

Государственное бюджетное профессиональное
образовательное учреждение
«Соликамский технологический колледж»

УТВЕРЖДАЮ
Директор колледжа
Н. В. Шипулина
« 25 » 2026 г.
Приказ от «25» сентября 2026 г.
№ 2026-24-49-01-05-138



МОДЕЛЬ УГРОЗ

Система менеджмента качества

**БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ
СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В
ГБПОУ «СОЛИКАМСКИЙ ТЕХНОЛОГИЧЕСКИЙ
КОЛЛЕДЖ»**

М СМК 6.4-07-2026



ПОДЛИННИК



КОНТРОЛИРУЕМАЯ КОПИЯ № _____

Соликамск

ГБПОУ «Соликамский технологический колледж»		Положение		М СМК 6.4-07-2026
---	--	-----------	--	-------------------

МОДЕЛЬ УГРОЗ

БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБПОУ «СОЛИКАМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

Дата введения: 2026-09-25

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее — Модель угроз) разработана в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методическим документом ФСТЭК России «Методика оценки угроз безопасности информации» (утв. 05.02.2021);
- Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации».

1.2 Модель угроз определяет перечень возможных угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн) Колледжа, оценку их актуальности и является основой для разработки системы защиты персональных данных.

1.3 Модель угроз подлежит актуализации в случаях:

- изменения законодательства Российской Федерации в области персональных данных;
- изменения архитектуры ИСПДн, состава обрабатываемых данных или категорий субъектов;
- выявления новых угроз безопасности информации;

ГБПОУ «Соликамский технологический колледж»	Положение	М СМК 6.4-07-2026
---	-----------	-------------------

- по результатам анализа инцидентов информационной безопасности;
- не реже одного раза в три года.

2 ОБЪЕКТЫ ЗАЩИТЫ

2.1 К объектам защиты в Колледже относятся:

2.1.1 Персональные данные следующих категорий субъектов:

- работники Колледжа — Ф.И.О., паспортные данные, адрес, сведения об образовании, трудовой стаж, сведения о заработной плате, СНИЛС, ИНН, сведения о воинском учёте;
- обучающиеся — Ф.И.О., дата рождения, адрес, паспортные данные (или данные свидетельства о рождении), сведения об успеваемости, сведения о состоянии здоровья (в объёме, необходимом для образовательного процесса), сведения о родителях (законных представителях);
- законные представители несовершеннолетних обучающихся — Ф.И.О., паспортные данные, адрес, контактные телефоны, место работы;
- абитуриенты — Ф.И.О., дата рождения, данные документа об образовании, контактные данные;
- третьи лица — контрагенты, посетители сайта (в части данных, обрабатываемых с использованием метрик).

2.1.2 Технические средства и системы:

- автоматизированные рабочие места (АРМ) сотрудников колледжа, сетевое оборудование;
- машинные носители информации (жёсткие диски, USB-накопители, резервные копии);
- операционные системы, прикладное программное обеспечение;
- средства защиты информации
- - информационные системы:
 - ЭПОС
 - ЕГИССО
 - ФИС ФРДО
 - ФИС ГИА и Приема
 - ЕИС УФХД ПК
 - Госуслуги
 - сайт ГБПОУ «СТК»
 - Zakupki.GOV.RU
 - МСЭД ПК
 - Цифровая система оценивания ДЭ (ЦСО) и связанные с ней Сервис управления центрами проведения демонстрационного экзамена (ЦПДЭ), Система сбора и синхронизации ресурсов
 - Портал «Работа в России»

ГБПОУ «Соликамский технологический колледж»	Положение	М СМК 6.4-07-2026
---	-----------	-------------------

2.1.3 Помещения и каналы связи:

- помещения, в которых размещены АРМ сотрудников, сетевое оборудование.
- каналы передачи данных (внутренние и внешние).

3 ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЁННОСТИ ИСПДН

3.1 В соответствии с Постановлением Правительства РФ № 1119 определены следующие ИСПДн:

№	Наименование ИСПДн	Категория ПДн	Количество субъектов	Уровень защищённости
1	ЕИС УФХД	Иные категории	менее 100 000	УЗ-3
2	ФИС ГИА и приема	Иные категории	менее 100 000	УЗ-3
3	ФИС ФРДО	Иные категории	менее 100 000	УЗ-3
4	ЕГИССО	Иные категории	менее 100 000	УЗ-3
5	ЭПОС	Иные категории	менее 100 000	УЗ-3
6	Госуслуги	Иные категории	менее 100 000	УЗ-3
7	МСЭД ПК	Иные категории	менее 100 000	УЗ-3
8	сайт ГБПОУ «СТК»	Иные категории	менее 100 000	УЗ-3
9	DE.FIRPO.RU Цифровая платформа (ЦП) по демонстрационному экзамену	Иные категории	менее 100 000	УЗ-3
10	ZAKUPKI.GOV.RU	Иные категории	менее 100 000	УЗ-3
11	Портал «Работа в России»	Иные категории	менее 100 000	УЗ-3

