

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ-
		страница 1 из 12

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

начальник
управления по информационной безопасности

СМК-ДИ-

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ страница 2 из 12
-----	-------------------------------------------------------------------------------	----------------------------

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. Начальник 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 непосредственно подчиняется ректору.

1.3. В своей деятельности начальник 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, начальник 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 утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ страница 3 из 12
-----	-------------------------------------------------------------------------------	----------------------------

соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.4. Начальник 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 специфику обеспечения информационной безопасности Университета;

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 формированием 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;

1.4.8.3 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 по 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;

1.4.9.8. Возможности и назначение типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;

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

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

1.4.9.11. Антикризисное управление и принятие управленческих решений при

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ
		страница 4 из 12

реагировании на кризисы и компьютерные инциденты;

1.4.9.12. Планирование деятельности по обеспечению информационной безопасности КемГМУ;

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

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

1.4.9.15. Внедрение политики;

1.4.9.16. Организация контроля и анализа применения политики;

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

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

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

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

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

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

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

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

1.5. Начальник 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. Начальник 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 Начальник управления по информационной безопасности:

3.1.1. Организация информационной безопасности;

3.1.2. Управления персональными данными.

4. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

4.1. *В рамках процесса организации информационной безопасности:*

4.1.1. Организует разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности КемГМУ и его процессов функционирования в случае

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ страница 5 из 12
-----	-------------------------------------------------------------------------------	----------------------------

проведения компьютерных атак, отвечает за согласование и утверждение политики КемГМУ, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

4.1.2. Организует и осуществляет разработку и внедрение нормативных и распорядительных документов в части вопросов касающихся информационной безопасности;

4.1.3. Изучает, анализирует и оценивает состояние информационной безопасности;

4.1.4. Изучает и обобщает научно-техническую литературу, нормативные и методические материалы по техническим средствам и способам защиты информации;

4.1.5. Формулирует требования по защите информации при создании и развитии объектов информатизации;

4.1.6. Предлагает рекомендации по внедрению средств защиты, их модернизации или замене;

4.1.7. Выявляет угрозы и уязвимости информационной безопасности, каналы утечки информации, оценивает риски и уровни сложности автоматизированных систем;

4.1.8. Осуществляет задачи и функции, возложенные утвержденными планами мероприятий, в части информационной безопасности;

4.1.9. Организует и проводит установку, модернизацию или замену средств защиты информации;

4.1.10. Организует и проводит первичную настройку средств защиты информации;

4.1.11. Организует и участвует в испытаниях и приемке автоматизированных систем в защищенном исполнении, предназначенных для обработки информации, составляющей служебную или коммерческую тайну, а также персональных данных;

4.1.12. Организует контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации;

4.1.13. Организует и разрабатывает (вносит изменения) технические паспорта автоматизированных систем и выделенных (защищаемых) помещений;

4.1.14. Организует контроль пользователей информационных ресурсов КемГМУ в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации;

4.1.15. Организует планирование мероприятий по обеспечению информационной безопасности;

4.1.16. Обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 Указа Президента Российской Федерации от 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

4.1.17. Поддерживает в актуальном состоянии техническую документацию для соблюдения требований федерального законодательства в части информационной безопасности и обработки персональных данных;

4.1.18. Поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые для обеспечения информационной безопасности;

4.1.19. Осуществляет регулярное и своевременное информирование руководства КемГМУ о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в органе (организации) и результатах практических учений по противодействию компьютерным атакам;

4.1.20. Проводит в структурных подразделениях КемГМУ плановые и внеплановые проверки состояния информационной безопасности;

4.1.21. При необходимости проводит занятия направленные на поддержание грамотности работников КемГМУ в области информационной безопасности.

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ страница 6 из 12
-----	-------------------------------------------------------------------------------	----------------------------

4.2. В рамках процесса управления персональными данными.

4.2.1. Организует и осуществляет разработку и внедрение нормативных и распорядительных документов в части касающейся управления персональными данными;

4.2.2. Проводит в структурных подразделениях КемГМУ плановые и внеплановые проверки соблюдения требований по защите персональных данных;

4.2.3. При необходимости проводит занятия направленные на поддержание грамотности работников КемГМУ в области обработки персональных данных;

4.2.4. Участвует в планировании деятельности КемГМУ по обработке, обсуждению, хранению, передаче информации, составляющей служебную или коммерческую тайну, а также персональных данных;

4.2.5. Осуществляет координацию действий структурных подразделений при локализации инцидентов, связанных с нарушением конфиденциальности, целостности или доступности персональных данных, а также руководит работами по ликвидации последствий таких инцидентов.

