УДК 004.4

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБРАЗОВАНИЯ: РИСК-ОРИЕНТИРОВАННАЯ МОДЕЛЬ И ПРАКТИКИ ВНЕДРЕНИЯ

Домбровский Я.А.

старший преподаватель

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Комаров К.А.

магистрант

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация.

Цифровизация образования приводит к росту объёмов обрабатываемых данных, расширению поверхности атак (LMS, электронные журналы, облачные сервисы, видеоконференцсвязь), усложнению цепочек поставки ИТ-услуг и увеличению доли человеческого фактора. В этих условиях информационная безопасность (ИБ) образовательной организации должна рассматриваться не как набор разрозненных технических мер, а как управляемая система, основанная на оценке рисков и соблюдении нормативных требований. В статье предложена риск-ориентированная модель обеспечения ИБ в образовательной организации, включающая правовой, организационный, технический и педагогико-просветительский контуры. Представлена типовая матрица «актив–угроза–меры защиты», а также практический алгоритм внедрения системы управления информационной безопасностью (СУИБ) с опорой на требования российского законодательства и подходы стандартов серии ISO/IEC 27000.

Ключевые слова: цифровизация образования, информационная безопасность, персональные данные, риск-менеджмент, СУИБ, кибергигиена, образовательная организация, LMS.

ENSURING INFORMATION SECURITY IN THE CONTEXT OF DIGITALIZATION OF EDUCATION: RISK-ORIENTED MODEL AND IMPLEMENTATION PRACTICES

Dombrovsky Y.A.
Senior Lecturer
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Komarov K.A.
Master's student
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Abstract.
Digitalization of education leads to an increase in the volume of processed data, an expansion of the attack surface (LMS, electronic journals, cloud services, video conferencing), the complexity of IT service supply chains, and an increase in the share of the human factor. In these conditions, the information security (IS) of an educational organization should be considered not as a set of disparate technical measures, but as a managed system based on risk assessment and compliance with regulatory requirements. The article proposes a risk-oriented model of information security in an educational organization, which includes legal, organizational, technical, and pedagogical and educational components. It presents a typical "asset-threat-protection measures" matrix,

as well as a practical algorithm for implementing an information security management system (ISMS) based on the requirements of Russian legislation and the approaches of the ISO/IEC 27000 series of standards.

Keywords: digitalization of education, information security, personal data, risk management, ISMS, cyber hygiene, educational organization, LMS.

Современная образовательная организация функционирует в гибридной среде: очные процессы дополняются дистанционными, а управление обучением и контингентом поддерживается информационными системами (электронный журнал/дневник, LMS, системы приёма, прокторинг, электронные библиотечные ресурсы). Это повышает эффективность и доступность образования, но одновременно усиливает риски: утечки персональных данных обучающихся и сотрудников, компрометация учётных записей, подмена результатов оценивания, заражение рабочих мест вымогателями, атаки на доступность сервисов и распространение нежелательного контента. Требование защищать информацию закреплено в российском правовом поле: в части общих принципов защиты информации [8], обработки персональных данных [9], регулирования образовательной деятельности [11] и защиты детей от вредной информации [12]. Стратегические ориентиры в информационной сфере задаёт Доктрина информационной безопасности Российской Федерации [7].

Практика показывает, что «точечные» меры (антивирус, запреты, разовые инструктажи) не обеспечивают устойчивой защиты в условиях постоянных изменений цифровой инфраструктуры. Следовательно, актуальна разработка комплексной, управляемой и измеримой модели ИБ, адаптированной к типовым процессам образовательной организации.

Правовые и методические требования к ИБ в образовательной сфере формируют многослойную рамку. Базовые требования по защите информации

закреплены в Федеральном законе № 149-ФЗ [8]. Обработка персональных данных регламентируется Федеральным законом № 152-ФЗ [9], а состав организационных и технических мер защиты персональных данных при их обработке в ИСПДн конкретизируется приказом ФСТЭК России № 21 [5]. Специфика образовательной деятельности задаётся Федеральным законом № 273-ФЗ [11]. Защита обучающихся от вредной информации обеспечивается Федеральным законом № 436-ФЗ [12] и методическими материалами по ограничению доступа обучающихся к нежелательным видам информации в сети «Интернет» [3].

