Автономная некоммерческая профессиональная образовательная организация «Межрегиональный медицинский колледж» (АНПОО «ММК»)

Принято:
Правлением колледжа
АНПОО «ММК»
Протокол №5 от 03.03.2026г.

Утверждено:
Директор
_____ Жукова Н.А.
«03» 03 2026 г.
Приказ №16 от 03.03.2026

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0227159C0002B342AD4CCAA950C3095308
Владелец: ЖУКОВА НАТАЛЬЯ АЛЕКСАНДРОВНА
Действителен: с 20.06.2025 до 20.09.2026

ПОЛИТИКА
в области информационной безопасности в Автономной некоммерческой профессиональной образовательной организации «Межрегиональный медицинский колледж» АНПОО «ММК»

Ессентуки

2026г.

1. Общие положения

1.1. Политика в области информационной безопасности (далее - Политика) регламентирует процессы обеспечения информационной безопасности в Автономной некоммерческой профессиональной образовательной организации «Межрегиональный медицинский колледж» АНПОО «ММК» (далее –АНПОО «ММК», Колледж), в соответствии с требованиями законодательства Российской Федерации в области информационной безопасности,

1.2. Основные понятия, используемые в Политике:

Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования.

Доступность информации – состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность – состояние защищенности интересов Колледжа.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационный ресурс (актив) – все, что имеет ценность и находится в распоряжении Колледжа.

Инцидент информационной безопасности – одно или серия нежелательных или неожиданных событий безопасности, представляющих угрозу ИБ.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – состояние защищенности информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Несанкционированный доступ – доступ к информации иди действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Политика – общие цели и указания, формально выраженные руководством.

Система управления информационной безопасностью – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

События информационной безопасности – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

2. Цели и задачи.

3.1 Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов Колледжа от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация рисков информационной безопасности.

3.2 Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, и прогнозирование источников угроз информационной безопасности;
- создание механизма оперативного реагирования на угрозы информационной безопасности;
- предотвращение и/или снижение ущерба от реализации угроз информационной безопасности;
- защита от вмешательства в процесс функционирования информационной системы посторонних лиц;
- соответствие требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части информационной безопасности;
- достижение адекватности мер по защите от угроз ИБ;
- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;

• выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников.

4 Область применения.

4.1 Настоящая Политика распространяется на все процессы и обязательна для применения всеми работниками и руководством Колледжа, а также пользователями его информационных ресурсов.

4.2 Каждый работник обязан поддерживать конфиденциальность и целостность деловой информации Колледжа и защищать эту информацию от несанкционированного, незаконного или случайного раскрытия, искажения или уничтожения.

5. Объекты обеспечения информационной безопасности

5.1. В рамках обеспечения информационной безопасности объектами защиты в Колледже является информация, обрабатываемая в Колледже, вне зависимости от формы представления; информационные активы, включая, но не ограничиваясь следующим перечнем:

- автоматизированные рабочие места, средства обработки информации и мобильные технические средства;
- информационные системы, системы хранения данных, программное обеспечение и отдельные технические решения;
- автоматизированные системы;
- информационно-технологическая инфраструктура;
- информационно - телекоммуникационные сети и системы связи;

6. Объекты защиты.

6.1. В Колледже реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

6.2. В Колледже присутствуют следующие типы ресурсов:

• информационные системы и ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Колледжа;

• открыто распространяемая информация, публикуемая в интернет ресурсах, на сайтах Колледжа;

• информационная инфраструктура, включая технические и программные средства, каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

7. Система управления информационной безопасностью (СУИБ).

7.1. Для достижения указанных целей и задач в Колледже внедряется система управления информационной безопасностью.

7.2 СУИБ документирована в настоящей Политике, в правилах, рабочих инструкциях, которые являются обязательными для всех работников Колледжа в области действия системы. Документированные требования СУИБ доводятся до сведения работников Колледжа.

8. Ответственность за нарушения в области информационной безопасности.

8.1. Работники Колледжа должны выполнять требования и правила информационной безопасности при работе с информацией, в том числе касающейся самих работников, соискателей, родственников работников, уволенных работников, студентов, обучающихся, законных представителей, контрагентов.

8.2. Требования распорядительных документов и правил обеспечения информационной безопасности обязательны для всех без исключения работников Колледжа и должны учитываться во взаимоотношениях указанными лицами.

8.3. Руководство Колледжа возлагает ответственность на руководителей структурных подразделений Колледжа за организацию повседневной деятельности и выделение необходимых ресурсов для обеспечения информационной безопасности как неотъемлемой составляющей Процессов Колледжа.

8.4. При использовании сети Интернет, при общении в социальных сетях и мессенджерах, использовании электронной почты, сайтов, других средств телекоммуникаций и мобильных технических средств работникам Колледжа рекомендуется проявлять осмотрительность и сдержанность, чтобы не допускать рисков личной безопасности, а также избегать непреднамеренной утечки рабочей информации.

8.5. Каждый работник Колледжа за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

9. Управление инцидентами информационной безопасности.

9.1. Пользователи информационных систем и ресурсов Колледжа должны сообщать Руководству Колледжа о любых замеченных или подозреваемых недостатках безопасности в системах или услугах как можно быстрее.

9.2. Пользователи ни при каких обстоятельствах не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

9.3. Все инциденты информационной безопасности должны быть идентифицированы, зафиксированы, доведены до соответствующих служб и решены (минимизированы негативные последствия).

10. Заключительные положения.

10.1 Настоящая Политика вступает в силу с даты ее утверждения.

10.2 Требования настоящей Политики могут расширяться другими локальными нормативными документами Колледжа, которые дополняют и уточняют ее.

10.3 В случае изменения действующего законодательства и иных нормативных актов, а также Устава Колледжа настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Колледжа.

по защите информации или рабочей группой по пересмотру Политики.

10.4. Изменения и дополнения Политики утверждаются директором Колледжа либо лицом, его замещающим.