Индивидуальный предприниматель
Васильева Яна Александровна

УТВЕРЖДАЮ
Индивидуальный предприниматель
_____ Васильева Я.А.
«13» марта 2025г.

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1.1. Настоящая модель угроз безопасности персональных данных (далее – «Модель угроз») содержит систематизированный перечень угроз, которые могут возникнуть при обработке персональных данных (ПДн) в информационных системах персональных данных (ИСПДн). Документ также описывает меры защиты для минимизации данных рисков.

1.2. Цель документа:

- Определение возможных угроз безопасности персональных данных в ИСПДн.
- Разработка системы мер защиты, соответствующих законодательным требованиям.
- Обеспечение непрерывности работы системы дистанционного обучения и защиты информации.

1.3 Основание: Документ разработан в соответствии с:

- Федеральным законом № 152-ФЗ «О персональных данных»
- Приказом ФСТЭК России № 21 от 11.02.2013
- Приказом ФСБ России № 378 от 10.07.2020
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (и иных) операций. Защита информации»
- Методическими рекомендациями ФСТЭК по разработке модели угроз безопасности персональных данных

2. Описание информационной системы персональных данных (ИСПДн)

2.1 Категория обрабатываемых данных

Обрабатываемые персональные данные включают:

- Общие персональные данные: ФИО, дата рождения, адрес электронной почты, номер телефона, паспортные данные.

• Данные о процессе обучения: успеваемость, выполненные задания, сертификаты, оценки, комментарии преподавателей.

• Платежные данные: реквизиты карт, счета, история оплат.

• Данные учетных записей: логины, пароли, IP-адреса, метаданные активности пользователей.

2.2 Техническая структура ИСПДн

ИСПДн включает:

• Система дистанционного обучения (LMS) – веб-платформа для проведения онлайн-курсов.

• Сервер базы данных – централизованное хранилище данных пользователей, платежной информации, логов.

• Облачные сервисы – используются для хранения файлов, резервных копий и архивов данных.

• Средства связи – электронная почта, мессенджеры, API-интеграции с внешними сервисами.

• Системы мониторинга и защиты – антивирусные программы, системы обнаружения вторжений (IDS), межсетевые экраны (firewall).

3. Субъекты персональных данных

Субъектами ПДн являются:

• Обучающиеся – студенты, слушатели курсов.

• Преподаватели и тренеры – авторы курсов, менторы.

• Администраторы системы – лица, ответственные за управление платформой.

• Финансовые и административные сотрудники – сотрудники, обрабатывающие платежи, договоры, бухгалтерскую отчетность.

4. Объекты обработки персональных данных

Персональные данные обрабатываются в следующих объектах:

• Базы данных пользователей – централизованные хранилища учетной информации.

• Личный кабинет обучающегося – интерфейс пользователя, содержащий индивидуальные данные.

• Системы резервного копирования – защищенные хранилища данных для предотвращения потери информации.

• Веб-интерфейсы и API – используемые для интеграции с партнёрскими сервисами.

5. Источники угроз

Основные источники угроз:

• Внешние злоумышленники – хакеры, киберпреступники, конкуренты.

• Внутренние угрозы – недобросовестные сотрудники, случаи утечки данных по вине персонала.

• Ошибки пользователей – слабые пароли, неосторожные действия, переход по вредоносным ссылкам.

• Технические сбои – аппаратные отказы, сбои в работе программного обеспечения.

6. Классификация угроз

6.1 Угрозы конфиденциальности

• Взлом учетных записей пользователей (фишинг, подбор паролей).

• Несанкционированный доступ к базам данных (SQL-инъекции, атаки на API).

• Доступ третьих лиц к передаваемым данным (перехват трафика, атаки «человек посередине»).

6.2 Угрозы целостности

• Вредоносное ПО (шифровальщики, трояны, бэкдоры).

• Неавторизованное изменение данных администратором или злоумышленником.

• Уязвимости в коде, позволяющие подменять информацию.

6.3 Угрозы доступности

• DDoS-атаки на серверы LMS.

• Физические сбои оборудования (отказы серверов, выход из строя дисков).

• Блокировка доступа к данным вследствие атак злоумышленников.

7. Меры защиты

7.1 Организационные меры

• Разграничение прав доступа сотрудников по принципу минимально необходимого доступа.

• Регулярное обучение персонала по вопросам кибербезопасности.

• Проведение внутренних аудитов безопасности и тестирование на проникновение.

• Контроль за действиями администраторов через системы логирования и мониторинга.

7.2 Технические меры

• Использование современного шифрования данных (SSL/TLS, AES-256).

• Двухфакторная аутентификация (2FA) для всех критически важных учетных записей.

• Установка антивирусного ПО, межсетевых экранов (firewall), DLP-систем.

• Мониторинг подозрительной активности и автоматизированное реагирование на инциденты.

• Регулярное обновление программного обеспечения для устранения уязвимостей.

7.3 Правовые меры

• Политика конфиденциальности и пользовательские соглашения, включающие механизмы защиты ПДн.

• Заключение договоров с подрядчиками и хостинг-провайдерами, содержащих требования к защите данных.

- Взаимодействие с государственными органами и реагирование на инциденты в соответствии с законодательством РФ.

8. Заключение

Настоящая модель угроз персональных данных разработана для минимизации рисков, связанных с киберугрозами, и обеспечения соответствия требованиям законодательства РФ. Внедрение предложенных мер позволит защитить персональные данные пользователей и предотвратить возможные инциденты.