Риск-ориентированное управление ИБ поддерживается подходами стандартов: требования к СУИБ (ГОСТ Р ИСО/МЭК 27001-2021) [1] и свод практик/контролей (ГОСТ Р ИСО/МЭК 27002-2021) [2]. Отдельный контур просвещения целесообразно выстраивать с учётом государственных инициатив по кибергигиене [4] и методических материалов по соблюдению законодательства в области персональных данных, подготовленных профильными органами [6].

Таким образом, образовательной организации требуется модель, которая связывает правовое соответствие, управление рисками и повседневные практики (процессы и поведение пользователей).

Предлагаемая модель включает четыре взаимосвязанных контура.

1) Управленческий контур (политики и ответственность). Формируется политика ИБ, распределяются роли (владелец процесса, администратор безопасности, ответственный за ПДн, комиссия по инцидентам), утверждается перечень защищаемых активов и целевые показатели (например, доля пользователей с MFA, время восстановления сервиса, доля завершивших обучение по кибергигиене). Такой подход соответствует логике СУИБ как системы управления [1].

2) Правовой и комплаенс-контур (соответствие требованиям). Включает: реестр ИСПДн, основания обработки ПДн, локальные акты и процедуры, порядок

доступа к данным, хранение и уничтожение, реагирование на обращения субъектов ПДн. Основа – требования 152-ФЗ [9] и меры по приказу ФСТЭК № 21 [5]. Для контентных рисков – требования 436-ФЗ [12] и методические материалы по ограничению доступа [3].

3) Технический контур (защита инфраструктуры и данных). Реализует контролируемые меры: управление идентификацией и доступом, сегментация сети, резервное копирование, журналирование, шифрование, безопасные настройки, защита конечных устройств, контроль обновлений, защита почты, антифишинговые меры, мониторинг событий безопасности. Подбор контролей обосновывается оценкой рисков и может опираться на практики ГОСТ Р ИСО/МЭК 27002-2021 [2].

4) Педагогико-просветительский контур (человеческий фактор). ИБ в образовании неизбежно зависит от цифровой грамотности обучающихся и сотрудников: безопасная работа с учётными записями, распознавание социальной инженерии, корректная публикация материалов, этика онлайн-взаимодействия. Эффективны регулярные форматы кибергигиены и микро-обучение [4].

Ниже приведён пример матрицы, применимой для школы, колледжа или вуза (таблица 1).

Таблица 1 – Матрица «актив–угроза–меры защиты» для образовательной организации

Актив/процесс	**Ключевые угрозы**	**Уязвимости**	**Приоритетные меры (пример)**	**Метрики контроля**
Учётные записи LMS/почты	фишинг, подбор пароля, захват сессии	слабые пароли, отсутствие MFA	MFA, политика паролей, обучение антифишингу, контроль аномалий входа	% MFA, число фишинг-инцидентов
Базы ПДн (обучающиеся/сотрудники)	утечка, несанкционированный доступ	избыточные права, отсутствие регламентов	разграничение прав, журналирование, регламенты обработки/выдачи данных (152-ФЗ, ФСТЭК) [5; 9]	результаты проверок, число нарушений

Электронный журнал/оценивание	подмена оценок, компрометация целостности	общие аккаунты, слабый аудит	запрет общих учётных записей, ролевая модель, протоколирование изменений	доля изменений с идентификацией
Дистанционные занятия (ВКС)	утечка ссылок, вмешательство посторонних, запись без согласия	открытые комнаты, слабая настройка	комнаты ожидания, пароли/токены, ограничения демонстрации, правила занятия	число нарушений на занятиях
Сеть и рабочие станции	вредоносное ПО/вымогатели	нет обновлений, нет резервного копирования	управление обновлениями, защита конечных устройств, резервное копирование, сегментация	RTO/RPO, % актуальных патчей
Доступ обучающихся к Интернету	вредный/нецелевой контент	отсутствие фильтрации/контроля	контент-фильтрация, перечни категорий, регламенты ограничения доступа [3; 12]	число блокировок/попыток обхода

