



**федеральное государственное
бюджетное образовательное учреждение высшего образования
«Тюменский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО Тюменский ГМУ Минздрава России)**

ПРИНЯТО УЧЕНЫМ СОВЕТОМ

ФГБОУ ВО Тюменский ГМУ
Минздрава России
Протокол № 12 от 25.05.2023 г.

УТВЕРЖДЕНО

Ректором ФГБОУ ВО Тюменский
ГМУ Минздрава России
И.М. Петров

ПОЛОЖЕНИЕ

Об отделе информационной безопасности

г. Тюмень, 2023

1. Общие положения

1.1. Настоящее Положение определяет назначение, основные задачи, организационную структуру, функции, обязанности и права, ответственность, взаимодействие с подразделениями отдела информационной безопасности управления информационных технологий Дирекции информатизации и цифровой трансформации (далее - Отдел), который создан на основании решения Ученого совета федерального государственного бюджетного образовательного учреждения высшего образования «Тюменский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее - Тюменский ГМУ), утвержденного ректором Тюменского ГМУ.

1.2. Отдел является структурным подразделением Управления информационных технологий Дирекции информатизации и цифровой трансформации Тюменского ГМУ (далее - Управление).

1.3. Отдел в своей деятельности руководствуется Конституцией Российской Федерации, международными договорами Российской Федерации, федеральными конституционными законами, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, и иными нормативными правовыми актами, а также настоящим Положением.

1.4. Подразделение возглавляет начальник Отдела, назначаемый на должность и освобождаемый от занимаемой должности приказом ректора.

1.5. Квалификационные требования к начальнику Отдела: На должность начальника Отдела назначается лицо, имеющее высшее профессиональное образование и стаж работы в сфере информационных технологий не менее 5 лет.

1.6. В случае временного отсутствия начальника Отдела, в том числе болезни, отпуска, командировки, а также в случае прекращения трудовых отношений до замещения должности, его обязанности исполняет лицо, назначенное приказом Ректора в установленном законом порядке.

2. Организационная структура

2.1. Структура и штат Отдела формируется с учетом основных функциональных задач, специфики и объема, возлагаемых на него обязанностей и утверждается ректором Тюменского ГМУ.

2.2. Отдел возглавляет начальник отдела, назначаемый на должность и освобождаемый от занимаемой должности приказом ректора Тюменского ГМУ, по представлению начальника управления информационных технологий, директора Дирекции информатизации и цифровой трансформации. Другие категории работников Отдела назначаются на должность и освобождаются от занимаемой должности приказом ректора по представлению руководителя Отдела, в порядке, установленным действующим законодательством.

2.3. Квалификационные требования, функциональные обязанности, права, ответственность руководителя Отдела и других работников регламентируются трудовыми договорами и должностными инструкциями, утверждаемыми ректором.

3. Задачи

Основными задачами Отдела являются:

3.1. Организация и обеспечение защиты информации ограниченного доступа, включая персональные данные, не содержащей сведения, составляющие государственную тайну, от актуальных угроз безопасности информации при обработке указанной информации в информационных системах и программно-технических комплексах (далее - информационные системы).

3.2. Обеспечение технической защиты информации ограниченного доступа, содержащей сведения, составляющие государственную тайну, при её обработке средствами вычислительной

техники.

3.3. Реализация организационных и технических мер защиты информации, в том числе с применением средств криптографической защиты информации, не содержащей сведения, составляющие государственную тайну, а также информации ограниченного доступа, содержащей сведений, составляющих государственную тайну.

3.4. Организация периодического аудита состояния защиты информации ограниченного доступа, а также планирование и проведение мероприятий по устранению выявленных угроз безопасности информации.

3.5. Исполнение функций регионального органа криптографической защиты Университета.

4. Функции

В соответствии с основными задачами Отдел по защите информации осуществляет следующие функции:

4.1. Планирование и организация работ по защите информационных систем Университета, а также регулярное проведение аудита эффективности реализованных мер по обеспечению безопасности информации.

4.2. Осуществление эксплуатации подсистем и средств защиты информации, обрабатываемой в информационных системах, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации).

4.3. Проведение периодического контроля и анализа состояния защиты информации, а также внесение по результатам проведенного анализа предложений по совершенствованию состава мер и средств защиты информации руководству.

4.4. Взаимодействие с региональными подразделениями федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации и иными организациями по вопросам, отнесенным к компетенции подразделения по защите информации.

