

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ КАМЧАТСКОГО КРАЯ

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КАМЧАТСКОГО КРАЯ
«КАМЧАТСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»**



ПОЛИТИКА ЗАЩИТЫ ИНФОРМАЦИИ

Государственного бюджетного профессионального образовательного учреждения
Камчатского края «Камчатский медицинский колледж»

Петропавловск-Камчатский, 2026 год

I. Общие положения

1.. Настоящая Политика защиты информации Государственного бюджетного профессионального образовательного учреждения Камчатского края «Камчатский медицинский колледж» (далее соответственно – Политика, ГБПОУ КК «КМедК», Колледж) определяет цели, принципы, область действия, организационную систему управления и основные направления деятельности по защите информации в ГБПОУ КК «КМедК».

2. Политика разработана с учетом Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119, приказа ФСТЭК России от 11.04.2025 № 117 в действующей редакции, а также иных применимых нормативных правовых, нормативных и методических документов в области защиты информации.

3. Политика является документом верхнего уровня. Конкретные требования к эксплуатации информационных систем, использованию средств вычислительной техники, программного обеспечения, сети Интернет, электронной почты, удаленного доступа, средств защиты информации, резервному копированию, управлению учетными записями, обработке инцидентов и иным процессам устанавливаются внутренними стандартами, регламентами, положениями, инструкциями, распорядительными и техническими документами ГБПОУ КК «КМедК».

4. До приведения ранее утвержденных локальных документов в соответствие с настоящей Политикой они применяются в части, не противоречащей законодательству Российской Федерации, обязательным требованиям по защите информации и настоящей Политике.

5. Настоящая Политика не изменяет установленное законодательством Российской Федерации, трудовыми договорами, должностными инструкциями и распорядительными документами ГБПОУ КК «КМедК» распределение полномочий и ответственности. Конкретные специальные функции по защите информации закрепляются за работниками в установленном порядке.

II. Область действия и объекты защиты

6. Политика распространяется на информацию, информационные системы и компоненты информационно-телекоммуникационной инфраструктуры, находящиеся в сфере ответственности ГБПОУ КК «КМедК» и подлежащие защите в соответствии с применимыми требованиями.

7. К защищаемой информации относятся персональные данные, иная информация ограниченного доступа, а также информация, нарушение целостности или доступности которой может повлечь нарушение деятельности ГБПОУ КК «КМедК», прав и законных интересов граждан, работников, обучающихся или иных лиц.

8. К объектам защиты относятся информационные системы, серверы, рабочие станции, мобильные и переносные устройства, сетевое оборудование, локальные вычислительные сети, средства хранения и резервного копирования, программное обеспечение, базы данных,

средства защиты информации, средства аутентификации, каналы связи, облачные и иные сервисы в пределах ответственности ГБПОУ КК «КМедК».

9. Перечень категорий информации, информационных систем и компонентов информационно-телекоммуникационной инфраструктуры, попадающих под действие Политики, приведен в приложении № 1 к настоящей Политике.

10. Конкретный состав информационных систем и объектов защиты, их назначение, владельцы (операторы), используемые компоненты, категории обрабатываемой информации, ответственные лица и иные учетные сведения определяются отдельными реестрами, перечнями, паспортами, моделями угроз, актами, приказами и иными документами ГБПОУ КК «КМедК» и актуализируются при изменении состава или условий эксплуатации.

11. Отдельно формируется и поддерживается в актуальном состоянии перечень информационных систем, в которые осуществляется передача информации из государственных информационных систем, с указанием категорий передаваемой информации, если такая передача осуществляется.

III. Цели, задачи и принципы защиты информации

12. Целями защиты информации являются обеспечение конфиденциальности, целостности и доступности информации в соответствии с установленными требованиями; устойчивое и безопасное функционирование информационных систем; предотвращение неправомерного доступа, уничтожения, изменения, блокирования, копирования, предоставления и распространения информации; снижение рисков реализации угроз безопасности информации.

13. Основными задачами являются выявление и оценка угроз, планирование и реализация организационных и технических мер, управление доступом, применение средств защиты информации, обеспечение резервного копирования и восстановления, управление уязвимостями и обновлениями, регистрация и анализ событий безопасности, выявление и обработка инцидентов, обучение пользователей, контроль и совершенствование защиты.

14. Защита информации осуществляется на основе законности, обоснованности и соразмерности мер, разграничения полномочий, минимально необходимых прав доступа, документирования существенных решений, регулярного контроля, учета фактической зоны технического управления ГБПОУ КК «КМедК» и применения специальных компетенций и лицензий в случаях, когда это обязательно.

