

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ заместителя начальника управления по информационной безопасности	СМК-ДИ
		страница 1 из 10

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ

«Кемеровский государственный медицинский университет»

Министерства здравоохранения Российской Федерации

(ФГБОУ ВО КемГМУ Минздрава России)

УТВЕРЖДАЮ

Ректор ФГБОУ ВО КемГМУ

Минздрава России

\_\_\_\_\_ С.Л.Кан

«\_\_» \_\_\_\_\_ 20 \_\_ г.

## ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

заместителя начальника  
управления по информационной безопасности

**СМК-ДИ-**

Кемерово 2026

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ заместителя начальника управления по информационной безопасности	СМК-ДИ
		страница 2 из 10

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая должностная инструкция разработана в соответствии с Трудовым кодексом Российской Федерации (далее – РФ) профессиональным стандартом «Специалист по защите информации в автоматизированных системах» и иными нормативно-правовыми актами, регулирующими трудовые отношения.

1.2. Заместитель начальника управления по информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Кемеровской государственной медицинской академии» Министерства здравоохранения Российской Федерации (далее – КемГМУ) относится к категории административно-управленческого персонала и подчиняется начальнику управления по информационной безопасности.

1.3. В своей деятельности заместитель начальника управления по информационной безопасности руководствуется:

1.3.1. Действующим законодательством Российской Федерации в рамках своего функционала;

1.3.2. Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

1.3.3. Конституцией РФ;

1.3.4. Трудовым кодексом РФ;

1.3.5. Соответствующими указами и распоряжениями Президента Российской Федерации;

1.3.6. Приказами и распоряжениями соответствующих министерств и ведомств РФ;

1.3.7. Распоряжениями и приказами ректора КемГМУ;

1.3.8. Уставом федерального государственного бюджетного образовательного учреждения высшего образования «Кемеровской государственной медицинской академии» Министерства здравоохранения Российской Федерации;

1.3.9. Коллективным договором;

1.3.10. Правилами внутреннего трудового распорядка КемГМУ;

1.3.11. Положением о структурном подразделении и иными локальными актами КемГМУ;

1.3.12. Настоящей должностной инструкцией;

1.3.13. Другими законодательными и нормативно-правовыми актами РФ.

Кроме вышеназванных, заместитель начальника управления по информационной безопасности руководствуется:

1.3.14. Федеральным законом РФ от 27.07.2006 № 152 «О персональных данных»;

1.3.15. Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.3.16. Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.3.17. Локальными нормативно-правовыми актами КемГМУ в области обработки и защиты персональных данных;

1.3.18. Приказом Федеральной службы по техническому и экспортному контролю России (далее - ФСТЭК) от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.3.19. Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

1.3.20. Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

1.3.21. Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ заместителя начальника управления по информационной безопасности	СМК-ДИ
		страница 3 из 10

утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

1.4. Заместитель начальника управления по информационной безопасности должен знать:

1.4.2. Законы и иные нормативные правовые акты Российской Федерации по вопросам обеспечения информационной безопасности и защиты персональных данных;

1.4.3. Нормативно-правовые акты в области обработки и защиты персональных данных;

1.4.4. Требования к работе на персональных компьютерах, иных электронно-цифровых устройствах;

1.4.5. Правила по охране труда и пожарной безопасности;

1.4.6. Основные (в том числе производственные, бизнес и управленческие) процессы КемГМУ и специфика обеспечения информационной безопасности КемГМУ;

1.4.7. Влияние информационных технологий на деятельность Университета, в том числе:

1.4.7.1. Роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования КемГМУ;

1.4.7.2. Зависимость основных процессов функционирования КемГМУ от информационных технологий;

1.4.8. Информационно-телекоммуникационные технологии, в том числе:

1.4.8.1. современные информационно-телекоммуникационные технологии, используемые в КемГМУ;

1.4.8.2. Способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее - системы и сети), в том числе ограниченного доступа;

1.4.8.3. Типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;

1.4.8.4. Принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей;

1.4.9. Обеспечение информационной безопасности, в том числе:

1.4.9.1. Цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;

1.4.9.2. Цели обеспечения информационной безопасности применительно к основным процессам функционирования КемГМУ, реализации и контроля их достижения;

1.4.9.3. Принципы и направления стратегического развития информационной безопасности КемГМУ;

1.4.9.4. Правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности КемГМУ, состав и содержание таких документов;

1.4.9.5. Порядок организации работ по обеспечению информационной безопасности КемГМУ;

1.4.9.6. Основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности КемГМУ для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности КемГМУ;

1.4.9.7. Основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз; возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;