4.5. Осуществление текущего контроля выполнения требований нормативных и организационно-методических документов по информационной безопасности, включая, в том числе: контроль за организацией резервного копирования информационных ресурсов, администрирование реестров информационных ресурсов, периодическую актуализацию списков администраторов информационных ресурсов (системных, баз данных, приложений, безопасности), а также списков работников, допущенных к обработке информации ограниченного доступа.

4.6. Анализ и подготовка отчетов в Министерства, контролирующие органы.

4.7. Администрирование средств защиты информации включая их получение, выдачу, установку, настройку, ввод в действие, деинсталляцию и уничтожение.

4.8. Ведение поэкземплярного учета средств защиты информации и документации.

4.9. Организация учета машинных носителей информации, проведение ежегодного переучета машинных носителей информации, а также контроль использования съемных машинных носителей информации.

4.10. Осуществление контроля за уничтожением (стиранием) информации на машинных носителях информации при их передаче или списании.

4.11. Организация и контроль работы комиссии по уничтожению списанных машинных носителей информации.

4.12. Разработка и своевременная актуализация организационных документов по обеспечению защиты информации, предусмотренных нормативными актами регуляторов и организационно-распорядительных документов Университета.

4.13. Проведение инвентаризации, а также разработка и совершенствование организационно-распорядительных документов Университета по вопросам обеспечения информационной безопасности и представление предложений в Департамент по обеспечению информационной безопасности по разработке и совершенствованию организационно-распорядительных документов в области обеспечения информационной безопасности.

4.14. Участие в проведении расследований случаев нарушений порядка и правил эксплуатации информационных систем и/или средств защиты информации, разработке предложений по устранению предпосылок таких нарушений по результатам расследований.

4.15. Участие в работе комиссий по проверке подразделений по вопросам организации и обеспечения защиты информации.

4.16. Методическое обеспечение, координация и контроль деятельности работников Университета по вопросам обеспечения защиты информации, включая их обучение порядку обращения с информацией ограниченного доступа и средствами ее защиты.

4.17. Участие в аттестации работников подразделений в части проверки их знаний порядка обращения с информацией ограниченного доступа и средствами ее защиты.

4.18. Подготовка предложений по обучению специалистов подразделения по защите информации на курсах повышения квалификации и прохождения переподготовки по направлениям информационной безопасности.

4.19. Осуществление деятельности органа криптографической защиты включая эксплуатацию средств криптографической защиты информации, обеспечение безопасности их применения в соответствии с правилами пользования, требованиями эксплуатационной и технической документации.

4.20. Ведение поэкземплярного учета средств криптографической защиты информации и документации.

4.21. Осуществление мероприятий, необходимых для получения (переоформления) в установленном порядке лицензии на выполнение работ и оказание услуг, относящихся к лицензируемым видам деятельности, в отношении выполнения стоящих перед подразделением по защите информации задач.

4.22. Организация и осуществление выпуска и выдачи ключей электронных подписей, сертификатов ключей проверки электронных подписей, в том числе копий сертификатов ключей проверки электронных подписей на бумажном носителе, и/или их получение в ином удостоверяющем центре для работников Университета.

4.23. Управление сертификатами ключей проверки электронных подписей.

4.24. Обеспечение применения средств электронной подписи в информационных системах, ведение поэкземплярного учета средств электронной подписи.

4.25. Организация и обеспечение работ по аттестации объектов информатизации, выделенных или защищаемых помещений по требованиям безопасности информации, проведению специсследований и спецпроверок технических средств и систем.

4.26. Ведение в подразделении по защите информации самостоятельного конфиденциального делопроизводства, в том числе организация и осуществление получения, учета, хранения, выдачи/приема и уничтожения конфиденциальных документов по тематике подразделения по защите информации.

4.27. Организация системы разграничения доступа к информационным ресурсам Университета.

4.28. Согласование технических заданий на проектирование систем охранно-пожарной сигнализации, контроля и управления доступом, видеонаблюдения в зданиях Университета, проведение оценки целесообразности предлагаемых технических решений при проектировании, а также участие в приеме этих систем в эксплуатацию.

4.29. Организация закупки средств защиты информации, а также услуг по обеспечению защиты информации, в соответствии с утвержденным бюджетом.

4.30. Осуществляет иные функции, предусмотренные распоряжениями и приказами руководства Университета.

5. Обязанности начальника Отдела

Начальник Отдела обязан:

5.1. Осуществляет руководство Отделом и организацию его деятельности, обеспечивает выполнение стоящих перед ним задач и возложенных на него функций.

