Приложение № 11

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 ПОЛИТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ГБПОУ «ПБМК»

Пермь, 2025

1. Общие положения

Настоящая Политика информационной безопасности (далее — Политика) Государственного бюджетного профессионального образовательного учреждения «Пермский базовый медицинский колледж» (далее — Оператор, ГБПОУ «ПБМК») определяет цели, задачи, принципы и направления обеспечения безопасности персональных данных и иной конфиденциальной информации, обрабатываемой в информационных системах колледжа.

Политика разработана в соответствии с требованиями следующих нормативных правовых актов Российской Федерации:

—Конституция Российской Федерации;

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

—Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

—Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (в части, касающейся объектов КИИ);

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

—Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

—Приказы ФСТЭК России и ФСБ России, регулирующие вопросы защиты информации (в т.ч. Приказ ФСТЭК № 21, № 17, № 31, Приказ ФСБ России № 378 и др.).

Политика устанавливает требования к персоналу, допущенному к обработке информации, определяет структуру системы защиты, ответственность сотрудников и порядок действий для обеспечения конфиденциальности, целостности и доступности информации.

Целью Политики является защита субъектов персональных данных от угроз безопасности информации, минимизация ущерба от возможных инцидентов, а также обеспечение соответствия Оператора требованиям законодательства РФ.

2. Область действия

Требования настоящей Политики обязательны для исполнения всеми работниками Оператора (штатными, временными, работающими по договорам ГПХ), а также лицами, привлекаемыми к работе с информационными системами Оператора на договорной основе (подрядчики, волонтеры, практиканты).

3. Система защиты информации

Система защиты информации (СЗИ) Оператора строится на основании следующих организационно-распорядительных и технических документов:

—Перечня информации, подлежащей защите (включая персональные данные).

—Акта классификации информационных систем персональных данных (ИСПДн).

—Модели угроз безопасности информации (частной модели актуальных угроз и вероятного нарушителя).

—Положения о разграничении прав доступа.

—Технической документации на средства защиты информации (СЗИ), имеющих действующие сертификаты ФСТЭК/ФСБ России.

На основе проведенного анализа угроз и класса ИСПДн Оператор определяет необходимый уровень защищенности и реализует организационные и технические меры защиты, которые фиксируются в Плане мероприятий по защите информации.

Организационные меры включают:

—Наличие правовых оснований для обработки данных (согласия, договоры, локальные акты);

—Назначение ответственного за организацию обработки персональных данных и ответственного за обеспечение безопасности информации;

—Регламентацию процессов обработки информации как с использованием средств автоматизации, так и без них;

—Контроль физической защиты объектов, съемных носителей и порядка уничтожения информации.

Технические меры могут включать:

—Средства защиты от несанкционированного доступа;

—Средства антивирусной защиты;

—Межсетевые экраны (Next-Generation Firewall);

—Средства криптографической защиты информации (при передаче данных по открытым каналам связи);

—Средства предотвращения утечек данных (DLP-системы);

—Средства анализа защищенности (сканирования уязвимостей) и обнаружения вторжений (IDS/IPS).

4. Требования к подсистемам безопасности

Система защиты информации Оператора включает функциональные подсистемы, реализуемые в зависимости от класса защищенности ИСПДн:

4.1. Подсистема управления доступом, регистрации и учета

Должна обеспечивать:

—Идентификацию и аутентификацию пользователей (пароль не менее 8 символов, включая буквы разного регистра, цифры и спецсимволы; рекомендуется внедрение двухфакторной аутентификации для привилегированных пользователей).

—Регистрацию событий входа/выхода из системы, доступа к ресурсам, попыток несанкционированного доступа в журналах (логах) событий.

—Учет и маркировку машинных носителей информации, содержащих защищаемые данные.

4.2. Подсистема обеспечения целостности и доступности

Должна обеспечивать:

—Контроль целостности программного обеспечения СЗИ и критичных компонентов ОС (по контрольным суммам).

—Физическую защиту серверного и сетевого оборудования, а также помещений, где обрабатывается информация (контроль доступа, видеонаблюдение).

—Регулярное резервное копирование данных и СЗИ с возможностью восстановления.