15. Полномочия по организации, управлению, контролю и непосредственному выполнению мероприятий по защите информации разграничиваются. Возложение на работника функций по координации или контролю не прекращает обязанностей иных работников, которым конкретные функции непосредственно закреплены должностными инструкциями или распорядительными документами.

16. При недостаточности собственных ресурсов, компетенций, технических средств либо при обязательности специальных лицензий, независимой оценки или иных условий ГБПОУ КК «КМедК» в установленном порядке привлекает специализированные организации и специалистов.

IV. Организационная система управления защитой информации

17. Организационная система управления защитой информации включает директора ГБПОУ КК «КМедК»; заместителя директора, на которого распорядительным документом возложены организация деятельности по защите информации, управление данной деятельностью и контроль; Отдел информационных технологий; специалиста (техника) по защите информации; иных работников, назначенных ответственными по отдельным направлениям; руководителей структурных подразделений; пользователей информационных систем.

18. Директор ГБПОУ КК «КМедК» утверждает Политику и иные локальные документы, определяет организационную систему управления защитой информации, назначает ответственных лиц, принимает решения о ресурсах, финансировании и привлечении специализированных организаций, рассматривает информацию о существенных рисках и инцидентах.

19. Заместитель директора, на которого возложены соответствующие полномочия, организует деятельность по защите информации на уровне ГБПОУ КК «КМедК», осуществляет управление данной деятельностью и контроль ее выполнения в пределах предоставленных полномочий, координирует взаимодействие структурных подразделений и ответственных работников.

20. Отдел информационных технологий организует и координирует работы по обеспечению информационной безопасности и безопасности персональных данных в пределах своей компетенции и во взаимодействии с работниками, назначенными ответственными по соответствующим направлениям.

21. Начальник Отдела ИТ организует выполнение относящихся к компетенции Отдела ИТ мероприятий, распределяет задачи между работниками с учетом их должностных обязанностей, квалификации и закрепленных направлений деятельности, контролирует исполнение, обеспечивает взаимодействие с ответственными работниками и специализированными организациями, своевременно информирует руководство о существенных рисках, инцидентах, недостаточности ресурсов и необходимости управленческих решений.

22. Специалист (техник) по защите информации выполняет мероприятия по защите информации в пределах должностной инструкции, предоставленных полномочий и закрепленных распорядительными документами направлений, участвует в ведении документации, контроле функционирования средств защиты, обследовании объектов, подготовке к аттестации, анализе инцидентов и внутреннем контроле.

23. Функции по организации обработки персональных данных, обеспечению безопасности персональных данных в информационных системах, эксплуатации средств криптографической защиты информации и иным специальным направлениям выполняются работниками, которым соответствующие полномочия непосредственно предоставлены законодательством, должностными инструкциями и (или) распорядительными документами ГБПОУ КК «КМедК».

24. Руководители структурных подразделений определяют служебную необходимость доступа работников подразделения к информационным ресурсам, своевременно сообщают об

изменении должностных функций, переводе или увольнении работников, обеспечивают соблюдение требований защиты информации в подразделении в пределах своих полномочий.

25. Пользователи информационных систем обязаны соблюдать установленные требования, использовать доступ только в служебных целях, обеспечивать сохранность средств аутентификации и незамедлительно сообщать о выявленных или предполагаемых инцидентах установленным способом.

V. Основные направления защиты информации

26. ГБПОУ КК «КМедК» организует учет и инвентаризацию информационных систем, программных и программно-аппаратных средств, средств защиты информации и иных объектов, значимых для обеспечения защиты информации.

27. Доступ пользователей предоставляется на основании служебной необходимости, по принципу минимально необходимых прав и с учетом установленного порядка создания, изменения, блокирования и удаления учетных записей и средств аутентификации.

28. Для информационных систем устанавливаются и поддерживаются требования к конфигурациям, разрешенному программному обеспечению, подключению к сети Интернет, удаленному доступу, использованию мобильных устройств и внешних носителей, а также к подключению иных информационных систем.

29. Организуются получение, оценка, тестирование и применение обновлений; выявление, оценка и устранение уязвимостей; антивирусная защита; регистрация и анализ событий безопасности; резервное копирование и восстановление; физическая защита; контроль подключения и эксплуатации оборудования.

30. Служебная информация и информация ограниченного доступа обрабатываются, передаются и хранятся с использованием разрешенных ГБПОУ КК «КМедК» информационных систем, средств связи и сервисов с учетом установленных ограничений.

31. При предоставлении подрядным организациям доступа к информационным системам или содержащейся в них информации условия такого доступа, обязанность соблюдать применимые требования защиты информации, объем полномочий и порядок прекращения доступа определяются документально.

32. При использовании внешних информационных систем, облачных платформ и сервисов, не находящихся под техническим управлением ГБПОУ КК «КМедК», меры защиты реализуются в пределах распределения ответственности между Колледжем и оператором соответствующего сервиса.