1.4.9.8. Способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ заместителя начальника управления по информационной безопасности	СМК-ДИ
		страница 4 из 10

1.4.9.9. Порядок организации взаимодействия структурных подразделений КемГМУ при решении вопросов обеспечения информационной безопасности;

1.4.9.10. Антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;

1.4.9.11. Планирование деятельности по обеспечению информационной безопасности КемГМУ;

1.4.9.12. Формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности организации;

1.4.9.13. Организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности КемГМУ (далее - политика);

1.4.9.14. Внедрение политики;

1.4.9.15. Организация контроля и анализ применения политики;

1.4.9.16. Организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности КемГМУ;

1.4.9.17. Поддержка и совершенствование деятельности по обеспечению информационной безопасности КемГМУ;

1.4.9.18. Организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности КемГМУ;

1.4.9.19. Организация внедрения способов и средств для обеспечения информационной безопасности КемГМУ;

1.4.9.20. Организация мероприятий по анализу и контролю состояния информационной безопасности организации и модернизации (трансформации) процессов функционирования КемГМУ в целях обеспечения информационной безопасности КемГМУ;

1.4.9.21. Обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;

1.4.9.22. Организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы организации и реагированию на компьютерные инциденты;

1.4.9.23. Организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) КемГМУ.

1.5. Заместитель начальника управления по информационной безопасности назначается на должность и освобождается от должности приказом ректора КемГМУ в соответствии с действующим законодательством Российской Федерации.

## 2. КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ

2.1 Заместитель начальника управления информационной безопасности должен соответствовать следующим квалификационным требованиям: высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки (специальности), он должен пройти обучение по программе профессиональной переподготовки по направлению «Информационная безопасность».

## 3. ТРУДОВАЯ ФУНКЦИЯ

3.1. Трудовая функция заместителя начальника управления информационной безопасности:

3.1.1. Организация информационной безопасности;

3.1.2. Управления персональными данными.

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ заместителя начальника управления по информационной безопасности	СМК-ДИ
		страница 5 из 10

#### 4. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

##### 4.1. *В рамках процесса управления информационной безопасностью:*

- 4.1.1. Выполнять работы по обеспечению защиты информации в организации;
- 4.1.2. Разрабатывать предложения по размещению основных и вспомогательных технических средств, и систем с соблюдением установленных норм технической защиты информации;
- 4.1.3. Участвовать в обследовании объектов информатизации, их категорировании и аттестации;
- 4.1.4. Разрабатывать и готовить к утверждению проекты нормативных и методических документов, регламентирующих работу по обеспечению защиты информации, акты проверки, протоколы испытаний, предписания на право эксплуатации, а также положения, инструкции и другие организационно-распорядительные документы;
- 4.1.5. Участвовать в определении потребности в средствах технической защиты информации, составлять заявки на их приобретение с необходимыми обоснованиями и расчетами к ним, контролировать их поставку и использование;
- 4.1.6. Участвовать в приеме новых программных средств защиты информации;
- 4.1.7. Обеспечивать функционирование и поддержку работоспособности средств и систем защиты информации КемГМУ;
- 4.1.8. Обеспечивать настройку, администрирование защищенных каналов связи VIPNET, ведение сопутствующей документации;
- 4.1.9. Участвовать в аттестации объектов, относящихся к защищенным каналам связи, сторонними организациями;
- 4.1.10. Устанавливать, администрировать средства антивирусной защиты на автоматизированное рабочее место (далее – АРМ) пользователей и серверах;
- 4.1.11. Обеспечивает защиту каналов связи Университета от DDOS атак;
- 4.1.12. Мониторировать функционирование средств защиты информации;
- 4.1.13. Обеспечивать соблюдение требований по безопасности информации при эксплуатации технических средств, а также ремонт при выводе технических средств или их элементов из эксплуатации, в том числе передаче в ремонт;
- 4.1.14. Осуществлять контроль за процедурами резервного копирования и восстановления информационных систем и баз данных КемГМУ в части, касающейся обеспечения доступности и целостности информации;

##### 4.2 *В рамках процесса управления персональными данными:*

- 4.2.1 Установка, настройка и администрирование средств криптографической защиты информации на АРМ пользователей для доступа к сервисам федерального казначейства, ведение сопутствующих журналов и формуляров;
- 4.2.2 Оформление заявок учета и блокировок средства криптографической защиты информации в информационной системе автоматизации деятельности органов, криптографической защиты федерального казначейства;
- 4.2.3 Периодический контроль целостности печатей, пломб, наклеек на устройствах защищенных рабочих станций;
- 4.2.4 Проведение периодического инструктажа пользователей по правилам работы с используемыми средствами, системами защиты персональных данных;
- 4.2.5 Организация и контроль работы по обезличиванию персональных данных, используемых в целях статистики, тестирования или аналитики, без согласия субъектов;
- 4.2.6 Оперативное управление доступом пользователей (работников, обучающихся, сторонних лиц) к информационным системам, содержащим персональные данные (регистрация, наделение правами, блокировка при увольнении/отчислении);
- 4.2.7 Организация проведения регламентных работ по обновлению программного обеспечения и средств защиты информации в системах, обрабатывающих персональные данные, с целью устранения уязвимостей;

