QAZAQ JOURNAL OF YOUNG SCIENTIST

2026, Vol.4, No. 4 S (April)

https://qazaqjournal.kz/

УДК 004.056

SAAS ПРИЛОЖЕНИЕ ДЛЯ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Кабильдина А.Ж.[1], Калынюк С.С.[2] , Шавкунов Р.А.[3]
«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 иминимальными 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].

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 [5, 6].

Анализ угроз и мер защиты. Многоуровневая аутентификация (MFA), ролевой доступ (RBAC) и принцип наименьших привилегий являются ключевыми инструментами предотвращения несанкционированного доступа [1, 7]. Например, компания 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) [6, 8]. Slack и другие корпоративные платформы реализуют сквозное шифрование сообщений и файлов, обеспечивая соответствие стандартам GDPR и SOC 2 [9, 10]. Кроме того, шифрование API-ключей и резервных копий данных снижает риск утечек при нарушении безопасности облачного сервиса [8, 11].

Интегральная оценка уровня безопасности. Для количественной оценки защищённости SaaS-приложения предлагается использовать интегральный показатель безопасности S, рассчитываемый на основе взвешенной суммы охваченных угроз и применённых мер:

$$S = \frac{\sum_{i=1}^{n} w_i \cdot c_i}{\sum_{i=1}^{n} w_i} \times 100\%$$

где n-количество рассматриваемых угроз; w_i-весовой коэффициент важности i-й угрозы (определяется экспертным путём на основе ISO/IEC 27005); c_i-коэффициент покрытия угрозы мерами защиты (0-меры отсутствуют, 0,5-меры частичны, 1-полное покрытие). Нормировка позволяет получить значение в диапазоне от 0 до 100%, где 100% соответствует идеальной защищённости. Например, для угрозы «Утечка данных» при $w = 0.4$ и полном покрытии ($c = 1$) вклад составит 0.4, а при отсутствии шифрования ($c = 0$)-0.

Разработка программного инструмента «SaaS Security Assistant». Для практической реализации предложенных подходов создано веб-приложение на базе фреймворка Streamlit (язык Python). Приложение реализует интерактивный калькулятор угроз и мер безопасности, позволяющий пользователю выбрать тип угрозы из выпадающего списка и мгновенно получить описание, рекомендуемые меры защиты, соответствующие стандарты и реальный пример из практики. Данные об угрозах, мерах, стандартах и примерах хранятся в отдельном модуле threats_data.py в виде структурированных словарей.

```
threats = {
    "Утечка данных": {
        "description": "Несанкционированное раскрытие корпоративных или пользовательских данных",
        "measures": [
            "Сквозное шифрование (AES-256, TLS 1.3)",
            "Шифрование API-ключей и резервных копий",
            "Регулярные аудиты и баг-баунти программы"
        ],
        "standards": ["GDPR", "SOC 2", "ISO/IEC 27001"],
        "example": "Slack внедрил сквозное шифрование сообщений и файлов"
    },
    "Несанкционированный доступ": {
        "description": "Злоумышленник получает доступ к учетной записи или системе",
        "measures": [
            "Многоуровневая аутентификация (MFA)",
            "Ролевой доступ (RBAC)",
            "Принцип наименьших привилегий"
        ],
        "standards": ["ISO/IEC 27001", "CSA Cloud Controls Matrix"],
        "example": "Atlassian внедрил MFA - снижение инцидентов на 60%"
    },
    "DDoS-атака": {
        "description": "Перегрузка сервиса с целью нарушения доступности",
        "measures": [
            "Мониторинг трафика в реальном времени",
            "Использование SIEM-систем",
            "Автоматическое реагирование на аномалии"
        ],
        "standards": ["ISO/IEC 27001", "CSA Cloud Controls Matrix"],
        "example": "Microsoft Azure: снижение времени реакции с 48 до 6 часов"
    }
}
general_recommendations = [
    "Внедрение мультимодальной аутентификации",
    "Использование AI/ML для выявления аномалий",
    "Интеграция SIEM для быстрого реагирования",
    "Внедрение DevSecOps"
]
```

```
keywords = [
   "информационная безопасность", "SaaS", "MFA", "RBAC",
   "шифрование", "SIEM", "DevSecOps", "ISO 27001"
]
```

