УДК 004.056.5:377

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ ПРИ ВНЕДРЕНИИ АДАПТАЦИОННЫХ ЦИФРОВЫХ СЕРВИСОВ В КОЛЛЕДЖЕ

Охотенко Александра Леонидовна, магистрант
Шаталова Виктория Викторовна, доцент, к.т.н., доцент
Белорусский государственный университет информатики и радиоэлектроники

ANALYSIS OF INFORMATION RISKS IN THE IMPLEMENTATION OF ADAPTIVE DIGITAL SERVICES IN COLLEGE

Okhotenko Alexandra, master's student, kasandranova65@gmail.com
Shatalova Victoria, Associate Professor, PhD, Associate Professor, shatalova@bsuir.by
Belarusian State University of Informatics and Radioelectronics

Аннотация. В статье проведен анализ информационных рисков при внедрении адаптационных цифровых сервисов в колледжах Республики Беларусь в условиях отсутствия готового сертифицированного программного решения.

Ключевые слова: информационная безопасность, персональные данные, адаптационные цифровые сервисы.

Abstract. This article analyzes the information risks associated with the implementation of digital adaptation services in colleges in the Republic of Belarus in the absence of a ready-made certified software solution.

Keywords: information security, personal data, digital adaptation services.

Введение. Современный этап развития системы среднего специального образования Республики Беларусь характеризуется активным внедрением цифровых технологий во все сферы деятельности учреждений образования. Министерство образования последовательно реализует комплекс мер, направленных на цифровую трансформацию образовательного процесса, включая применение цифровых помощников на основе технологий искусственного интеллекта и усиление практикоориентированной составляющей обучения [1, с.118]. В этом контексте особую актуальность приобретает задача создания комфортной и безопасной среды для адаптации учащихся первого курса, которые сталкиваются с целым рядом вызовов: новой академической нагрузкой, сменой социального окружения, зачастую переездом в другой город и началом самостоятельной жизни в общежитии.

Основная часть. На сегодняшний день на рынке программного обеспечения Республики Беларусь и стран СНГ не существует готового, сертифицированного продукта, который одновременно сочетал бы в себе полноценный функционал адаптационной платформы и соответствовал жестким требованиям законодательства о защите персональных данных. Отдельные LMS-системы и платформы адаптированные под образовательные нужды и предлагают базовые возможности тестирования и мониторинга активности пользователей, однако ни одна из них не реализует в полном объеме специфические функции, необходимые для сопровождения адаптации первокурсников колледжа, а именно: проведение психологического тестирования с обработкой результатов, относящихся к специальной категории персональных данных, анализ тональности коммуникации в неформальных чатах с соблюдением конфиденциальности переписки [2].

Данное обстоятельство порождает ситуацию, при которой учреждение среднего специального образования, стремящееся внедрить адаптационный цифровой сервис, вынуждено выбирать один из двух путей, каждый из которых сопряжен с собственным набором рисков. Первый путь – это приобретение существующей образовательной платформы и ее глубокая кастомизация под специфические задачи адаптации. Второй путь – заказ полностью оригинальной разработки у стороннего подрядчика. Оба варианта требуют пристального внимания к вопросам информационной безопасности на всех этапах жизненного цикла системы, начиная от составления технического задания и заканчивая выводом сервиса из эксплуатации.

Вне зависимости от того, какой путь создания адаптационного сервиса будет выбран, проектная команда сталкивается с необходимостью обработки сведений, выходящих далеко за пределы

стандартного набора данных, требуемых для зачисления учащегося. В классической модели информационной системы колледжа циркулируют паспортные данные, сведения о регистрации по месту жительства, данные о родителях и законных представителях, а также академическая успеваемость. Адаптационная же платформа по своей сути нацелена на сбор информации, относящейся к специальным персональным данным, а также к сведениям, косвенно позволяющим составить детальный профиль личности.

В структуру собираемой информации, как правило, включаются результаты психологического тестирования и опросников, направленных на выявление уровня тревожности, суицидальных рисков, агрессивности и особенностей межличностного восприятия в группе. Подобные сведения, согласно статье 1 Закона Республики Беларусь от 7 мая 2021 года № 99-З «О защите персональных данных», относятся к категории специальных персональных данных, поскольку касаются состояния психического здоровья [3]. Это требует не просто письменного согласия, а оформления отдельного информированного согласия на обработку таких данных.

Поскольку готового решения на рынке не существует, многие колледжи рассматривают возможность приобретения универсальной образовательной платформы или LMS-системы с последующей доработкой под задачи адаптации. Данный подход, кажущийся на первый взгляд менее затратным и более быстрым, несет в себе целый спектр специфических рисков, которые необходимо учитывать на этапе принятия решения.

Первый и наиболее серьезный риск связан с архитектурой хранения данных. Большинство популярных образовательных платформ, особенно предлагаемых по модели SaaS (программное обеспечение как услуга), размещают свои серверы за пределами Республики Беларусь, что вступает в прямое противоречие с требованиями о локализации баз персональных данных. Даже если предлагается опция развертывания на серверах заказчика, архитектура системы изначально не проектировалась под раздельное хранение различных категорий данных. В результате данные психологического тестирования и личной переписки могут оказаться в той же базе данных, что и стандартные учетные записи пользователей, что многократно повышает ценность потенциальной утечки.

Второй риск заключается в том, что механизмы интеграции с внешними сервисами, такими как мессенджеры в готовых платформах реализованы без учета белорусских требований к криптографической защите каналов связи. Стандартные протоколы шифрования, используемые западными или российскими разработчиками, могут не соответствовать стандартам, принятым в Республике Беларусь. Это создает уязвимость на этапе передачи данных от устройства учащегося к серверу платформы [4].