—Периодическое тестирование функций СЗИ.

4.3. Антивирусная защита

Обязательна для всех узлов ИСПДн (рабочие станции, серверы), имеющих подключение к сетям общего пользования или использующих съемные носители. Используемые средства должны иметь централизованное управление и регулярно обновляться.

4.4. Межсетевое экранирование

Должно обеспечивать фильтрацию сетевого трафика на всех уровнях, контроль за служебными протоколами, аутентификацию администраторов межсетевых экранов и регистрацию их действий.

4.5. Анализ защищенности и обнаружение вторжений

В зависимости от класса системы могут применяться средства сканирования уязвимостей и системы обнаружения/предотвращения вторжений (IDS/IPS) для выявления аномальной активности.

4.6. Защита от утечек по техническим каналам (ТКУИ)

Размещение средств отображения информации (мониторов) должно исключать возможность ее просмотра посторонними лицами.

5. Категории пользователей информационных систем

В ИСПДн Оператора выделяются следующие категории пользователей:

5.1. Администраторы безопасности ИСПДн

Штатный сотрудник, назначенный приказом директора, ответственный за функционирование СЗИ.

Уровень доступа: Полная информация об ИСПДн, права администратора, доступ к управлению средствами защиты.

Полномочия: Настройка СЗИ, управление учетными записями, аудит событий безопасности, расследование инцидентов.

5.2. Пользователи ИСПДн

Штатные сотрудники, осуществляющие обработку данных в рамках своих должностных обязанностей (ввод данных, формирование отчетов и т.п.).

Уровень доступа: Доступ только к тем данным и функциям, которые необходимы для выполнения служебных задач (принцип минимальных привилегий).

5.3. Системные администраторы (технические специалисты)

Сотрудники (штатные или аутсорсинговых компаний), обеспечивающие работоспособность инфраструктуры (серверы, СКС, АРМ).

Ограничения: Не имеют прав на управление средствами защиты информации, если это не входит в их функции, согласованные с администратором безопасности. Их деятельность по настройке системы должна протоколироваться.

Примечание: Актуальные списки групп пользователей, их полномочия и уровни доступа фиксируются в «Положении о разграничении прав доступа».

6. Обязанности сотрудников по обеспечению безопасности

Все сотрудники Оператора обязаны:

—Знать и строго выполнять требования настоящей Политики и иных локальных актов по защите информации.

—При трудоустройстве проходить инструктаж под подпись.

—Обеспечивать сохранность аутентификационных данных (паролей, ключей, токенов). Запрещается передавать их третьим лицам и записывать на видных местах.

—Использовать сложные пароли и своевременно их менять.

—Блокировать рабочую станцию при прекращении работы (клавиши Win + L).

—Немедленно сообщать администратору безопасности или руководителю о подозрительных действиях, инцидентах, потере идентификаторов.

—Соблюдать требования по физической защите оборудования.

Сотрудникам запрещается:

—Устанавливать неучтенное программное обеспечение.

—Подключать личные устройства (ноутбуки, смартфоны, флешки) к АРМ и серверам без разрешения администратора.

—Выносить носители информации за пределы контролируемой зоны без разрешения.

—Разглашать защищаемую информацию, ставшую известной в процессе работы, третьим лицам, в том числе в мессенджерах и социальных сетях.

—Оставлять документы и носители с защищаемой информацией на рабочих столах без присмотра.

7. Ответственность сотрудников

В соответствии со ст. 24 Федерального закона № 152-ФЗ «О персональных данных» и иными нормативными актами РФ, лица, виновные в нарушении требований законодательства при работе с персональными данными, несут **дисциплинарную, административную, гражданско-правовую или уголовную** ответственность.

Администраторы безопасности несут персональную ответственность за действия, совершенные с использованием их учетных записей и вверенных им систем, если не доказан факт несанкционированного использования.

За нарушение правил эксплуатации средств хранения, обработки или передачи информации, повлекшее уничтожение, блокирование или модификацию данных, сотрудники могут быть привлечены к ответственности в соответствии с Трудовым кодексом РФ и КоАП РФ.