УДК 004

Скорикова Арина Александровна

студент

3 курс, факультет «Информатика и вычислительная техника»

Донской государственный технический университет

Россия, г. Ростов-на-Дону

РАЗРАБОТКА СИСТЕМЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *В статье исследуются вопросы обеспечения информационной безопасности при организации дистанционного обучения в образовательных учреждениях Российской Федерации. Автор проводит анализ специфических угроз безопасности персональных данных, возникающих при использовании систем управления обучением (LMS), вебинарных платформ и облачных сервисов хранения данных.*

В работе предложена архитектура комплексной системы защиты, учитывающая требования Федерального закона № 152-ФЗ «О персональных данных» и актуальных приказов ФСТЭК России. Особое внимание уделено методам идентификации и аутентификации пользователей, защите каналов связи с использованием криптографических средств, а также организационным мерам контроля доступа. Результатом исследования является модель системы защиты, обеспечивающая выполнение требований по уровню защищенности ПДн (УЗ-2, УЗ-3) и минимизирующая риски утечек в условиях распределенной образовательной среды.

Ключевые слова: *персональные данные, дистанционное обучение, информационная безопасность*

Abstract. *This article examines information security issues in distance learning at educational institutions in the Russian Federation. The author analyzes specific threats to personal data security arising from the use of learning management systems (LMS), webinar platforms, and cloud storage services.*

The paper proposes the architecture of a comprehensive security system that takes into account the requirements of Federal Law No. 152-FZ "On Personal Data" and current orders of the Federal Service for Technical and Export Control of Russia. Particular attention is paid to user identification and authentication methods, protecting communication channels using cryptographic means, and organizational access control measures. The result of the study is a security system

model that ensures compliance with personal data security requirements (UZ-2, UZ-3) and minimizes the risk of leaks in a distributed educational environment.
Keywords: *personal data, distance learning, information security.*

Введение

Дистанционное обучение (ДО) прочно вошло в жизнь современного российского общества. От школьных онлайн-платформ и университетских LMS (Learning Management System) до корпоративных университетов и EdTech-проектов — цифровая образовательная среда сегодня обрабатывает колоссальные объемы персональных данных (ПДн). Это не только имена и фамилии, но и логины, пароли, оценки, результаты тестирований, история обучения, платежная информация и даже биометрические данные участников образовательного процесса. Утечка такой информации несет за собой не только репутационные потери и административные штрафы, но и может подорвать само доверие к цифровому образованию.

В России процесс цифровизации образования идет в условиях жесткого законодательного регулирования, направленного на обеспечение безопасности ПДн и технологического суверенитета. С 2025 по 2026 годы нормативная база претерпела значительные изменения: ужесточились требования к локализации данных, вступили в силу новые правила получения согласий, а регуляторы (Роскомнадзор, ФСТЭК России) активизировали проверки и расширили полномочия по контролю. В этих условиях разработка системы безопасности персональных данных для организации дистанционного обучения становится не просто рекомендацией, а обязательным и критически важным проектом.

Нормативно-правовая база Российской Федерации

Фундаментом любой системы защиты ПДн в России является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Он определяет принципы и условия обработки ПДн, права субъектов и обязанности операторов, а также требует от организаций принимать необходимые правовые, организационные и технические меры для защиты

данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Ключевым подзаконным актом, конкретизирующим меры безопасности, является Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Этот документ устанавливает перечень обязательных мер: от назначения ответственных лиц и издания внутренних регламентов до использования средств защиты информации (СЗИ), контроля доступа, регистрации событий безопасности и антивирусной защиты.

Для организаций, обрабатывающих ПДн с использованием государственных информационных систем или систем органов государственной власти, с 2025 года действуют новые требования, утвержденные Приказом ФСТЭК России от 11.04.2025 № 117, который пришел на смену устаревшим нормативам. Этот документ ужесточает подходы к защите информации и требует непрерывного мониторинга защищенности, что особенно актуально для образовательных учреждений, входящих в ведомственную сеть.

Наконец, нельзя не упомянуть требования к криптографической защите информации (СКЗИ), которые регулируются Приказом ФСБ России № 378. Для передачи ПДн по открытым каналам связи (а дистанционное обучение почти полностью основано на передаче данных через Интернет) необходимо использовать сертифицированные ФСБ России средства шифрования, работающие по алгоритмам ГОСТ.

