ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Документ отправлен на официальный сайт: edut.simedu.ru
Уполномоченное лицо – руководитель образовательного учреждения:
Ельцова Татьяна Сергеевна
Действителен с: с 24.04.2026, 07:48
Действителен до: до 18.07.2027, 07:48
Ключ подписи: 10F9103327135FF8F7149A8DBA25426D

УТВЕРЖДЕНО:
Директор МБ УДО «ЦДЮТ»
г. Симферополя
_____ Т.С.Ельцова
Приказ № 46 от 25.05.2026г.

Модель угроз безопасности персональных данных в МБ УДО «ЦДЮТ» г. Симферополя

1. Общие положения

Модель угроз — это документ, описывающий потенциальные угрозы, которым может подвергаться информационная система (ИС) МБ УДО «ЦДЮТ» г. Симферополя при обработке персональных данных (ПДн). Он необходим для:

- разработки системы защиты ПДн,
- проведения анализа рисков,
- формирования перечня организационных и технических мер (ОТМ),
- расчёта показателя Коэффициента защищенности информации (КЗИ).

2. Категории персональных данных в МБ УДО «ЦДЮТ» г. Симферополя

В ИС МБ УДО «ЦДЮТ» г. Симферополя обрабатываются следующие категории ПДн:

- Ученики: ФИО, дата рождения, адрес, паспортные данные (при необходимости), данные о родителях, посещаемость, медицинские данные.
- Сотрудники: ФИО, паспортные данные, СНИЛС, ИНН, табель учёта рабочего времени, данные о заработной плате.
- Родители: ФИО, контактные данные, данные о ребёнке.

3. Источники угроз

№	*Источник угроз*	*Описание*
1	Внутренние пользователи	Сотрудники, ученики, родители, имеющие доступ к ИС. Возможны утечки, ошибки, злонамеренные действия.
2	Внешние злоумышленники	Хакеры, боты, сканеры, целенаправленные атаки (в т.ч. через веб-порталы, электронную почту).
3	Подрядные организации	IT-аутсорсинг, облачные провайдеры, техподдержка — риск через их инфраструктуру.
4	Физические угрозы	Пожар, затопление, кража серверов, несанкционированный доступ в серверную.
5	Технические сбои	Сбои оборудования, ПО, сети, потеря данных из-за сбоев резервного копирования.
6	Социальная инженерия	Фишинг, мошенничество, подмена сотрудников.

4. Перечень угроз безопасности персональных данных

№	*Угроза*	*Классификация*	*Возможные последствия*
1	Несанкционированный доступ к ПДн через учетные записи сотрудников	Внутренняя, техническая	Утечка ПДн, изменение данных
2	Утечка ПДн через съемные носители (флешки, диски)	Внутренняя, организационная	Распространение ПДн в открытом доступе
3	Вредоносное ПО (вирусы, трояны) через email или интернет	Внешняя, техническая	Шифрование данных, утечка, DDoS
4	Фишинговые атаки на сотрудников	Внешняя, социальная	Получение логинов/ паролей, доступ к ИС

№	*Угроза*	*Классификация*	*Возможные последствия*
5	Атаки типа DDoS на веб-портал школы	Внешняя, техническая	Недоступность системы, сбои в работе
6	Несанкционированный доступ к серверу или рабочей станции	Физическая, внутренняя	Кража данных, изменение информации
7	Утеря или кража ноутбука с ПДн	Физическая, внутренняя	Утечка ПДн
8	Ошибки при настройке ПО или политик безопасности	Организационная, внутренняя	Слабая защита, уязвимости
9	Несоблюдение политики паролей	Организационная, внутренняя	Подбор паролей, взлом учетных записей
10	Несвоевременное обновление ПО и ОС	Техническая, внутренняя	Эксплуатация уязвимостей
11	Отсутствие резервного копирования	Техническая, организационная	Потеря данных при сбое
12	Несанкционированный доступ через Wi-Fi	Техническая, внешняя	Перехват трафика, доступ к ИС
13	Удалённый доступ без MFA	Техническая, внутренняя	Взлом привилегированных учетных записей
14	Несанкционированный доступ через подрядчика	Внешняя, техническая	Утечка через стороннюю ИС

5. Уровни защищённости

Для МБ УДО «ЦДЮТ» г. Симферополя, устанавливается второй уровень защищённости ПДн (средний), если:

- обрабатываются ПДн более чем 1000 человек,
- есть доступ к ИС из интернета (АИС «Навигатор», сайт, т.д.).

Требования ко второму уровню включают:

- Обязательное антивирусное ПО на всех устройствах.
- Регулярное резервное копирование.
- Журналирование событий безопасности.
- Разделение прав доступа.
- Парольная политика (минимум 8 символов, смена не реже чем раз в 90 дней).
- Обучение сотрудников основам ИБ.

6. Рекомендуемые меры по защите

1. Организационные меры:

- Утвердить Положение об обеспечении безопасности ПДн.
- Назначить ответственного за ИБ.
- Проводить ежегодное обучение сотрудников.
- Вести журнал учёта инцидентов ИБ.
- Разработать план реагирования на инциденты.

2. Технические меры:

- Установить антивирус на все устройства (ПК, ноутбуки, серверы).
- Организовать резервное копирование (не реже 1 раза в день).
- Включить журналирование событий (логи входа, доступа к ПДн).
- Обеспечить физическую защиту серверной (замки, видеонаблюдение).

3. Контрольные действия:

- Проводить аудит доступов раз в квартал.
- Проверять наличие уязвимостей (сканирование раз в месяц).