VI. Документирование, внутренние стандарты и регламенты

33. В развитие настоящей Политики разрабатываются и актуализируются внутренние стандарты и регламенты по защите информации в объеме, определяемом законодательством Российской Федерации, обязательными требованиями, составом информационных систем и фактическими процессами ГБПОУ КК «КМедК».

34. Внутренние стандарты устанавливают требования к управлению доступом, идентификации и аутентификации, разрешенному программному обеспечению, типовым конфигурациям, подключению к сети Интернет, удаленной работе, конечным и мобильным

устройствам, непрерывности, резервному копированию, регистрации событий и иным мерам защиты.

35. Внутренние регламенты устанавливают порядок выполнения процессов, включая управление учетными и привилегированными учетными записями, средствами аутентификации, удаленным доступом, доступом подрядчиков и иных организаций, Интернет-доступом, обучением пользователей, уязвимостями, обновлениями, информацией ограниченного доступа, физической защитой и обработкой инцидентов.

36. Необходимость разработки отдельных документов по специальным направлениям, включая персональные данные и криптографическую защиту, определяется применимыми требованиями и фактически используемыми средствами, и системами.

37. Документы утверждаются директором ГБПОУ КК «КМедК» либо иным уполномоченным лицом в пределах предоставленных полномочий и доводятся до работников и подрядных организаций в части, их касающейся.

VII. Оценка состояния защиты, аттестация и совершенствование

38. Состояние защиты информации оценивается с применением действующих нормативных и методических документов уполномоченных органов в объеме, применимом к информационным системам ГБПОУ КК «КМедК».

39. Необходимость аттестации информационных систем и объектов информатизации либо проведения иных мероприятий по оценке соответствия определяется исходя из применимых обязательных требований, статуса информационной системы, категории обрабатываемой информации и условий ее эксплуатации.

40. Отдел ИТ и специалист по защите информации в пределах своих полномочий организуют и осуществляют подготовительные мероприятия, предоставление технических сведений, подготовку объектов и документации и взаимодействие со специализированными организациями.

41. Работы, для выполнения которых законодательством установлено обязательное наличие лицензии или иного разрешения, выполняются лицами и организациями, имеющими соответствующие действующие лицензии или разрешения.

42. По результатам контроля, оценки состояния защиты, аттестации, обследований, инцидентов и иных мероприятий формируются предложения по устранению выявленных недостатков и совершенствованию защиты информации с определением при необходимости сроков, ответственных исполнителей и потребности в ресурсах.

VIII. Планирование и ресурсное обеспечение

43. Мероприятия по защите информации планируются с учетом обязательных требований, результатов оценки состояния защиты, выявленных угроз и уязвимостей, изменений информационных систем, сроков эксплуатации средств защиты и потребности в обучении работников.

44. При формировании потребности в бюджетном финансировании предусматриваются расходы на приобретение, сопровождение и обновление средств защиты информации, проведение необходимых аттестационных и иных специализированных работ,

обучение работников и иные мероприятия, обязательные или обоснованно необходимые для защиты информации.

45. Структурные подразделения и специалисты, участвующие в защите информации, представляют руководству обоснованные предложения о необходимых организационных, материально-технических и иных ресурсах, включая возможные последствия их отсутствия.

46. При выявлении невозможности надлежащего выполнения обязательного мероприятия имеющимися силами, средствами или в установленные сроки соответствующее должностное лицо обязано своевременно информировать руководство ГБПОУ КК «КМедК» и представить предложения о необходимых управленческих решениях.

IX. Обучение и осведомленность

47. Работники, на которых возложены функции по защите информации, должны обладать компетенциями, необходимыми для выполнения закрепленных обязанностей, и проходить обучение, повышение квалификации или профессиональную переподготовку в случаях и объеме, предусмотренных применимыми требованиями.

48. Пользователи информационных систем знакомятся с требованиями защиты информации в части, необходимой для выполнения должностных обязанностей, и проходят предусмотренные ГБПОУ КК «КМедК» мероприятия по повышению осведомленности.

49. Ознакомление работников с обязательными для них локальными документами осуществляется в установленном в ГБПОУ КК «КМедК» порядке.

X. Инциденты информационной безопасности

50. ГБПОУ КК «КМедК» устанавливает порядок выявления, регистрации, классификации, эскалации, локализации, устранения последствий и анализа инцидентов информационной безопасности.

51. Работник, обнаруживший признаки возможного нарушения защиты информации, обязан незамедлительно сообщить об этом установленным способом и не предпринимать самостоятельных действий, способных затруднить расследование или увеличить ущерб, кроме действий, прямо предусмотренных инструкциями.

