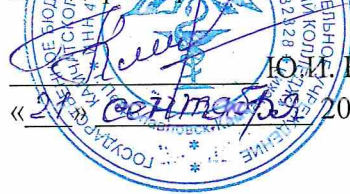


МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ КАМЧАТСКОГО КРАЯ

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

УТВЕРЖДАЮ

И.о. директора ГБПОУ КК «КМедК»



Ю.И. Климова

«21 сентября» 2026 г.

**ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

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

Петропавловск-Камчатский, 2026 год

I. Общие положения

1. Настоящее Положение об информационной безопасности Государственного бюджетного профессионального образовательного учреждения Камчатского края «Камчатский медицинский колледж» (далее соответственно – Положение, ГБПОУ КК «КМедК», Колледж) устанавливает обязательные организационные и эксплуатационные правила безопасного использования информационных систем, информационно-телекоммуникационной инфраструктуры, средств вычислительной техники, программного обеспечения и информационных ресурсов ГБПОУ КК «КМедК».

2. Положение разработано в развитие Политики защиты информации ГБПОУ КК «КМедК» и применяется совместно с иными локальными нормативными, организационно-распорядительными, техническими и эксплуатационными документами по защите информации.

3. Требования Положения обязательны для работников ГБПОУ КК «КМедК», обучающихся и иных лиц в части предоставленного им доступа к информационным системам и ресурсам Колледжа, а также для работников подрядных организаций в части, установленной договорными и иными документами.

4. Конкретные специальные обязанности по защите информации выполняются работниками, которым они закреплены должностными инструкциями и (или) распорядительными документами. Сам факт использования информационных технологий либо работы в Отделе ИТ не означает возложения всех специальных функций по защите информации на одного работника.

5. Вопросы, не урегулированные настоящим Положением, регулируются Политикой защиты информации, специализированными регламентами и инструкциями ГБПОУ КК «КМедК», а также применимыми требованиями законодательства Российской Федерации.

II. Основные обязанности участников

6. Директор ГБПОУ КК «КМедК» принимает управленческие решения по вопросам защиты информации в пределах своих полномочий, утверждает локальные документы и назначает ответственных лиц.

7. Заместитель директора, на которого возложены организация деятельности по защите информации, управление данной деятельностью и контроль, координирует выполнение соответствующих мероприятий на уровне ГБПОУ КК «КМедК».

8. Отдел ИТ организует и координирует технические и организационные работы по защите информации в пределах своей компетенции, осуществляет техническое сопровождение информационных систем и инфраструктуры, находящихся в его зоне ответственности.

9. Начальник Отдела ИТ организует работу Отдела ИТ, распределяет задачи между работниками с учетом их должностных обязанностей и квалификации, контролирует исполнение, взаимодействует с ответственными работниками и специализированными организациями и информирует руководство о существенных рисках и недостаточности ресурсов.

10. Специалист (техник) по защите информации выполняет закрепленные за ним мероприятия по защите информации, участвует в ведении документации, контроле средств защиты, подготовке к аттестации, обработке инцидентов и внутреннем контроле.

11. Руководители структурных подразделений обеспечивают своевременное направление сведений о необходимости предоставления, изменения и прекращения доступа работников и контролируют соблюдение требований Положения в подразделении в пределах предоставленных полномочий.

12. Пользователь обязан соблюдать требования настоящего Положения, использовать информационные ресурсы в служебных целях, выполнять указания уполномоченных работников по безопасной эксплуатации и сообщать о выявленных нарушениях и инцидентах.

III. Учетные записи, идентификация и права доступа

13. Доступ к информационным системам и ресурсам предоставляется персонально в объеме, необходимом для выполнения должностных обязанностей или иных законных функций.

14. Создание, изменение, блокирование и удаление учетных записей осуществляются уполномоченными работниками на основании установленного в ГБПОУ КК «КМедК» основания: заявки, приказа, служебной записки, кадрового события или иного предусмотренного документа.

15. Руководители подразделений обязаны своевременно сообщать об изменении функций работника, переводе, длительном отсутствии, прекращении трудовых отношений либо иной необходимости изменить или прекратить доступ.

16. Использование общих учетных записей допускается только при наличии технологической необходимости и установленных мер, позволяющих определить круг допущенных лиц и обеспечить контролируемое использование.

17. Привилегированные учетные записи используются только уполномоченными работниками и исключительно для выполнения административных задач. Их использование подлежит повышенному контролю в предусмотренном локальными документами объеме.

18. Периодически проводится пересмотр предоставленных прав доступа. Избыточные и неактуальные права подлежат прекращению.