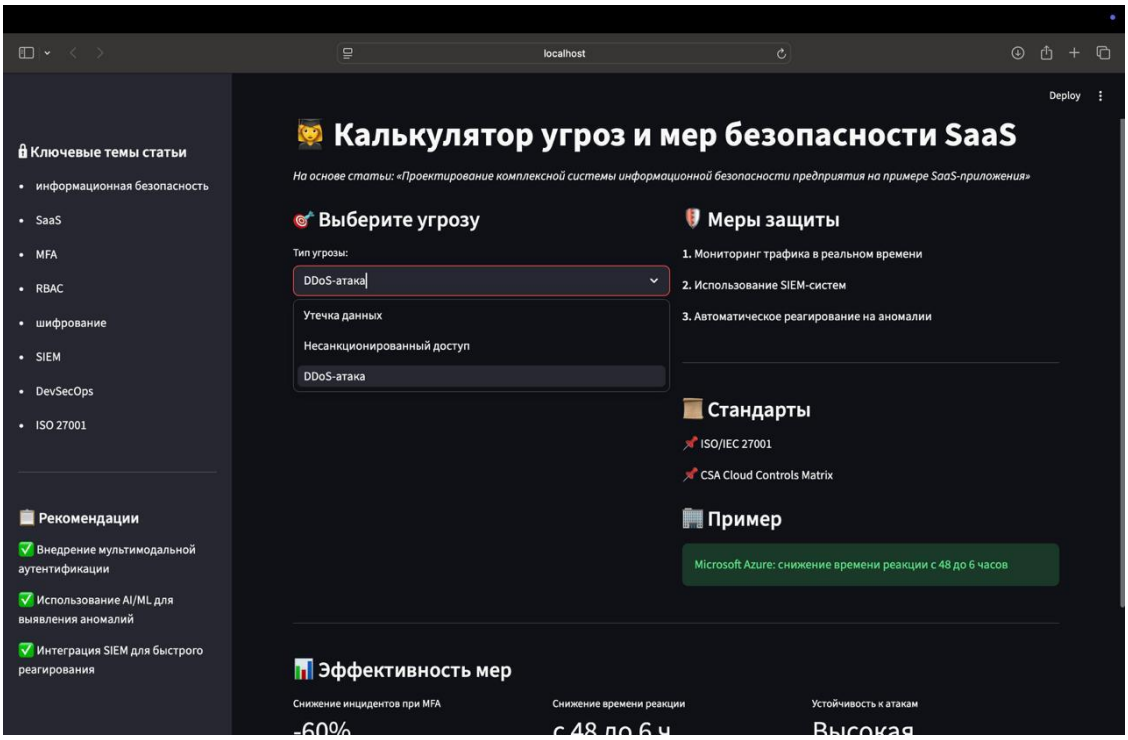

Рисунок 1 – Общий вид веб-приложения «SaaS Security Assistant»

Пользователю доступен выбор трёх типов угроз: «Утечка данных», «Несанкционированный доступ» и «DDoS-атака». При выборе, например, угрозы «DDoS-атака» система отображает меры защиты (мониторинг трафика, использование SIEM, автоматическое реагирование), стандарты (ISO/IEC 27001, CSA Cloud Controls Matrix) и пример из практики Microsoft Azure (рисунок 2).

Аналогичным образом для угрозы «Утечка данных» приложение предлагает меры шифрования (сквозное шифрование AES-256/TLS 1.3, шифрование API-ключей и резервных копий, регулярные аудиты и баг-баунти), стандарты (GDPR, SOC 2, ISO/IEC 27001) и пример из практики компании Slack (рисунок 3).

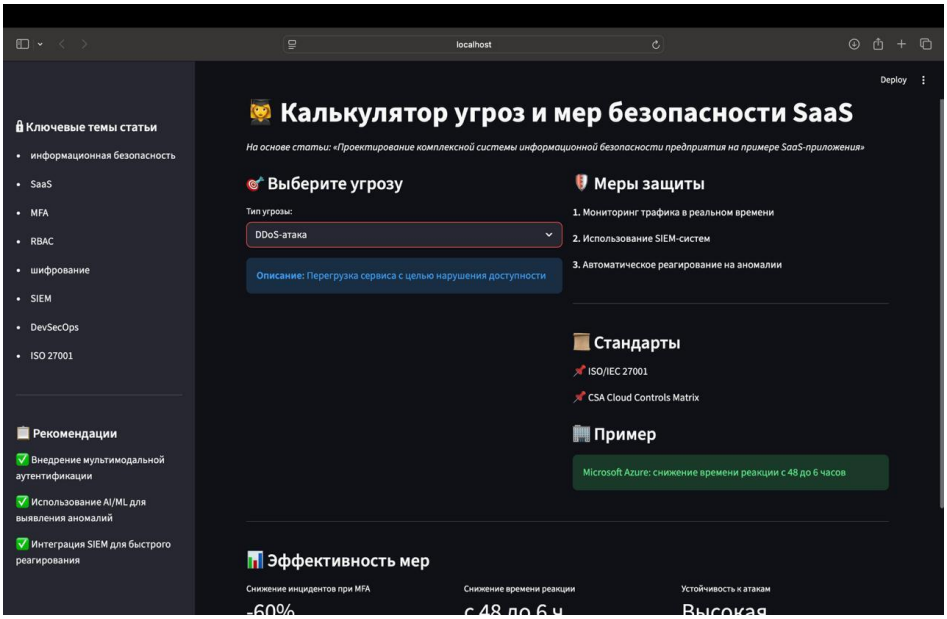

Рисунок 2 – Отображение мер защиты, стандартов и примера для угрозы «DDoS-атака»