Третий риск связан с обновлениями и технической поддержкой. При глубокой кастомизации платформы под специфические нужды колледжа каждое обновление несет угрозу нарушения работоспособности доработанных модулей или, что еще опаснее, отключения критически важных функций безопасности, реализованных в ходе кастомизации. Практика показывает, что учреждения образования зачастую откладывают установку обновлений безопасности именно из-за опасений нарушить работу кастомизированных модулей, что со временем превращает систему в легко уязвимую цель для злоумышленников.

Альтернативой кастомизации готового решения является заказ полностью оригинальной разработки у стороннего подрядчика или, при наличии соответствующих компетенций, силами собственного IT-подразделения колледжа. Этот путь позволяет изначально заложить в архитектуру системы все необходимые механизмы защиты, однако он сопряжен с собственным набором рисков.

Ключевой риск в таком случае – это человеческий фактор и недостаток специфических компетенций в области защиты персональных данных у разработчиков. Большинство компаний-разработчиков программного обеспечения в Республике Беларусь специализируются на создании веб-сайтов, интернет-магазинов или корпоративных порталов. Лишь немногие имеют практический опыт построения информационных систем, обрабатывающих специальные категории персональных данных в соответствии с требованиями Национального центра защиты персональных данных. В результате на этапе проектирования могут быть допущены фундаментальные ошибки, исправление которых на более поздних стадиях разработки потребует значительных финансовых и временных затрат.

Второй существенный риск – это отсутствие у подрядчика необходимых лицензий и сертификатов на деятельность в области защиты информации. На практике многие колледжи при выборе подрядчика руководствуются в первую очередь стоимостью и сроками разработки, оставляя вопросы лицензирования «на потом», что впоследствии может привести к невозможности легальной эксплуатации созданной системы.

Третий риск касается долгосрочной поддержки и развития системы. В отличие от тиражируемых программных продуктов, которые поддерживаются вендором на протяжении многих лет, оригинальная разработка часто оказывается «привязанной» к конкретному подрядчику или даже к конкретным разработчикам. Смена подрядчика или уход ключевых сотрудников может привести к ситуации, когда исходный код системы становится «мертвым грузом», который никто не способен ни поддерживать, ни развивать. Учитывая, что адаптационный сервис аккумулирует чувствительные данные учащихся, такая ситуация создает отложенные риски утечки информации при попытках экстренного исправления уязвимостей силами нового, не знакомого с архитектурой системы персонала.

Независимо от того, каким путем был создан адаптационный сервис, на этапе его эксплуатации возникают общие для всех сценариев уязвимости. Наиболее слабым звеном в цепи информационной безопасности колледжа практически всегда оказывается не хакерская атака с применением уязвимостей нулевого дня, а человеческий фактор.

Внедрение цифрового сервиса подразумевает, что доступ к административной панели с агрегированными данными получают не только сотрудники отдела информационных технологий, но и штатные психологи, кураторы групп, а иногда и члены ученического самоуправления из числа старшекурсников. Разграничение прав доступа в таких проектах зачастую проводится формально, без учета принципа минимально необходимых привилегий. Однако если система спроектирована как единая панель для куратора, велика вероятность того, что сотрудник, обладая полным доступом, рано или поздно станет жертвой фишинговой атаки или просто по неосторожности оставит сессию открытой на общедоступном компьютере в учительской, что приведет к моментальной утечке всей базы.

Заключение. Подводя итог проведенному анализу, необходимо подчеркнуть, что внедрение адаптационных цифровых сервисов в учреждениях среднего специального образования Республики Беларусь является объективной необходимостью современной педагогики, соответствующей общему пути цифровизации, заданному Министерством образования. Отказ от них под предлогом рисков утечки данных был бы недальновидным решением. Однако отсутствие на рынке готового программного продукта, в полной мере удовлетворяющего как функциональным требованиям адаптации, так и жестким стандартам защиты персональных данных, накладывает на учреждения образования особую ответственность.

Осознание того, что идеального готового решения не существует, должно не останавливать процесс цифровизации адаптации, а напротив, побуждать к более вдумчивому и системному подходу. Каждое учреждение среднего специального образования, встающее на этот путь, должно пройти все этапы – от анализа собственных потребностей и составления детального технического задания с учетом требований законодательства до тщательного отбора подрядчика и организации обучения сотрудников. Только при условии соблюдения баланса между педагогической полезностью сервиса и его технической безопасностью цифровая среда колледжа станет для первокурсника не зоной повышенного риска, а надежным инструментом для успешного вхождения в профессию и взрослую жизнь. В противном случае последствия компрометации даже одной базы данных учащихся могут перечеркнуть годы работы по формированию позитивного имиджа учреждения образования и доверия со стороны родителей и общественности, а также повлечь за собой ответственность, предусмотренную законодательством Республики Беларусь.

Список использованных источников

1. Снитко, Д. А. Современные подходы к защите информационных ресурсов в учебных заведениях / Д. А. Снитко, И. Г. Скиба, С. А. Мигалевич // Инженерное образование в цифровом обществе : материалы Международной научно-методической конференции / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2024. – С. 118-120.

2. Концепция информационной безопасности Республики Беларусь: утверждена Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=P219s0001. – Дата доступа: 08.04.2026.

3. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=H12100099. – Дата доступа: 08.04.2026.

4. Зинькевич, В. Н. Безопасность при передаче файлов в образовании / В. Н. Зинькевич, И. Ю. Перцев // КиберЛенинка [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/bezopasnost-pri-peredache-faylov-v-obrazovanii. – Дата доступа: 12.04.2026.