IV. Пароли и средства аутентификации

19. Пользователь обязан обеспечивать конфиденциальность паролей, кодов, ключей, токенов, сертификатов и иных средств аутентификации, предоставленных ему для работы.

20. Запрещается передавать собственные учетные данные другим лицам, использовать учетные данные другого пользователя либо хранить пароли в открытом виде в доступных посторонним местах.

21. Требования к длине, сложности, срокам действия и иным характеристикам паролей и средств аутентификации определяются внутренними стандартами, настройками соответствующих информационных систем и требованиями их операторов.

22. При подозрении на компрометацию средства аутентификации пользователь обязан немедленно прекратить его использование, если это возможно, и сообщить об этом установленным способом.

V. Использование оборудования

23. Компьютерное, серверное, сетевое и иное оборудование ГБПОУ КК «КМедК» используется в служебных и образовательных целях в соответствии с его назначением.

24. Самостоятельное изменение аппаратной конфигурации, подключение несанкционированного оборудования, вскрытие системных блоков и иных устройств пользователями не допускаются, кроме работников, которым соответствующие действия разрешены в рамках должностных обязанностей.

25. Служебные данные рекомендуется хранить на предоставленных ГБПОУ КК «КМедК» сетевых, серверных или иных ресурсах, для которых установлен порядок резервного копирования. Хранение единственного экземпляра значимых служебных данных только на локальном рабочем месте не допускается, если для таких данных предоставлено централизованное место хранения.

26. При передаче оборудования в ремонт, перемещении, списании или утилизации должны быть приняты меры по защите, содержащейся на нем информации в соответствии с установленным порядком.

VI. Программное обеспечение и изменения конфигурации

27. На оборудовании ГБПОУ КК «КМедК» допускается использование программного обеспечения, разрешенного к применению и установленного уполномоченными работниками либо иным способом, предусмотренным внутренними стандартами.

28. Пользователям запрещается самостоятельно устанавливать, удалять, отключать или изменять настройки системного программного обеспечения, средств защиты информации и иных компонентов, если такие полномочия им не предоставлены.

29. Изменения конфигураций серверов, сетевого оборудования, средств защиты и значимых информационных систем осуществляются уполномоченными работниками в пределах закрепленных полномочий и, когда это предусмотрено, регистрируются или согласовываются в установленном порядке.

30. Требование согласования конкретного технического изменения с директором применяется только в случаях, когда такое согласование прямо предусмотрено локальным актом, распорядительным документом, бюджетной процедурой либо характером изменения. Обычные эксплуатационные действия выполняются в пределах должностных полномочий.

VII. Сеть Интернет и сетевые ресурсы

31. Доступ к сети Интернет предоставляется для выполнения служебных и образовательных задач с учетом установленных ограничений и технических мер защиты.

32. Запрещается использовать сетевые ресурсы ГБПОУ КК «КМедК» для противоправной деятельности, обхода установленных ограничений, несанкционированного

сканирования и анализа защищенности, распространения вредоносного программного обеспечения либо действий, создающих угрозу функционированию информационных систем.

33. Подключение к внешним сетям и сервисам, использование туннелей, анонимизаторов, неразрешенных VPN и иных средств обхода сетевой политики допускается только при наличии служебной необходимости и разрешения в установленном порядке.

34. ГБПОУ КК «КМедК» вправе осуществлять технический мониторинг сетевых соединений, событий информационной безопасности и использования ресурсов в объеме, необходимом для защиты информации и обеспечения работоспособности систем, с соблюдением законодательства Российской Федерации.

VIII. Электронная почта, мессенджеры и обмен файлами

35. Для служебной переписки, передачи документов и обмена служебной информацией используются корпоративные или иные официально разрешенные ГБПОУ КК «КМедК» средства связи и сервисы.

36. Передача персональных данных и иной информации ограниченного доступа через личные почтовые ящики, личные облачные хранилища, неразрешенные мессенджеры и иные неутвержденные сервисы не допускается, если иное прямо не установлено уполномоченным лицом и применимыми требованиями.

37. Перед отправкой сообщения пользователь обязан проверить адресатов, состав вложений, необходимость передачи информации и наличие оснований для передачи информации ограниченного доступа.

38. Полученные из внешних источников вложения и ссылки должны обрабатываться с осторожностью. При наличии признаков фишинга, вредоносного содержимого или необычного поведения пользователь обязан прекратить взаимодействие и сообщить об этом установленным способом.