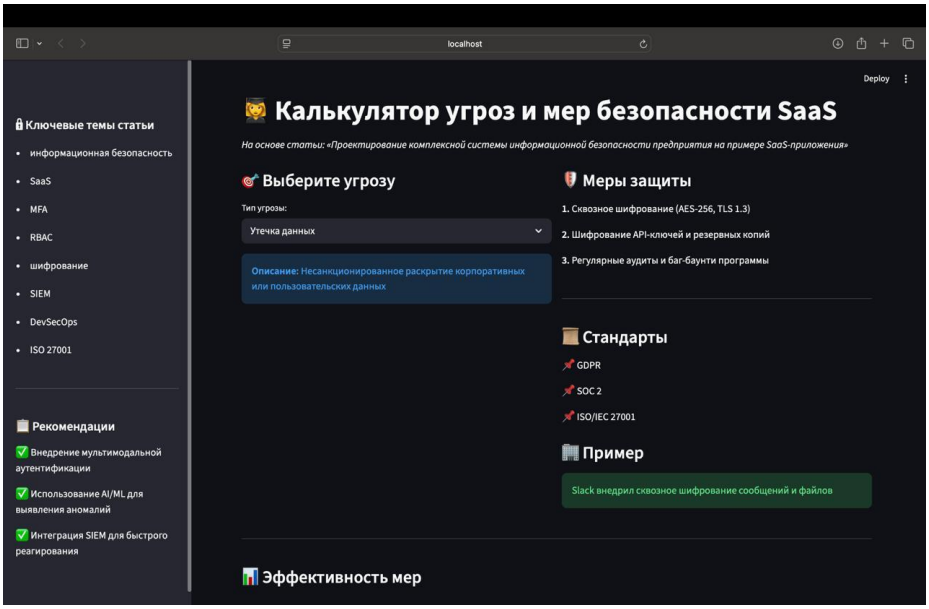

Рисунок 3 – Отображение мер защиты, стандартов и примера для угрозы «Утечка данных»

В нижней части интерфейса размещён блок статистики эффективности внедрённых мер (рисунок 4). Он содержит три ключевые метрики: снижение инцидентов при использовании MFA на 60%, сокращение времени реагирования на инциденты с 48 до 6 часов (благодаря SIEM), а также общую оценку устойчивости к атакам (высокая).

