Приложение № 13

Государственное бюджетное профессиональное образовательное учреждение
«Пермский базовый медицинский колледж»
(ГБПОУ «ПБМК»)

СОГЛАСОВАНО
На заседании педагогического совета ГБПОУ «ПБМК»
протокол № 7 от «10» декабря 2025 г.

УТВЕРЖДАЮ
Директор ГБПОУ «ПБМК»
_____ Е.А. Колесова
«10» декабря 2025 г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
ГБПОУ «ПБМК»

Пермь, 2025

1. Общие положения

1.1. Настоящее Положение определяет цели, задачи, стратегию построения системы защиты персональных данных (далее — СЗПДн) в Государственном бюджетном профессиональном образовательном учреждении «Пермский базовый медицинский колледж» (далее — Оператор, ГБПОУ «ПБМК»), а также требования к обеспечению безопасности персональных данных при их обработке.

1.2. Правовую основу настоящего Положения составляют следующие нормативные правовые акты Российской Федерации (в актуальной редакции):

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями, внесенными Федеральными законами от 24.06.2025 № 156-ФЗ и от 27.02.2025 № 43-ФЗ);

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (вступает в силу с 1 марта 2026 г., но применяется для планирования мероприятий) ;

ГОСТ Р 70262.2-2025 «Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации» (утв. Приказом Росстандарта от 29.05.2025 № 503-ст, введен в действие с 1 октября 2025 г.);

Приказы ФСТЭК России и ФСБ России, регулирующие вопросы защиты информации (в части, не противоречащей актуальному законодательству).

1.3. Настоящее Положение обязательно для исполнения всеми работниками Оператора (штатными, временными, работающими по договорам ГПХ), а также лицами, привлекаемыми к работе с информационными системами Оператора на договорной основе.

1.4. Основные понятия, используемые в Положении, соответствуют терминологии Федерального закона № 152-ФЗ и ГОСТ Р 50922.

2. Цели и задачи системы защиты персональных данных

2.1. Основной целью СЗПДн является обеспечение конфиденциальности, целостности и доступности персональных данных при их обработке, а также предотвращение несанкционированного доступа, уничтожения, модификации, блокирования, копирования и распространения персональных данных.

2.2. Для достижения указанной цели решаются следующие задачи:

- реализация правовых, организационных и технических мер по защите ПДн;
- своевременное выявление и нейтрализация угроз безопасности ПДн;
- контроль доступа к ресурсам информационных систем;
- регистрация и учет действий пользователей;
- непрерывное совершенствование системы защиты.

3. Объекты защиты

3.1. Объектами защиты в ГБПОУ «ПБМК» являются:

- персональные данные работников, обучающихся и иных субъектов, обрабатываемые в информационных системах;

- информационные ресурсы и базы данных, содержащие ПДн;
- программно-технические средства обработки и защиты информации;
- каналы информационного обмена и телекоммуникации;
- помещения, в которых размещены компоненты информационных систем.

4. Принципы построения системы защиты персональных данных

СЗПДн строится на основе следующих принципов:

4.1. Законность. Все меры защиты реализуются в строгом соответствии с требованиями законодательства РФ. Пользователи должны быть осведомлены о порядке работы с защищаемой информацией и ответственности за ее нарушение.

4.2. Системность. Учет всех взаимосвязанных элементов, условий и факторов, влияющих на безопасность ПДн, включая анализ уязвимостей и прогнозирование угроз.

4.3. Комплексность. Согласованное применение организационных, технических, правовых и физических мер защиты, обеспечивающих эшелонированную защиту.

4.4. Непрерывность. Защита ПДн обеспечивается на всех этапах жизненного цикла информационных систем, включая проектирование, ввод в эксплуатацию, сопровождение и вывод из эксплуатации.

4.5. Своевременность. Меры защиты реализуются упреждающе, на ранних стадиях разработки и внедрения информационных систем.

4.6. Преемственность и совершенствование. Постоянное обновление и адаптация системы защиты с учетом изменений угроз, законодательства и опыта эксплуатации.

4.7. Персональная ответственность. Каждый сотрудник несет ответственность за соблюдение требований безопасности в пределах своих полномочий.

4.8. Минимизация полномочий. Пользователям предоставляется минимально необходимый доступ к ПДн для выполнения должностных обязанностей (принцип «все, что не разрешено — запрещено»).

4.9. Гибкость. Средства защиты должны допускать настройку и адаптацию к изменяющимся условиям без нарушения функционирования систем.

4.10. Открытость алгоритмов. Защита не должна основываться исключительно на секретности архитектуры; надежность обеспечивается доказанными методами и средствами.

4.11. Простота применения. Механизмы защиты должны быть интуитивно понятны, автоматизированы и не создавать существенных дополнительных трудозатрат для пользователей.

4.12. Научная обоснованность и техническая реализуемость. Применяемые решения должны соответствовать современному уровню развития науки и техники, быть апробированными и сертифицированными.

