring Secure SaaS: Best Practices and Approaches for Integrating Security to Cloud-Based Applications.* Available at: jtipublishing.com.
5. *ISO/IEC 27001 — International Standard for Information Security Management.* Available at: ru.wikipedia.org.

6. *ISO 27000 — Series of Information Security Standards.* Available at: ru.wikipedia.org.

7. Yandex Cloud. *Information Security in Cloud Systems: Principles and Methods.* Available at: yandex.cloud.

8. Yandex Cloud. *Cloud Security: Research and Forecasts.* Available at: yandex.cloud.

9. Cloud Security Alliance (CSA). *Top Threats of Cloud Computing v1.0: Analysis of Threat Models for Cloud Services (SaaS, PaaS, IaaS).* Available at: scientificjournal.ru.

10. Chouhan, P. K., Yao, F., Yerima, S. Y., & Sezer, S. *Software as a Service: Analyzing Security Issues.* Available at: arxiv.org.

11. Hannousse, A., & Yahiouche, S. *Securing Microservices and Microservice Architectures: A Systematic Mapping Study.* Available at: arxiv.org.

12. Rexhepi, O. *Cybersecurity of SaaS Products: Secure-by-Design Engineering and Continuous Assurance.* Available at: tacje.net.