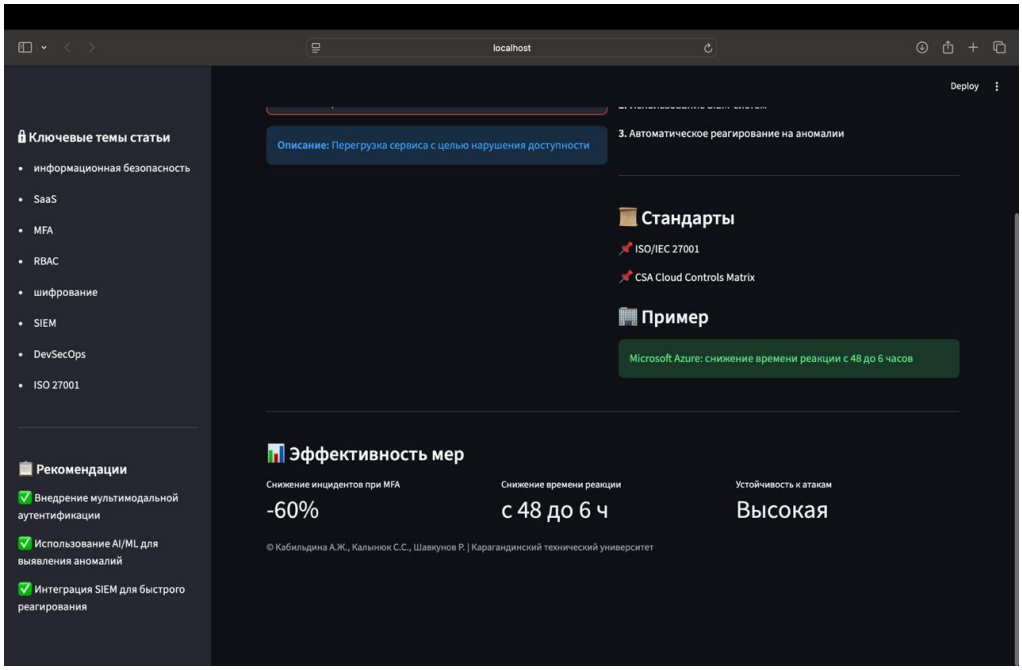

Рисунок 4 – Блок статистики эффективности мер безопасности

Программная реализация выполнена с использованием объектно-ориентированного подхода. Модуль threats_data.py содержит словарь threats, где для каждой угрозы заданы описание, меры защиты, стандарты и пример. Основной модуль app.py на Streamlit отвечает за построение пользовательского интерфейса: боковую панель с ключевыми словами и рекомендациями, основную область с выбором угрозы и отображением результатов, а также блок статистики. Такой подход обеспечивает лёгкость масштабирования — добавление новой угрозы требует лишь расширения словаря.

Сравнительный анализ и рекомендации. Сравнение подходов международных компаний (Slack, Atlassian, Salesforce) 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, 13]. Для повышения безопасности SaaS-приложений рекомендуется:

- внедрять мультимодальную аутентификацию, объединяющую биометрические методы, токены доступа и поведенческую аналитику;
- использовать искусственный интеллект и машинное обучение (TensorFlow, OpenCV) для выявления аномальной активности;
- интегрировать SIEM-платформы для автоматизированного обнаружения угроз и реагирования;
- применять DevSecOps и принцип «безопасность по дизайну» на этапе разработки [14, 15].

Заключение

В результате работы проведён анализ угроз информационной безопасности SaaS-приложений, выявлены ключевые меры защиты (MFA, RBAC, шифрование, SIEM, DevSecOps) и соответствующие стандарты. Разработано веб-приложение «SaaS Security Assistant», реализующее интерактивный калькулятор угроз и мер безопасности. Предложена формула интегральной оценки уровня защищённости, позволяющая количественно оценить эффективность системы безопасности.

Разработанный инструмент может быть использован как для обучения сотрудников, так и для предварительной оценки рисков при внедрении SaaS-решений. Перспективы дальнейшего развития связаны с интеграцией базы знаний по уязвимостям (CVE), добавлением динамического расчёта показателя S на основе пользовательских весов и подключением к реальным SIEM-системам через API.

Список использованных источников

1. Atlassian. (2023). Security Report 2023: MFA implementation results. URL: https://www.atlassian.com/trust/security (дата обращения: 15.04.2026).

2. Kumar, S., & Rani, R. (2022). Access control models for SaaS applications: A comparative study. Journal of Cloud Computing, 11(3), 45–58.

3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection-Information security management systems.

4. ISO/IEC 27701:2019. Security techniques-Extension to ISO/IEC 27001 for privacy information management.

5. DevSecOps Alliance. (2024). State of DevSecOps in cloud-native environments. White paper.

6. NIST Special Publication 800-210. (2020). General Access Control Guidance for Cloud Systems.

7. Chen, Y., & Zhao, H. (2023). Multi-factor authentication in SaaS: Challenges and solutions. IEEE Transactions on Cloud Computing, 11(2), 1234–1245.

8. Singh, R., & Verma, P. (2024). End-to-end encryption for enterprise SaaS: Performance and security trade-offs. Expert Systems with Applications, 238, 121890.

9. Microsoft Azure. (2023). Security Intelligence Report: Incident response times with SIEM. URL: https://azure.microsoft.com/en-us/security (дата обращения: 15.04.2026).

10. Slack. (2023). Transparency Report: Data encryption and bug bounty. URL: https://slack.com/trust (дата обращения: 15.04.2026).

11. CSA (Cloud Security Alliance). (2021). Cloud Controls Matrix v4.0.

12. Atoum, Y., Chen, L., Liu, A.X., Hsu, S.D.H., & Liu, X. (2021). Automated Online Exam Proctoring. IEEE Transactions on Multimedia, 23, 2345–2358.

13. Nguyen, T., et al. (2023). AI-based cheating detection in online exams. arXiv preprint arXiv:2301.01234.

14. Vaishnavi, D. A. L., Kumar, A. C., Harish, S., & Divya, M. L. (2022). MediaPipe to recognise the hand gestures. In Proc. of ICICCS, 789–794.
15. Zhang, T. (2025). Deep learning-based object detection using YOLO in smart monitoring systems. Expert Systems with Applications, 245, 123456.

КӘСІПОРЫНЫҢ ҚАУІПТІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖҮЙЕСІНЕ SAAS ӨТІНІШІ

Кабильдина А.Ж., Калынюк С.С., Шавкунов Р.А.

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.

SAAS APPLICATION FOR A COMPREHENSIVE ENTERPRISE INFORMATION SECURITY SYSTEM

Kabildina A. Zh., Kalynyuk S. S., Shavkunov R. A.

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.