4.13. Специализация и профессионализм. К разработке и внедрению мер защиты привлекаются специализированные организации, имеющие соответствующие лицензии ФСТЭК и ФСБ России.

4.14. Обязательность контроля. Все действия пользователей и средств защиты подлежат оперативному контролю и регистрации.

5. Способы и меры обеспечения безопасности персональных данных

5.1. Правовые меры.

Разработка и актуализация локальных актов, регламентирующих обработку и защиту ПДн.

Получение отдельного согласия на обработку персональных данных, оформленного в соответствии с требованиями ч. 1 ст. 9 Федерального закона № 152-ФЗ

(с 1 сентября 2025 г. согласие должно быть выделено отдельно от иных документов и не может содержаться в тексте договоров, правил пользования и т.п.) .

Ведение реестра операторов, уведомление Роскомнадзора о начале обработки ПДн (обязательно с 30 мая 2025 г.).

Обеспечение локализации баз данных при сборе ПДн граждан РФ (использование баз данных, находящихся на территории РФ).

5.2. Морально-этические меры.

Формирование культуры информационной безопасности среди сотрудников.

Проведение разъяснительной работы и тренингов.

5.3. Организационные (административные) меры.

Назначение ответственного за организацию обработки ПДн и администратора безопасности.

Регламентация доступа в помещения, где ведется обработка ПДн.

Разработка инструкций для пользователей и администраторов.

Планирование и проведение внутренних проверок и аудитов.

Обучение сотрудников компетенциям в области информационной безопасности (семинары, тренинги, учебные фишинговые рассылки).

5.4. Физические меры защиты.

Оснащение помещений системами контроля доступа, охранной сигнализацией, видеонаблюдением.

Хранение носителей информации в запираемых шкафах (сейфах).

Контроль доступа посторонних лиц в зоны обработки ПДн.

5.5. Технические (аппаратно-программные) меры.

В соответствии с требованиями ФСТЭК и актуальными стандартами, в состав СЗПДн включаются:

5.5.1. Средства идентификации и аутентификации.

Реализация уровней доверия аутентификации в соответствии с ГОСТ Р 70262.2-2025.

Парольная защита: длина пароля не менее 8 символов (буквы разного регистра, цифры, спецсимволы), смена не реже одного раза в 90 дней. Для привилегированных пользователей рекомендуется двухфакторная аутентификация.

Применение сертифицированных средств при использовании биометрических данных.

5.5.2. Средства разграничения доступа.

Реализация принципа минимальных привилегий.

Управление учетными записями и правами доступа.

5.5.3. Средства обеспечения целостности.

Контроль целостности ПО и данных.

Использование средств резервного копирования и восстановления (регулярное резервирование, хранение резервных копий в защищенном виде).

5.5.4. Средства регистрации и учета.

Регистрация событий входа/выхода, доступа к ресурсам, попыток НСД.

Хранение журналов событий не менее 1 года (в соответствии с политикой безопасности).

5.5.5. Антивирусная защита.

Обязательное применение сертифицированных антивирусных средств на всех узлах ИСПДн.

Централизованное управление и регулярное обновление антивирусных баз.

5.5.6. Межсетевое экранирование.

Фильтрация сетевого трафика на всех уровнях.

Защита периметра сети, контроль служебных протоколов.

5.5.7. Средства обнаружения вторжений и анализа защищенности.

Применение систем обнаружения вторжений (IDS/IPS) для выявления аномальной активности.

Регулярное сканирование уязвимостей и управление обновлениями.

5.5.8. Средства криптографической защиты информации (СКЗИ).

Применение сертифицированных СКЗИ при передаче ПДн по открытым каналам связи (включая организацию VPN).

Защита каналов связи с использованием технологий, сертифицированных ФСБ России.

5.5.9. Средства защиты от утечек по техническим каналам.

Размещение средств отображения информации, исключающее просмотр посторонними лицами.

Контроль побочных электромагнитных излучений и наводок (ПЭМИН) при необходимости.

6. Управление инцидентами и реагирование на угрозы

6.1. Оператор обязан незамедлительно реагировать на инциденты, связанные с нарушением безопасности ПДн.

6.2. В случае выявления инцидента (например, утечки данных) Оператор обязан:

- в течение 24 часов уведомить Роскомнадзор о факте инцидента;
- в течение 72 часов предоставить результаты внутреннего расследования.

6.3. При утечках, затрагивающих более 1000 субъектов, применяются повышенные меры реагирования и штрафные санкции (до 15 млн рублей).

7. Ответственность

7.1. Лица, виновные в нарушении требований настоящего Положения и законодательства РФ о персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

7.2. Административные штрафы за нарушения в области ПДн в 2025 году могут составлять:

- за отсутствие уведомления или согласия — до 300 000 рублей на оператора;
- за нарушение порядка получения письменного согласия — до 700 000 рублей;
- за утечку персональных данных — до 15 млн рублей.

7.3. Субъекты персональных данных вправе требовать возмещения морального вреда и убытков в судебном порядке.