52. Технические и организационные мероприятия по обработке инцидента выполняются работниками в пределах их компетенции и полномочий. Существенные инциденты и риски доводятся до директора ГБПОУ КК «КМедК» и должностного лица, осуществляющего организацию и контроль деятельности по защите информации.

53. Уведомление государственных органов, операторов информационных систем, субъектов персональных данных или иных лиц осуществляется в случаях и порядке, установленных законодательством Российской Федерации, уполномоченным на это должностным лицом.

XI. Контроль и ответственность

54. Контроль выполнения требований настоящей Политики осуществляется в пределах предоставленных полномочий директором ГБПОУ КК «КМедК», ответственным

должностным лицом, Отделом ИТ, специалистом по защите информации и иными работниками, которым соответствующие контрольные функции закреплены документально.

55. Работники несут ответственность за нарушение требований законодательства Российской Федерации и локальных нормативных актов в пределах, предусмотренных законодательством, их должностными обязанностями и предоставленными полномочиями.

56. Начальник Отдела ИТ отвечает за организацию деятельности Отдела ИТ, обоснованное распределение задач между работниками, контроль исполнения порученных работ и своевременное информирование руководства о существенных рисках, инцидентах, недостаточности ресурсов или невозможности надлежащего выполнения отдельных работ имеющимися силами и средствами – в пределах предоставленных полномочий.

57. Работники Отдела ИТ и иные ответственные работники несут персональную ответственность за надлежащее исполнение функций и обязанностей, непосредственно закрепленных за ними трудовыми договорами, должностными инструкциями, дополнительными соглашениями, приказами и иными распорядительными документами.

58. Ответственность за отдельные направления информационной безопасности, обработки персональных данных, технической и криптографической защиты информации и иные специальные функции определяется документами, которыми соответствующие обязанности закреплены за конкретными работниками.

59. Выявленные нарушения и недостатки подлежат документированию и устранению в порядке и сроки, определенные уполномоченным должностным лицом с учетом их критичности и доступных ресурсов.

XII. Заключительные положения

60. Настоящая Политика вступает в силу с даты ее утверждения.

61. Политика подлежит пересмотру при изменении законодательства и обязательных требований, организационной структуры, состава информационных систем, характера обрабатываемой информации, распределения полномочий либо при выявлении необходимости по результатам контроля и инцидентов.

62. Изменения и дополнения в Политику утверждаются в установленном в ГБПОУ КК «КМедК» порядке.

ПЕРЕЧЕНЬ КАТЕГОРИЙ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ СИСТЕМ И КОМПОНЕНТОВ, ПОДЛЕЖАЩИХ ЗАЩИТЕ

	Категория	Состав
1	Информация	Персональные данные; иная информация ограниченного доступа; служебная информация; сведения, нарушение целостности или доступности которых способно нарушить деятельность Колледжа.
2	Информационные системы	Информационные системы персональных данных; государственные и иные информационные системы, используемые ГБПОУ КК «КМедК» в пределах его полномочий; корпоративные, прикладные и учетные информационные системы, находящиеся в зоне ответственности Колледжа.
3	Серверная инфраструктура	Физические и виртуальные серверы, серверные операционные системы, базы данных, файловые ресурсы, службы каталогов и иные серверные компоненты.
4	Рабочие и мобильные устройства	Рабочие станции, ноутбуки и иные конечные устройства, используемые для доступа к защищаемой информации и информационным системам.
5	Сетевая инфраструктура и связь	Локальные сети, маршрутизаторы, коммутаторы, точки беспроводного доступа, межсетевые средства, каналы связи и иные компоненты, обеспечивающие передачу данных.
6	Программное обеспечение и сервисы	Операционные системы, прикладное и серверное программное обеспечение, корпоративная электронная почта, системы обмена сообщениями, веб-сервисы и иные сервисы в пределах ответственности ГБПОУ КК «КМедК».
7	Средства защиты информации	Антивирусные средства, средства разграничения доступа, регистрации событий, криптографической и иной защиты информации, используемые в соответствии с установленными требованиями.
8	Средства хранения и резервного копирования	Системы резервного копирования, сетевые и локальные хранилища, съемные носители и иные средства, на которых хранится защищаемая информация.
9	Облачные и внешние сервисы	Сервисы и информационные системы сторонних операторов, используемые ГБПОУ КК «КМедК», в части ответственности и полномочий Колледжа.

Примечание. Конкретные наименования, идентификаторы, владельцы (операторы), ответственные лица, категории обрабатываемой информации, технический состав и статус оценки соответствия конкретных информационных систем и объектов фиксируются в отдельных актуализируемых учетных и организационно-распорядительных документах ГБПОУ КК «КМедК».