Основные угрозы и риски в среде дистанционного обучения

Среда ДО имеет специфические уязвимости, которые необходимо учитывать при проектировании системы защиты. Во-первых, это человеческий фактор: фишинговые атаки, нацеленные на преподавателей и студентов с целью кражи учетных данных, остаются одной из главных угроз.

Во-вторых, распространено вредоносное ПО, способное перехватывать данные или предоставлять злоумышленникам удаленный доступ к системам.

Третья группа рисков связана с техническими ошибками конфигурации: некорректная настройка прав доступа, использование слабых паролей, открытые сетевые порты и ненадежно настроенные облачные хранилища. Четвертый важный аспект — угрозы, связанные с конечными устройствами. Студенты и преподаватели подключаются к системе обучения со своих домашних компьютеров, ноутбуков, планшетов, часто не имеющих должного уровня защищенности. Если злоумышленник компрометирует такое устройство, он может получить доступ к сессии обучения и к данным, передаваемым через LMS. Наконец, угроза утечки интеллектуальной собственности — уникальных учебных материалов, курсов и методик — также является серьезным риском для образовательных организаций.

Организационные меры: от политик до обучения персонала

Любая система безопасности начинается не с технологий, а с людей и процессов. Согласно 152-ФЗ и Приказу № 21, организация обязана назначить лицо, ответственное за обработку ПДн, и разработать пакет внутренних документов. В него входят:

1. Политика в отношении обработки персональных данных — документ, который должен быть опубликован в открытом доступе и информировать субъектов о целях, способах и сроках обработки их данных.
2. Перечень мер по обеспечению безопасности ПДн, включающий как технические, так и организационные мероприятия.
3. Правила рассмотрения запросов субъектов ПДн и порядок действий при инцидентах.
4. Положение об обработке ПДн без использования средств автоматизации (если такие процессы имеют место, например, бумажные журналы).
5. Инструкции для сотрудников о работе с ПДн и ответственности за их разглашение.

Критически важным элементом является регулярное обучение персонала. Как показывает практика проверок Роскомнадзора, одной из типичных причин наложения штрафов является отсутствие документально подтвержденного обучения сотрудников, работающих с ПДн, или проведение его ненадлежащим образом. Поэтому в план разработки системы безопасности должны быть включены регулярные тренинги по кибергигиене, правилам распознавания фишинговых атак и порядку действий при подозрении на утечку данных.

Технические решения: инструментарий защиты

Технический блок системы безопасности строится на нескольких ключевых направлениях.

Контроль доступа и аутентификация. Базовый, но важнейший элемент. Рекомендуется внедрение ролевой модели доступа (администратор, преподаватель, студент, гость) с минимизацией привилегий для каждой роли. Наиболее действенным способом защиты от взлома учетных записей является двухфакторная аутентификация (2FA). Как отмечают эксперты, одной из главных угроз в системах ДО являются ненадежные пароли, и 2FA многократно снижает этот риск.

Шифрование данных. Все данные, передаваемые между пользователем и сервером LMS, должны шифроваться с использованием протокола TLS. Для хранения чувствительных данных (например, платежной информации) на серверах также применяется шифрование. В государственных и крупных образовательных организациях использование сертифицированных СКЗИ (средств криптографической защиты информации), работающих по ГОСТ Р 34.10-2012, становится обязательным требованием.

Системы предотвращения утечек (DLP). Особенно актуальны для организаций, обрабатывающих большие объемы ПДн (более 10 000 субъектов). DLP-системы (Data Loss Prevention) контролируют все каналы передачи данных: корпоративную почту, мессенджеры, веб-трафик, USB-накопители, принтеры. При попытке несанкционированной отправки

персональных данных или учебного контента вовне DLP-система блокирует передачу и уведомляет службу безопасности. Для российского рынка доступны зрелые отечественные DLP-решения, такие как InfoWatch Traffic Monitor, Solar Dozor, «Кибер Протего» и другие, которые не уступают, а по ряду параметров превосходят зарубежные аналоги.

Виртуализация рабочих столов (VDI). Одно из самых надежных решений для защиты данных при удаленном доступе, набирающее популярность в России в условиях импортозамещения. При использовании VDI все приложения и данные остаются не на устройстве студента или преподавателя, а на централизованном защищенном сервере в дата-центре организации. Пользователь видит лишь «картинку» рабочего стола, передаваемую по защищенному каналу, но не может скопировать файлы на локальный диск или выгрузить данные на флешку. В случае утери или взлома конечного устройства, конфиденциальная информация не покидает пределы контролируемой инфраструктуры.