4 ИСТОЧНИКИ УГРОЗ И МОДЕЛЬ НАРУШИТЕЛЯ

4.1 Источниками угроз являются:

- внешние нарушители — лица, не имеющие права доступа к ИСПДн (хакеры, криминальные структуры, конкуренты, иностранные спецслужбы);
- внутренние нарушители — работники Колледжа, обучающиеся, имеющие доступ к ИСПДн;
- техногенные источники — отказы технических средств, сбои программного обеспечения, аварии систем связи;
- природные источники — пожары, наводнения, иные стихийные бедствия.

ГБПОУ «Соликамский технологический колледж»	Положение	М СМК 6.4-07-2026
---	-----------	-------------------

4.2 Модель нарушителя определяется в соответствии с Методикой ФСТЭК России:

Уровень	Тип нарушителя	Возможности	Актуальность для Колледжа
H1	Лица, случайно или по неосторожности нарушившие правила обработки ПДн	Базовые	Актуален
H2	Лица, имеющие доступ к ИСПДн (работники, обучающиеся), с базовыми повышенными возможностями	Использование уязвимостей, фишинг, вредоносное ПО	Актуален
H3	Лица, имеющие доступ к ИСПДн, со средними возможностями	Целенаправленные атаки, использование НДВ	Актуален
H4	Спецслужбы иностранных государств	Высокие	неактуален

4.3 Основные категории нарушителей для Колледжа:

- работники Колледжа, имеющие доступ к ПДн (сотрудники кадров, бухгалтерии, учебной части);
- обучающиеся, имеющие доступ к отдельным информационным ресурсам;
- внешние лица, осуществляющие попытки несанкционированного доступа через сеть «Интернет»;
- подрядные организации, осуществляющие техническое обслуживание ИСПДн.

5 ПЕРЕЧЕНЬ ВОЗМОЖНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Угрозы безопасности персональных данных классифицируются по следующим основаниям:

5.1.1 По природе возникновения:

- техногенные — связанные с отказами и сбоями технических средств;
- антропогенные — связанные с действиями человека (преднамеренными или непреднамеренными);
- природные — связанные с природными явлениями.

5.1.2 По степени преднамеренности:

- преднамеренные — связанные с умышленными действиями нарушителя;
- непреднамеренные — связанные с ошибками персонала, сбоями.

ГБПОУ «Соликамский технологический колледж»		Положение		М СМК 6.4-07-2026
---	--	-----------	--	-------------------

5.1.3 По виду нарушаемого свойства информации:

- угрозы конфиденциальности — утечка, перехват, несанкционированный доступ;
- угрозы целостности — модификация, подмена, искажение данных;
- угрозы доступности — блокирование, уничтожение, отказ в обслуживании.

6 АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 По результатам анализа для ИСПДн Колледжа признаны актуальными следующие угрозы:

6.1.1 Угрозы конфиденциальности

Идентификатор	Наименование угрозы	Объект воздействия	Вероятность	Актуальность
УБИ.001	Угроза несанкционированного доступа к АРМ ПДн через сеть «Интернет»	АРМ	Средняя	Актуальна
УБИ.002	Угроза перехвата ПДн при передаче по открытым каналам связи	Каналы связи	Средняя	Актуальна
УБИ.003	Угроза утечки ПДн через съёмные носители информации	АРМ, USB-порты	Высокая	Актуальна
УБИ.004	Угроза разглашения ПДн работниками Колледжа	Документы, базы данных	Высокая	Актуальна
УБИ.005	Угроза использования слабых паролей и аутентификационной информации	Учётные записи	Высокая	Актуальна

6.1.2 Угрозы целостности

Идентификатор	Наименование угрозы	Объект воздействия	Вероятность	Актуальность
УБИ.006	Угроза модификации ПДн вследствие ошибок персонала при вводе данных	Базы данных	Высокая	Актуальна
УБИ.007	Угроза внедрения вредоносного ПО	АРМ	Средняя	Актуальна
УБИ.008	Угроза подмены данных при передаче по сети	Каналы связи	Низкая	Условно актуальна

ГБПОУ «Соликамский технологический колледж»		Положение		М СМК 6.4-07-2026
--	--	------------------	--	--------------------------

6.1.3 Угрозы доступности

Идентификатор	Наименование угрозы	Объект воздействия	Вероятность	Актуальность
УБИ.009	Угроза отказа в обслуживании (DDoS-атака)	сеть	Низкая	Условно актуальна
УБИ.010	Угроза уничтожения ПДн вследствие отказа оборудования	Жёсткие диски	Средняя	Актуальна
УБИ.011	Угроза блокирования доступа к ПДн вследствие сбоя ПО	Прикладное ПО	Средняя	Актуальна
УБИ.012	Угроза утраты носителей информации	Съемные носители, ноутбуки	Средняя	Актуальна