Практически применимый алгоритм можно представить как цикл PDCA (планируй – делай – проверяй – действуй), характерный для СУИБ [1]:

1. Инвентаризация и классификация активов: определение перечня ИС (LMS, электронный журнал, приёмная система, библиотека, почта), данных и владельцев процессов.

2. Моделирование угроз и оценка рисков: выделение сценариев (утечка ПДн, остановка LMS, подмена оценок, компрометация учётной записи преподавателя).

3. Выбор контролей и план обработки рисков: подбор мер на основе практик ГОСТ Р ИСО/МЭК 27002-2021 [2] и требований приказа ФСТЭК № 21 для ИСПДн [5].

4. Регламентация и обучение: локальные акты, инструкции, регулярная кибергигиена для сотрудников и обучающихся [4].

5. Мониторинг и реагирование на инциденты: каналы уведомления, первичный разбор, восстановление, анализ причин, корректирующие меры.

6. Аудит и улучшение: самопроверки, контроль метрик, корректировка политики ИБ при изменениях инфраструктуры и/или поставщиков.

В образовательных организациях часто встречаются повторяющиеся проблемные зоны:

- Смешение ролей и отсутствие владельцев процессов. Без владельца данных (например, «владелец реестра контингента») невозможно обеспечить устойчивое разграничение доступа и контроль изменений.
- Избыточные права и общие учётные записи. Это снижает подотчётность и затрудняет расследование инцидентов.
- Недооценка контентных рисков. Требования по ограничению доступа к вредной/нецелевой информации должны быть закреплены регламентами и поддержаны техническими средствами [3; 12].
- Нерегулярное обучение сотрудников. Разовые инструктажи не формируют устойчивых навыков противодействия социальной инженерии; эффективнее короткие регулярные форматы в логике кибергигиены [4].
- Отсутствие измеримости. Без метрик (MFA-покрытие, доля обновлённых устройств, RTO/RPO, число инцидентов по классам) ИБ становится неуправляемой как процесс.

В условиях цифровизации образования информационная безопасность должна рассматриваться как управляемая система, интегрированная в образовательные и административные процессы. Представленная риск-ориентированная модель позволяет связать требования законодательства, методические материалы по ограничению доступа к нежелательной информации и практики СУИБ в единый контур управления рисками. Практическая ценность подхода заключается в возможности поэтапного внедрения: от инвентаризации и оценки рисков до обучения пользователей и непрерывного улучшения. Для

образовательных организаций это обеспечивает не только снижение вероятности инцидентов (утечек, компрометации учётных записей, сбоев сервисов), но и повышение доверия участников образовательных отношений к цифровой среде.

Библиографический список:

1. ГОСТ Р ИСО/МЭК 27001-2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введ. 01.01.2022. М.: Стандартинформ, 2021.

2. ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. Введ. 30.11.2021. М.: Стандартинформ, 2021.

3. Минобрнауки России. Письмо от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет» (вместе с методическими рекомендациями).

4. Минцифры России. Программа «Кибергигиена» : официальный сайт. URL: https://digital.gov.ru/activity/kiberbezopasnost/programma-kibergigieny-2 (дата обращения: 13.01.2026).

5. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (зарег. в Минюсте России 14.05.2013 № 28375).

6. Роскомнадзор. Методические рекомендации для образовательных учреждений по соблюдению законодательства в области персональных данных.

URL: https://02.rkn.gov.ru/docs/2/Metodicheskie_rekomendacii.docx (дата обращения: 13.01.2026).

7. Российская Федерация. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

8. Российская Федерация. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

9. Российская Федерация. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

10. Российская Федерация. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

11. Российская Федерация. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

12. Российская Федерация. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».