5.2. Распределяет обязанности между работниками Отдела.

- 5.3. Утверждает должностные инструкции работников Отдела.
- 5.4. Вносит предложения о структуре, численности и штатном расписании Отдела.
- 5.5. Организует и обеспечивает исполнение поручений ректора. Осуществляет контроль и принимает оперативные меры по соблюдению Отделом установленных сроков исполнения поручений.
- 5.6. Докладывает начальнику управления информационных технологий по вопросам, входящим в компетенцию Отдела.
- 5.7. Вносит управления информационных технологий предложения для включения в планы основных мероприятий по вопросам, относящимся к компетенции Отдела.
- 5.8. Представляет на утверждение управления информационных технологий планы работ Отдела и отчеты об их исполнении.
- 5.9. Обеспечивает выполнение утвержденного плана работ Отдела.
- 5.10. Принимает участие в заседаниях, а также в совещаниях, проводимых ректором, при обсуждении вопросов, относящихся к деятельности Отдела.
- 5.11. Подписывает документы, направляемые от имени Отдела в структурные подразделения, органы и организации, по вопросам, входящим в компетенцию Отдела.
- 5.12. Организует работу Отдела на основе и во исполнение нормативных правовых актов Российской Федерации и дает указания, обязательные для исполнения всеми работниками Отдела, проверяет их исполнение.
- 5.13. Обеспечивает и в пределах своих полномочий контролирует соблюдение работниками Отдела трудового законодательства Российской Федерации.
- 5.14. В установленном порядке представляет кандидатуры работников для назначения на должности, предложения о поощрении работников Отдела, в том числе о награждении государственными наградами, а также ходатайствует о применении к работникам Отдела мер социальной защиты, о наложении взысканий на работников Отдела, в том числе об увольнении работников Отдела.
- 5.15. Представляет кандидатуры работников Отдела для включения их в состав соответствующих рабочих групп, комиссий, а также для направления в служебные командировки.
- 5.16. Осуществляет иные полномочия в соответствии с нормативными правовыми актами Университета, поручениями ректора.
- 5.18. Во время отсутствия начальника Отдела его обязанности назначаются в установленном порядке.

6. Права

Права подразделения реализуются начальником Отдела и его работниками в соответствии с установленным в должностных инструкциях распределением обязанностей.

- 6.1. Начальник Отдела имеет право:
- 6.1. Вносить, в пределах своей компетенции, на рассмотрение предложения по вопросам обеспечения информационной безопасности Университета.
- 6.2. Получать доступ к информации, а также документам, имеющимся в других структурных подразделениях в пределах компетенции Отдела.
- 6.3. Выносить на рассмотрение предложения по совершенствованию работы, перспективам развития, обеспечению роста профессиональной подготовки специалистов Отдела.
- 6.4. Требовать от работников Университета точного выполнения нормативных актов, руководящих документов по обеспечению защиты информации.
- 6.5. Привлекать, по согласованию с руководителями структурных подразделений Университета, отдельных специалистов к подготовке проектов документов по обеспечению информационной безопасности.

7. Ответственность

7.1. Начальник Отдела несет персональную ответственность за своевременное и качественное выполнение возложенных на Отдел задач и требований, определенных правовыми актами Российской Федерации, указаниями и поручениями Президента Российской Федерации, Правительства Российской Федерации, Минтруда России, Министерства здравоохранения, Министерства образования.

7.2. Начальник Отдела несет ответственность за несоблюдение обязанностей, запретов и ограничений, установленных Федеральным законом от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» и принятыми в соответствии с ним нормативными правовыми актами Российской Федерации, нормативными правовыми актами Университета.

7.3. Степень ответственности других работников Отдела устанавливается должностными инструкциями.

8. Взаимодействие со структурными подразделениями

8.1. Отдел осуществляет свою деятельность во взаимодействии с другими службами и структурными подразделениями Тюменского ГМУ, а также в пределах своей компетенции со сторонними органами, учреждениями и организациями, по вопросам, входящим в компетенцию Отдела.

9. Заключительные положения

9.1. Настоящее Положение принимается ученым советом Тюменского ГМУ утверждается ректором.

9.2. В настоящее Положение могут вноситься изменения и дополнения, процедура принятия, утверждения и введения в действие, которых аналогична процедуре, предусмотренной пунктом 8.1. настоящего Положения.

9.3. Настоящее Положение прекращает своё действие с момента его отмены, либо с момента введения в действие нового Положения.