39. При прекращении использования сервиса или изменении корпоративных адресов структурные подразделения обеспечивают организационное уведомление контрагентов, а Отдел ИТ в пределах технических возможностей организует необходимые настройки, переадресацию или иные переходные меры.

IX. Съёмные носители и мобильные устройства

40. Использование внешних носителей информации осуществляется только при служебной необходимости и с соблюдением установленных требований по защите информации.

41. Перед использованием внешнего носителя на оборудовании ГБПОУ КК «КМедК» он должен быть проверен средствами защиты, если такая проверка предусмотрена техническими возможностями и настройками.

42. Запрещается копировать информацию ограниченного доступа на личные или неучтенные носители без предусмотренного основания и разрешения.

43. Подключение личных мобильных и иных устройств к информационным системам Колледжа допускается только в случаях и порядке, установленных отдельными правилами или разрешением уполномоченного лица.

Х. Удаленный доступ

44. Удаленный доступ к информационным системам и ресурсам ГБПОУ КК «КМедК» предоставляется при наличии служебной необходимости, установленного основания и технической возможности обеспечить требуемый уровень защиты.

45. Удаленное подключение осуществляется только с использованием разрешенных ГБПОУ КК «КМедК» средств и учетных записей. Самовольная установка средств удаленного управления и предоставление удаленного доступа третьим лицам запрещаются.

46. При удаленной работе пользователь обязан исключить доступ посторонних лиц к экрану, устройству, средствам аутентификации и обрабатываемой информации.

47. Доступ подрядных организаций предоставляется на ограниченный срок и в необходимом объеме, документируется и прекращается после завершения работ. При наличии технической возможности действия подрядчика контролируются или регистрируются.

XI. Антивирусная защита, обновления и уязвимости

48. На оборудовании, для которого это предусмотрено архитектурой и требованиями безопасности, применяются средства антивирусной и иной защиты, установленные и сопровождаемые уполномоченными работниками.

49. Пользователям запрещается отключать, блокировать, удалять или изменять настройки средств защиты информации, если соответствующие полномочия им не предоставлены.

50. Обновления программного обеспечения и средств защиты устанавливаются в порядке, определенном внутренними стандартами и техническими возможностями, с учетом необходимости проверки совместимости и непрерывности работы.

51. Выявленные уязвимости оцениваются и устраняются с учетом их критичности, применимости к фактической конфигурации и доступных способов устранения. Существенные риски, которые невозможно устранить оперативно, доводятся до руководства.

XII. Резервное копирование и восстановление

52. Резервное копирование организуется для информационных систем, серверных и сетевых файловых ресурсов и иных данных, для которых оно предусмотрено внутренними документами и фактически выполняется ГБПОУ КК «КМедК».

53. Отдел ИТ организует резервное копирование, хранение и восстановление тех ресурсов, резервное копирование которых отнесено к его компетенции и обеспечено соответствующими техническими средствами.

54. Периодичность, глубина хранения, места размещения резервных копий и порядок проверки восстановления определяются отдельным регламентом или настройками соответствующих систем с учетом значимости данных и имеющихся ресурсов.

55. Пользователи обязаны размещать значимые служебные документы в предусмотренных для этого местах хранения и не должны считать локальный диск рабочего компьютера гарантированно резервируемым ресурсом, если иное не установлено.

XIII. Физическая защита и обращение с носителями

56. Доступ в помещения, где размещено серверное, сетевое оборудование или иные критичные компоненты, предоставляется только лицам, которым он необходим для выполнения обязанностей.

57. Оборудование и носители информации должны быть защищены от утраты, хищения, несанкционированного доступа, повреждения и иных воздействий в разумно необходимом объеме.

58. Перед повторным использованием, передачей, списанием или утилизацией носителей выполняется удаление информации способом, соответствующим категории информации и установленным требованиям, либо физическое уничтожение носителя, если надежное удаление невозможно или требуется установленным порядком.

59. Факт передачи, ремонта, списания или уничтожения оборудования и носителей оформляется в случаях и порядке, предусмотренных учетными и организационно-распорядительными документами.

XIV. Инциденты информационной безопасности

60. К признакам инцидента относятся, в частности: несанкционированный доступ или попытка доступа; утрата или компрометация пароля, токена или ключа; обнаружение вредоносного программного обеспечения; необычные сообщения или запросы на ввод учетных данных; утечка или ошибочная отправка информации; утрата устройства или носителя; нештатное изменение данных; существенное нарушение работы средств защиты.

61. Работник ГБПОУ КК «КМедК» обязан незамедлительно сообщить о выявленном или предполагаемом инциденте в Отдел ИТ либо иным установленным каналом. При существенном инциденте информация доводится до начальника Отдела ИТ, специалиста по защите информации, ответственного должностного лица и директора в соответствии с установленным порядком.