Мониторинг и управление инцидентами. Важнейший компонент, особенно с учетом требований Приказа № 117. Система должна включать средства централизованного сбора и анализа событий безопасности (SIEM), автоматическое оповещение о подозрительной активности и регламентированный порядок реагирования на инциденты.

Проектирование системы безопасности: этапы и подходы

Разработка системы защиты ПДн для организации ДО — это структурированный проектный процесс. На основе практического опыта (например, кейса компании LMS-Service по внедрению системы для крупного банка) можно выделить следующие этапы:

1. Обследование и аудит. Проводится интервьюирование сотрудников, анализ текущих бизнес-процессов и информационных систем, выявление всех мест хранения и каналов передачи ПДн.

2. Моделирование угроз. Определяются актуальные для данной системы угрозы безопасности с учетом отраслевой специфики, типа

обрабатываемых данных и инфраструктурных особенностей (например, использование облака).

3. Определение уровня защищенности. На основе типа ПДн (общедоступные, специальные, биометрические) и структуры угроз рассчитывается требуемый уровень защищенности информационной системы.

4. Разработка технического задания (ТЗ) на систему защиты. В ТЗ фиксируется состав необходимых организационных и технических мер для нейтрализации выявленных угроз.

5. Проектирование архитектуры системы защиты. Создается схема размещения средств защиты информации, определяются политики безопасности (например, парольная политика, регламент управления доступом), разрабатывается документация.

6. Внедрение и настройка СЗИ. Устанавливаются и конфигурируются выбранные средства: межсетевые экраны, антивирусы, DLP, системы шифрования и т.д.

7. Аттестация объекта информатизации. Проводится комплекс организационных и технических мероприятий, подтверждающих соответствие системы защиты установленным требованиям безопасности. По результатам выдается аттестат соответствия.

8. Оценка эффективности. Регулярное тестирование системы защиты, проведение контрольно-надзорных мероприятий и корректировка политик безопасности при изменении условий.

Заключение

Разработка системы безопасности персональных данных для организации дистанционного обучения в России — это комплексная, многоуровневая задача, требующая системного подхода. Она не сводится к покупке и установке антивируса или межсетевого экрана. Это непрерывный процесс, включающий в себя: соблюдение требований 152-ФЗ, Приказа № 21, требований к СКЗИ и иных нормативных актов; регулярную оценку рисков и моделирование угроз с учетом специфики ДО; внедрение организационных

мер: назначение ответственных, разработка внутренних документов, обучение персонала; развертывание технических средств: контроль доступа и 2FA, шифрование данных, DLP-системы, а в особо ответственных случаях — технология VDI; постоянный мониторинг событий безопасности и реагирование на инциденты.

Ужесточение законодательства и рост числа кибератак на образовательные учреждения делают эту задачу критически важной. Однако, как показывают успешные российские кейсы (Фоксфорд, LMS-Service, онлайн-школа с внедренной DLP), на рынке есть все необходимые компетенции и отечественные программно-аппаратные решения для построения эффективной системы защиты. Инвестиции в безопасность ПДн сегодня — это не издержки, а стратегическое вложение в доверие студентов и родителей, стабильность образовательного процесса и защиту от регуляторных рисков. В конечном счете, надежная защита персональных данных — это фундамент, на котором только и может строиться устойчивое и безопасное цифровое образование в России.

Использованные источники:

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
2. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»
3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных...».

5. Приказ Минпросвещения России от 14.03.2025 № 124 «О требованиях к государственным информационным системам в сфере образования» (актуальный регламент).

6. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: Учебное пособие. — 4-е изд. — М.: РИОР, 2024. — 322 с.

7. Петров С. В. Безопасность образовательной среды в условиях цифровизации: Монография. — М.: КноРус, 2025.

8. Степанов О. А. Правовые аспекты защиты персональных данных в цифровой образовательной среде // Государство и право. — 2025. — № 3. — С. 112–119.

9. Иванова М. А. Анализ угроз безопасности персональных данных при использовании облачных LMS-платформ // Защита информации. Инсайд. — 2025. — № 5.

10. Смирнов К. П. Опыт внедрения отечественных систем видеоконференцсвязи в образовательный процесс в рамках импортозамещения // Дистанционное обучение в России. — 2026. — № 1.

11. Васильев Д. Ю. Применение биометрической идентификации для контроля процесса онлайн-экзаменации (прокторинга) // Информационные технологии в образовании. — 2025. — Т. 14. — С. 88–95.