4.2.6. Организует проведение работ по классификации (категорированию) информационных систем персональных данных КемГМУ, а также по определению угроз безопасности персональным данным при их обработке.

4.2.7. Обеспечивает контроль за выполнением требований законодательства РФ, нормативных и методических документов ФСТЭК России, Федеральной службы безопасности (далее – ФСБ) России и Роскомнадзора в части обработки и защиты персональных данных;

4.2.8. Взаимодействует с государственными органами (Роскомнадзор, ФСТЭК, ФСБ, Министерство внутренних дел и др.) по вопросам, касающимся обработки, защиты и утечек персональных данных, включая подготовку ответов на запросы и участие в проверках;

4.2.9. Организует проведение анализа эффективности применяемых средств и методов защиты персональных данных, готовит предложения по их совершенствованию и внедрению новых технологий безопасности;

4.2.10. Согласовывает проекты договоров (контрактов), заключаемых КемГМУ, в части, касающейся передачи персональных данных третьим лицам (операторам, поручителям), а также условий их обработки и конфиденциальности;

4.2.11. Осуществляет методическое руководство и контроль за деятельностью структурных подразделений и должностных лиц, ответственных за обработку персональных данных на местах (в управлении кадров, бухгалтерии, деканатах);

4.2.12. Обеспечивает подготовку и своевременное представление сведений (уведомлений) в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) об обработке персональных данных, а также об изменениях в процессе обработки;

4.2.13. Участвует в работе комиссий по вводу в эксплуатацию информационных систем, предназначенных для обработки персональных данных, и по списанию носителей информации, содержащих персональные данные;

4.2.14. Организует ведение внутренней отчетности и документооборота по вопросам обработки и защиты персональных данных (журналы учета, акты классификации, частные модели угроз и т.д.);

4.2.15. Обеспечивает проведение оценки вреда (моделирования угроз), который может быть причинен субъектам персональных данных в случае нарушения требований безопасности, и участвует в определении уровня защищенности персональных данных при их обработке в информационных системах;

4.2.16. Организует внутренний аудит (контроль) соответствия обработки персональных данных требованиям Федерального закона № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, включая проверку наличия согласий субъектов на обработку их персональных данных;

4.2.17. Организует рассмотрение обращений и запросов субъектов персональных данных (сотрудников, обучающихся, третьих лиц) по вопросам обработки их персональных данных, обеспечивая подготовку мотивированных ответов и принятие мер по уточнению, блокированию или уничтожению персональных данных в установленных законом случаях.

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ страница 7 из 12
-----	-------------------------------------------------------------------------------	----------------------------

4.3. В рамках процесса оперативного управления.

- 4.3.1. Осуществляет руководство структурным подразделением, обеспечивающим информационную безопасность и управления персональными данными;
- 4.3.2. Осуществляет руководство и координацию деятельности по информационной безопасности и управлением персональными данными КемГМУ, руководит деятельностью подчиненного подразделения и осуществляет выполнение следующих обязанностей в рамках данной работы:
 - 4.3.2.1. Вносит предложения по формированию штатного расписания, принимает меры по обеспечению квалифицированными кадрами; обеспечивает организацию работы подчиненных, представляет кандидатов для назначения на должности работников управления;
 - 4.3.2.2. Разрабатывает должностные инструкции работников;
 - 4.3.2.3. Разрабатывает и обеспечивает исполнение планов работы и соблюдения положений управления;
 - 4.3.2.4. Вносит предложения по повышению квалификации работников управления;
 - 4.3.2.5. Обеспечивает выполнение работниками управления соблюдения трудовой и производственной дисциплины;
 - 4.3.2.6. Обеспечивает выполнение подчиненными должностных обязанностей по охране труда, соблюдение ими требований, норм, инструкций по охране труда;
- 4.3.3. Организует, координирует и осуществляет контроль за работой управления на всех объектах КемГМУ;
- 4.3.4. Осуществляет постановку целей и задач работникам подразделения в рамках организации процесса устройства рабочего пространства, материально-технического обеспечения деятельности работников КемГМУ;
- 4.3.5. Контролирует выполнение поставленных задач работниками подразделения в рамках организации процесса устройства рабочего пространства, материально-технического обеспечения деятельности работников КемГМУ;
- 4.3.6. Разрабатывает и внедряет нормы, регламентирующие материально-техническое обеспечение;
- 4.3.7. Обеспечивает выполнение предписаний, представлений и иных требований контролирующих органов, выданных КемГМУ;
- 4.3.8. Отчитывается в своей работе перед ректором;
- 4.3.9. Исполняет требования трудового законодательства, Устава КемГМУ, соблюдает Правила внутреннего трудового распорядка, Правила охраны труда, противопожарной и антитеррористической безопасности;
- 4.3.10. Выполняет разовые поручения ректора КемГМУ, не предусмотренные данной должностной инструкцией;
- 4.3.11. Выполняет требования СМК, согласно своим функциональным обязанностям;
- 4.3.12. Обеспечивает по запросу администрации представление требуемой в соответствии с законодательством РФ информации по направлению деятельности для дальнейшего размещения на официальном сайте КемГМУ и на мониторинговых сайтах Министерства науки и высшего образования РФ, других министерств и ведомств;
- 4.3.13. Обеспечивает своевременное составление и предоставление отчетной документации, в том числе ежегодной (статистической) отчетности;
- 4.3.14. По запросу администрации в установленные сроки предоставляет информацию и копии подтверждающих документов о пройденном повышении квалификации, профессиональной переподготовке, профессиональном обучении и повышении уровня профессионального мастерства;
- 4.3.15. Осуществляет работу на персональных компьютерах, с текстовыми редакторами, электронными таблицами, корпоративной электронной почтой и браузерами, мультимедийным оборудованием и иных электронно-цифровых устройствах, в том числе предназначенных для передачи информации, а также в электронной информационно-образовательной среде КемГМУ;
- 4.3.16. Соблюдает установленные требования по обработке и защите персональных данных;