62. Пользователь не должен самостоятельно удалять журналы, переустанавливать систему, продолжать работу с подозрительным объектом или предпринимать иные действия, способные уничтожить следы инцидента, если такие действия не предписаны инструкцией или уполномоченным работником.

63. Обработка инцидента включает регистрацию, первичную оценку, локализацию, устранение последствий, восстановление работоспособности, анализ причин и при необходимости подготовку корректирующих мероприятий.

XV. Доступ третьих лиц и подрядных организаций

64. Предоставление третьим лицам доступа к информационным системам, помещениям с критичными компонентами или информации ГБПОУ КК «КМедК» допускается только при наличии законного основания и в минимально необходимом объеме.

65. Условия доступа подрядных организаций, включая срок, состав ресурсов, правила обращения с информацией, требования по защите информации и порядок прекращения доступа, определяются договором, заявкой, техническим заданием, соглашением или иным документом.

66. Передача учетных данных работников Колледжа подрядчикам не допускается. Для подрядчика, когда это технически возможно и оправдано, создается отдельная учетная запись либо применяется иной контролируемый способ доступа.

67. После завершения работ временные права доступа подлежат прекращению, а выданные средства аутентификации – возврату, блокированию или иному предусмотренному действию.

XVI. Изменения, обслуживание и ремонт

68. Работы по обслуживанию и изменению информационных систем выполняются в пределах закрепленных полномочий и с учетом рисков для доступности, целостности и конфиденциальности информации.

69. Существенные изменения, способные повлиять на действительность ранее проведенной оценки соответствия, модель угроз, архитектуру защиты, состав средств защиты или границы информационной системы, подлежат предварительной оценке с точки зрения необходимости актуализации документации и дополнительных мероприятий.

70. При привлечении сервисной организации должна быть обеспечена защита информации, содержащейся на передаваемом оборудовании. При необходимости до передачи выполняется резервное копирование, удаление или иная защита данных.

71. Неисправности и изменения, которые невозможно безопасно устранить силами работников ГБПОУ КК «КМедК», передаются профильным специалистам или специализированным организациям.

XVII. Документация, обучение и ознакомление

72. В ГБПОУ КК «КМедК» ведутся организационно-распорядительные, учетные и технические документы по защите информации в объеме, необходимом с учетом применимых требований и фактически используемых информационных систем.

73. Работники знакомятся с требованиями настоящего Положения и иных обязательных для них документов в установленном порядке.

74. Для пользователей проводятся мероприятия по повышению осведомленности по вопросам безопасной работы, противодействия фишингу, обращения с персональными данными, использования средств аутентификации и сообщения об инцидентах.

75. Работники, выполняющие специальные функции по защите информации, проходят обучение в случаях и объеме, предусмотренных применимыми требованиями и решениями ГБПОУ КК «КМедК».

XVIII. Контроль и ответственность

76. Контроль соблюдения настоящего Положения осуществляется уполномоченными должностными лицами и работниками ГБПОУ КК «КМедК» в пределах закрепленных полномочий.

77. Технический контроль, осуществляемый Отделом ИТ и специалистом по защите информации, проводится в отношении систем и компонентов, находящихся в соответствующей зоне технического управления, и в пределах предоставленных полномочий.

78. Работники ГБПОУ КК «КМедК» несут ответственность за собственные действия и за надлежащее исполнение непосредственно возложенных на них обязанностей в порядке и пределах, установленных законодательством Российской Федерации.

79. Начальник Отдела ИТ несет ответственность за организацию работы Отдела ИТ, распределение задач, контроль их исполнения и своевременное информирование руководства о рисках и недостаточности ресурсов в пределах предоставленных полномочий. Это не подменяет ответственность работников, которым специальные функции закреплены непосредственно.

80. Нарушение требований настоящего Положения может являться основанием для применения мер ответственности в порядке, установленном законодательством Российской Федерации и локальными документами ГБПОУ КК «КМедК».

XIX. Заключительные положения

81. Настоящее Положение вступает в силу с даты его утверждения.

82. С даты вступления в силу настоящего Положения, Положение об информационной безопасности ГБПОУ КК «Камчатский медицинский колледж», утвержденное приказом № 255-П от 01.08.2023, признается утратившим силу.

84. Положение пересматривается при изменении обязательных требований, Политики защиты информации, организационной структуры, используемых информационных систем или при необходимости, выявленной по результатам контроля и инцидентов.

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