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ заместителя начальника управления по информационной безопасности	СМК-ДИ
		страница 6 из 10

4.2.8 Проверка выполнения требований по антивирусной защите и обновлению сигнатурных баз на всех рабочих станциях и серверах, где обрабатываются или хранятся персональные данные.

4.2.9 Организация, учет и контроль выдачи персональных данных третьим лицам (например, по запросам правоохранительных органов, судов, военкоматов), обеспечивая законность такой передачи и фиксацию в журналах.

## 5. ПРАВА

Заместитель начальника управления по информационной безопасности имеет право:

5.1. Давать указания и поручения работникам КемГМУ в части обеспечения информационной безопасности и защиты персональных данных;

5.2. Запрашивать у руководителей структурных подразделений и иных специалистов информацию и документы, необходимые для выполнения своих должностных обязанностей.

5.3. Требовать от руководства организационного и материально-технического обеспечения своей деятельности, а также оказания содействия в исполнении своих должностных обязанностей и прав;

5.4. Принимать решения по вопросам обеспечения информационной безопасности и защиты персональных данных;

5.5. Вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности и защиты персональных данных;

5.6. Инициировать проверки уровня (состояния) обеспечения информационной безопасности и защиты персональных данных;

5.7. Организовывать на объектах мероприятия по информационной безопасности, разработку и представление ректору предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий.

## 6. ОТВЕТСТВЕННОСТЬ

Заместитель начальника управления по информационной безопасности несет ответственность:

6.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, определенных трудовым законодательством Российской Федерации;

6.2. За невыполнение настоящей должностной инструкции;

6.3. За правонарушения, совершенные в процессе осуществления своей деятельности в пределах, определенных административным, уголовным и гражданским законодательством Российской Федерации;

6.4. За причинение материального ущерба в пределах, определенных трудовым и гражданским законодательством Российской Федерации;

6.5. За нарушение правил охраны труда и пожарной безопасности в порядке, установленном Трудовым кодексом РФ;

6.6. За выше перечисленные нарушения заместитель начальника управления по информационной безопасности может быть привлечен, в соответствии с действующим законодательством в зависимости от тяжести проступка к дисциплинарной, материальной, административной, гражданской и уголовной ответственности.



СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ заместителя начальника управления по информационной безопасности	СМК-ДИ
		страница 7 из 10

## 7. ВЗАИМООТНОШЕНИЯ

7.1 Заместитель начальника управления по информационной безопасности при необходимости взаимодействует со всеми структурными подразделениями КемГМУ и внешними организациями, и учреждениями по вопросам, входящим в его компетенции.

Должностная инструкция утверждается в 1-ом экземпляре и находится в управлении кадров, электронная версия документа представлена на сайте КемГМУ, что обеспечивает доступность документа в местах его применения.





СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ заместителя начальника управления по информационной безопасности	СМК-ДИ
		страница 9 из 10

## ИНФОРМАЦИОННЫЙ ЛИСТ

### 1. РАЗРАБОТАНА

Должность	ФИО	Подпись	Дата
Начальник управления по информационной безопасности	Цыгин Игорь Александрович		
Начальник управления информационных технологий	Клименко Илья Николаевич		

### 2. КОНСУЛЬТАНТЫ

Должность	ФИО	Подпись	Дата
Начальник управления кадров	Ганиева Лилия Бободжоновна		

### 3. СОГЛАСОВАНА

Должность	ФИО	Подпись	Дата
Ответственный за систему менеджмента качества КемГМУ, проректор по учебной работе	Большаков Василий Викторович		
Начальник управления лицензирования, аккредитации и менеджмента качества образования	Синькова Маргарита Николаевна		

**4. ВВЕДЕНА В ДЕЙСТВИЕ** со дня утверждения ректором «25» марта 2026 г., (Основание: протокол заседания Ученого совета № 9 от «25» марта 2026 г., протокол заседания Совета по качеству № 6 от «20» марта 2026 г.)

### 5. СПИСОК РАССЫЛКИ

#### Контрольный экземпляр:

- Управление кадров

#### Электронные копии:

- Управление стратегического планирования и мониторинга
- Управление по информационной безопасности

