наменовав переход от ремесленного подхода к инженерно-цифровой парадигме. Будущее направления связано с автоматизацией, ИИ в проектировании, печатью керамики и развитием биопечати для регенерации тканей. Массовому внедрению, однако, способствуют вызовы: высокая стоимость, необходимость обучения специалистов и развитие нормативной базы для инновационных материалов.

Литература

1. AL-Aimiri, M. A. M. K. ERPNEXT: revolutionizing manufacturing management in factories / M. A. M. K. AL-Aimiri, M. F. S. H. AL-Kamali // Инновационное станкостроение, технологии и инструмент : материалы I Междунар. науч.-практ. конф., Гомель, 30 нояб. 2023 г. / М-во пром-сти Респ. Беларусь ; под общ. ред. М. И. Михайлова. – Гомель : ГГТУ им. П. О. Сухого, 2024. – С. 102–104.
2. AL-Aimiri, M. A. M. K. Streamlining factory operations: designing an effective manufacturing management program / M. A. M. K. AL-Aimiri, M. F. S. H. AL-Kamali // Инновационное станкостроение, технологии и инструмент : материалы I Междунар. науч.-практ. конф., Гомель, 30 нояб. 2023 г. / М-во пром-сти Респ. Беларусь ; под общ. ред. М. И. Михайлова. – Гомель : ГГТУ им. П. О. Сухого, 2024. – С. 105–106.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В ПРИКЛАДНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ: ТЕХНОЛОГИИ ШИФРОВАНИЯ, ЗАЩИТЫ ОТ УТЕЧЕК И СООТВЕТСТВИЕ СТАНДАРТАМ (GDPR, HIPAA) В РАЗРАБОТКЕ ПРИЛОЖЕНИЙ

Ш. Аллакулыев, А. Суннатов

Государственный энергетический институт Туркменистана, г. Мары

Рассмотрены ключевые технологии шифрования, такие как симметричное и асимметричное шифрование, методы предотвращения утечек данных (DLP-системы) и требования стандартов GDPR и HIPAA. Цель исследования – анализ подходов к интег-рации этих мер в процесс разработки, включая оценку рисков, выбор инструментов и тести-рование. Методика основана на обзоре специализированной литературы и практических рекомендаций. Результаты показывают, что комбинированное исполь-зование шифрования данных в покое и в транзите, мониторинга доступа и аудита логов позволяет минимизировать риски утечек, обеспечивая соответствие регуляциям. В итоге подчеркивается необходимость комплексного подхода для повышения надежности ПО.

Ключевые слова: безопасность данных, шифрование, защита от утечек, GDPR, HIPAA, разработка приложений.

DATA SECURITY IN APPLICATION SOFTWARE: ENCRYPTION TECHNOLOGIES, LEAK PREVENTION, AND COMPLIANCE WITH STANDARDS (GDPR, HIPAA) IN APPLICATION DEVELOPMENT

S. Allakulyyev, A. Sunnatov

The State Energy Institute of Turkmenistan, Mary

The article examines key encryption technologies, such as symmetric and asymmetric encryption, data leak prevention methods (DLP systems), and GDPR and HIPAA standards requirements. The research aim is to analyze approaches to integrating these measures into the development process, including risk assessment, tool selection, and testing. The methodology is based on a review of specialized literature and practical recommendations. The results demonstrate that combining data encryption at rest and in transit, access monitoring, and log auditing minimizes leak risks, ensuring regulatory compliance. Ultimately, the need for a comprehensive approach to enhance software reliability is emphasized.

Keywords: data security, encryption, data leak prevention, GDPR, HIPAA, application development.

В современном мире, где приложения ежедневно обрабатывают огромные объемы личных и корпоративных данных, вопрос безопасности выходит на первый план. Утечки данных могут привести к финансовым потерям, репутационному ущербу и юридическим санкциям. По данным отчетов, в 2024 г. количество кибератак на приложения выросло на 30 % [1, с. 2], что подчеркивает актуальность темы. Целью данного исследования является изучение технологий шифрования, механизмов защиты от утечек и способов обеспечения соответствия стандартам GDPR (Общий регламент по защите данных ЕС) и HIPAA (Закон о переносимости и подотчетности медицинского страхования США) в процессе разработки прикладного ПО. Мы рассмотрим, как эти элементы интегрируются для создания надежных систем, минимизируя риски.

Методика проведения исследований опирается на анализ научной и практической литературы, включая обзоры стандартов и кейсы разработки. Были изучены рекомендации по шифрованию от ведущих источников, а также требования регуляторов [2, с. 3–5]. Для оценки эффективности применялись сравнительные методы: анализ преимуществ симметричного шифрования (например, AES-256) по сравнению с асимметричным (RSA), моделирование сценариев утечек и проверка compliance-чеклистов. Исследование проводилось на основе открытых данных и симуляций в тестовых средах, без реального доступа к конфиденциальным базам.