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ страница 8 из 12
-----	-------------------------------------------------------------------------------	----------------------------

4.3.17. Соблюдает конфиденциальность сведений, связанных с профессиональной, служебной, коммерческой деятельностью, сведений о фактах, событиях и обстоятельствах частной жизни гражданина, сведений, составляющих тайну следствия и судопроизводства получаемых от руководителя или иным путем, разглашение которых может повлечь коммерческий ущерб или ущерб имиджу КемГМУ.

5. ПРАВА

Начальник управления по информационной безопасности имеет право:

5.1. Давать указания и поручения работникам КемГМУ в части обеспечения информационной безопасности и управления персональными данными;

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 управления персональными данными;

5.5. Вступать во взаимоотношения с учреждениями и организациями для решения вопросов, входящих в компетенцию начальника по информационной безопасности;

5.6. По доверенности ректора представлять интересы КемГМУ в государственных органах, сторонних учреждениях и организациях, судебных органах, в общественных организациях по вопросам, входящим в компетенцию начальника по информационной безопасности;

5.7. Согласовывать все виды приказов и распоряжений по личному составу подчиненных его управления, подписывать, визировать и согласовывать документы в пределах своей компетенции;

5.8. Вносить на рассмотрение ректора предложения по улучшению работы служб, отделов и подразделений КемГМУ;

5.9. Принимать участие в конференциях и совещаниях, на которых рассматриваются вопросы, связанные с его работой;

5.10. 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;

5.11. Инициировать проверки уровня (состояния) обеспечения информационной безопасности и обработки персональных данных;

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

5.13. Повышать свою квалификацию;

5.14. Начальник по информационной безопасности пользуется всеми трудовыми правами в соответствии с Трудовым кодексом Российской Федерации.

6. ОТВЕТСТВЕННОСТЬ

Начальник 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 нарушения требований по обеспечению информационной безопасности и защиты персональных данных;

6.3. За невыполнение настоящей должностной инструкции;

6.4. За правонарушения, совершенные в процессе осуществления своей деятельности - в

СМК	ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ начальник управления по информационной безопасности	СМК-ДИ
		страница 9 из 12

пределах, определенных административным, уголовным и гражданским законодательством РФ;

6.5. За причинение материального ущерба - в пределах, определенных трудовым и гражданским законодательством РФ;

6.6. Нарушение правил охраны труда и пожарной безопасности – в порядке, установленном Трудовым кодексом РФ;

6.7. За вышеперечисленные нарушения начальник управления информационной безопасности может быть привлечен, в соответствии с действующим законодательством в зависимости от тяжести проступка к дисциплинарной, материальной, административной, гражданской и уголовной ответственности.

7. ВЗАИМООТНОШЕНИЯ

7.1 Начальник управления по информационной безопасности при необходимости взаимодействует со всеми структурными подразделениями КемГМУ, 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 начальник управления по информационной безопасности	СМК-ДИ
		страница 11 из 12

ИНФОРМАЦИОННЫЙ ЛИСТ

1. РАЗРАБОТАНА

Должность	ФИО	Подпись	Дата
Ректор	Кан Сергей Людовикович		
Начальник управления по информационной безопасности	Цыгин Игорь Александрович		

2. КОНСУЛЬТАНТЫ

Должность	ФИО	Подпись	Дата
-			

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		
Начальник управления кадров	Ганиева Лилия Бободжоновна		

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