6.1.4 Угрозы, связанные с использованием технологий искусственного интеллекта и облачных сервисов

Идентификатор	Наименование угрозы	Объект воздействия	Вероятность	Актуальность
УБИ.013	Угроза загрузки ПДн в внешние ИИ-сервисы (нейросети)	Данные, передаваемые в ИИ	Средняя	Актуальна
УБИ.014	Угроза использования облачных сервисов для обработки ПДн без надлежащей защиты	Облачные хранилища	Средняя	Актуальна

6.2 Неактуальными для ИСПДн Колледжа признаны:

- угрозы утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) — ввиду отсутствия в Колледже средств обработки информации, подлежащих защите от ПЭМИН;
- угрозы, связанные с действиями спецслужб иностранных государств (уровень нарушителя Н4) — ввиду отсутствия в ИСПДн информации, представляющей интерес для спецслужб;
- угрозы физического проникновения в контролируемую зону с применением спецсредств — ввиду низкой вероятности.

7 СПОСОБЫ РЕАЛИЗАЦИИ АКТУАЛЬНЫХ УГРОЗ

7.1 Основными способами реализации актуальных угроз являются:

- использование уязвимостей программного обеспечения — эксплуатация известных уязвимостей в ОС, прикладном ПО;
- внедрение вредоносного программного обеспечения — вирусы, трояны, шифровальщики;
- фишинг и социальная инженерия — получение доступа к учётным данным путём обмана работников;
- использование съёмных носителей — копирование ПДн на USB-накопители;
- нарушение правил обработки ПДн — ошибки персонала, разглашение, передача данных третьим лицам без согласия;
- неправомерный доступ к базам данных — внутренний нарушитель с избыточными правами доступа;
- использование внешних ИИ-сервисов — загрузка ПДн в нейросети и облачные сервисы без контроля.

8 ОЦЕНКА РИСКОВ РЕАЛИЗАЦИИ АКТУАЛЬНЫХ УГРОЗ

8.1 Оценка рисков проведена качественным методом по шкале: высокий / средний / низкий.

Угроза	Вероятность	Ущерб	Риск
Утечка ПДн через съёмные носители	Высокая	Высокий	Высокий
Разглашение ПДн работниками	Высокая	Средний	Высокий
Использование слабых паролей	Высокая	Высокий	Высокий
Модификация ПДн вследствие ошибок	Высокая	Средний	Средний
Внедрение вредоносного ПО	Средняя	Высокий	Средний
Отказ оборудования	Высокая	Средний	Средний
Несанкционированный доступ через Интернет	Средняя	Высокий	Средний
Загрузка ПДн в ИИ-сервисы	Средняя	Высокий	Средний
DDoS-атака	Низкая	Средний	Низкий

8.2 Наиболее высокие риски связаны с действиями внутренних нарушителей (работников) и использованием съёмных носителей. Это требует усиления организационных мер контроля доступа и обучения персонала.

9 МЕРЫ ПО НЕЙТРАЛИЗАЦИИ АКТУАЛЬНЫХ УГРОЗ

9.1 Для нейтрализации актуальных угроз применяются следующие меры:

9.1.1 Организационные меры

- назначение ответственного за организацию обработки ПДн;
- утверждение Политики обработки ПДн и Положения об обработке и защите ПДн;
- ознакомление работников с локальными актами под подпись;
- проведение регулярного обучения и инструктажей по вопросам защиты ПДн;

ГБПОУ «Соликамский технологический колледж»	Положение	М СМК 6.4-07-2026
---	-----------	-------------------

- разграничение прав доступа к ПДн на основе принципа минимальной необходимости;

- запрет использования внешних ИИ-сервисов для обработки ПДн без согласования;

- ведение журналов учёта обращений субъектов ПДн и носителей информации;

- контроль соблюдения пропускного режима.

9.1.2 Технические меры

- использование антивирусных средств защиты;

- применение межсетевых экранов;

- шифрование данных при передаче по каналам связи;

- парольная защита и многофакторная аутентификация для привилегированных пользователей;

- ограничение использования USB-портов на АРМ, работающих с ПДн;

- резервное копирование данных;

- регулярное обновление программного обеспечения и установка исправлений безопасности;

- ведение журналов событий безопасности.

9.1.3 Криптографические меры

- использование сертифицированных средств криптографической защиты информации (СКЗИ) при передаче ПДн по открытым каналам связи;

- применение электронной подписи для защиты документов.

9.2 Модель угроз подлежит пересмотру:

- не реже одного раза в три года;

- при изменении законодательства;

- при изменении архитектуры ИСПДн;

- по результатам анализа инцидентов.

9.3 Ответственность за актуализацию Модели угроз возлагается на ответственного за организацию обработки персональных данных.