В результате анализа выявлено, что технологии шифрования играют ключевую роль в защите данных. Например, шифрование в покое (at rest) с использованием AES обеспечивает конфиденциальность хранимых данных, предотвращая несанкционированный доступ даже при физическом взломе устройств [1, с. 4]. Для данных в транзите рекомендуется TLS 1.3, который интегрирует шифрование и аутентификацию, снижая риски перехвата [2, с. 6]. Защита от утечек реализуется через DLP-системы, такие как мониторинг трафика и классификация данных, где алгоритмы машинного обучения выявляют аномалии в реальном времени [3, с. 7]. В контексте GDPR акцент делается на принципах “privacy by design”, включая минимизацию данных и прозрачность обработки, что требует внедрения consent-менеджмента в коде приложения [2, с. 4]. Для HIPAA фокус на медицинских данных: обязательное шифрование PHI (protected health information), аудит логов и контроль доступа с использованием ролевых моделей (RBAC), что снижает вероятность нарушений на 40–50 % по статистике [3, с. 8–9]. Полученные результаты показывают, что интеграция этих мер на этапе дизайна ПО позволяет не только соответствовать стандартам, но и повысить общую устойчивость к угрозам, как демонстрируют кейсы из здравоохранения.

Обеспечение безопасности данных в прикладном ПО требует комплексного подхода, сочетающего передовые технологии шифрования, DLP-инструменты и строгое соблюдение GDPR и HIPAA. Исследование подтверждает, что ранняя интеграция этих элементов минимизирует риски и повышает доверие пользователей. В будущем, с ростом ИИ и облачных сервисов, разработчикам стоит фокусироваться на автоматизированных аудитах и адаптивных системах защиты [1, с. 10]. Это не только юридическая необходимость, но и стратегическое преимущество в конкурентной среде.

Литература

1. Topflight Apps. HIPAA Compliant App Development in 2025 // Topflightapps.com. – 2025. – P. 1–10.
2. Appventurez. GDPR & HIPAA Compliance in IT Services / Data Security Guide // Appventurez.com. – 2025. – P. 3–6.
3. MobiDev. Healthcare Software Security and Data Protection Strategies // Mobidev.biz. – 2025. – P. 7–9.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРИКЛАДНЫХ ПРИЛОЖЕНИЯХ

П. С. Мырадов

Государственный энергетический институт Туркменистана, г. Мары

Рассмотрены особенности применения технологии искусственного интеллекта в различных сферах человеческой деятельности.

Ключевые слова: искусственный интеллект, машинное обучение, обработка естественного языка, автоматизация.

USING ARTIFICIAL INTELLIGENCE IN APPLICATIONS

P. S. Myradov

The State Energy Institute of Turkmenistan, Mary

The article examines the specifics of applying artificial intelligence (AI) technology in various areas of human activity.

Keywords: artificial intelligence, machine learning, natural language processing, automation.

Развитие искусственного интеллекта стало одним из ключевых направлений цифровой трансформации общества. Сегодня ИИ перестал быть абстрактным понятием из научной фантастики и превратился в мощный инструмент, внедряемый в практические решения, направленные на повышение эффективности и точности в разных сферах деятельности человека. В основе большинства прикладных приложений лежат алгоритмы машинного обучения и методы обработки естественного языка, которые позволяют системам не просто выполнять запрограммированные действия, но и обучаться на данных, выявлять закономерности и принимать решения [1].

В медицинской практике искусственный интеллект используется для анализа изображений, прогнозирования заболеваний и выбора оптимальных схем лечения. Например, системы компьютерного зрения, основанные на нейронных сетях, способны с высокой точностью распознавать опухоли на рентгеновских снимках и МРТ, превосходя по эффективности традиционные методы диагностики [1]. Это не только ускоряет процесс постановки диагноза, но и снижает риск человеческих ошибок.

В финансовом секторе ИИ применяется для анализа поведения клиентов, выявления мошеннических операций и управления инвестиционными портфелями. Алгоритмы машинного обучения анализируют миллионы транзакций, определяя подозрительные паттерны и предотвращая финансовые преступления [2]. Кроме того, технологии ИИ используются для прогнозирования рыночных тенденций, что помогает компаниям принимать стратегические решения на основе данных, а не интуиции.

В сфере образования ИИ способствует формированию персонализированных образовательных траекторий. Интеллектуальные обучающие системы анализируют