ПРИНЯТО

Ученым Советом
ФГБОУ ВО Тверской ГМУ
Минздрава России

(Протокол № 9 от 17.10.2023)

УТВЕРЖДЕНО

Ректор ФГБОУ ВО Тверской ГМУ
Минздрава России
_____ Л.В. Чичановская
«27» ____11_____2023 г
Приказ ФГБОУ ВО ГМУ Минздрава
России от № 1089 от 23.11. 2023

ПОЛОЖЕНИЕ
ОБ ОТДЕЛЕ ПО ЗАЩИТЕ ИНФОРМАЦИИ
ФГБОУ ВО Тверской ГМУ Минздрава России

г. Тверь
2023

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Отдел по защите информации (далее – ОЗИ) является структурным подразделением Управления комплексной безопасности ФГБОУ ВО Тверской ГМУ Минздрава России (далее - Университет). ОЗИ находится в прямом подчинении начальника управления комплексной безопасности (далее – УКБ).

1.2 ОЗИ создаётся, реорганизуется и ликвидируется приказами ректора Университета.

1.3 В своей деятельности ОЗИ руководствуется действующим законодательством, регулирующим деятельность Университета в сфере информационной безопасности, Уставом и правилами внутреннего трудового распорядка Университета, приказами и распоряжениями ректора Университета, а также настоящим Положением.

2. РУКОВОДСТВО И СТРУКТУРА ОЗИ

2.1 ОЗИ возглавляет начальник, назначаемый на должность и освобождаемый от занимаемой должности приказом ректора Университета.

2.2 Начальник ОЗИ осуществляет непосредственное руководство деятельностью сотрудников отдела.

2.3 Структура и штатное расписание ОЗИ определяются в установленном порядке, в соответствии с объемами работ, решаемыми задачами и функциями, исполняемыми отделом.

3. ОСНОВНЫЕ ЗАДАЧИ ОЗИ

3.1 Разработка единой политики обеспечения информационной безопасности Университета.

3.2 Разработка, создание и сопровождение системы управления информационной безопасностью Университета (кроме защиты информации, содержащей сведения, составляющие государственную тайну), реализующей политику информационной безопасности Университета.

3.3 Организация мероприятий и координация работ всех подразделений Университета, по комплексной защите информации (кроме защиты информации, содержащей сведения, составляющие государственную тайну) на всех этапах технологических циклов ее создания, переноса на носитель (бумажный или электронный), обработки, хранения, передачи и уничтожения в соответствии с политикой обеспечения информационной безопасности.

3.4 Контроль и оценка эффективности принятых мер и применяемых средств защиты информации, совершенствование системы управления информационной безопасностью Университета.

4. ФУНКЦИИ

4.1 Мониторинг законодательства в области информационной безопасности.

4.2 Разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Университете.

4.3 Организация и контроль:

- обработки персональных данных в информационных системах персональных данных (далее – ИСПДн) и без применения средств автоматизации;
- учета, применения и хранения средства криптографической защиты информации (далее – СКЗИ) и криптографических ключей (электронных цифровых подписей (далее - ЭЦП);
- в вопросах формирования и поддержания в актуальном состоянии нормативной и методической документации, используемой при выполнении задач, возложенных на ОЗИ;
- обеспечения безопасности критической информационной инфраструктуры Университета;
- обращения с информацией, содержащей сведения конфиденциального характера, доступ к которой ограничен в соответствии с законодательством Российской Федерации;
- подготовка отчетной документации, ответов по запросам министерств и ведомств о состоянии работ по обеспечению информационной безопасности в Университете.

4.4 Выполнение следующих работ:

- оценка информационных потоков, информационных систем и объектов информатизации на соответствие требованиям информационной безопасности;
- анализ угроз информационной безопасности;
- разработка плана мероприятий по обеспечению информационной безопасности;
- разработка системы нормативных и распорядительных документов в области обеспечения информационной безопасности;
- реализация организационных мер, контроль применения и эксплуатации средств защиты информации;
- подготовка предложений к совершенствованию системы управления информационной безопасностью Университета;
- консультация пользователей в области информационной безопасности;

- формирование у работников и обучающихся Университета ответственного отношения к обеспечению информационной безопасности;
- информационная поддержка руководства и работников Университета в части изменений законодательства и нормативной базы в области защиты информации.

4.5 Участие в разработке основополагающих документов Университета с целью закрепления в них требований обеспечения информационной безопасности.

4.6 Организация учета, хранения и использования СКЗИ и криптографических ключей (ЭЦП), а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

4.7 Выполнение иных функций, исходя из поставленных целей и задач в рамках обеспечения информационной безопасности в Университете.

Возложение на отдел функций, не относящихся к компетенции отдела, не допускается.

5. ПРАВА И ОБЯЗАННОСТИ

5.1 Для решения задач, возложенных на ОЗИ, его сотрудники имеют следующие права:

- запрашивать и получать в установленном порядке доступ к работам и документам, необходимым для принятия решений по всем вопросам, отнесенным к компетенции подразделения;
- участвовать в испытаниях, разработанных и внедряемых информационных систем по вопросам оценки качества реализации требований по обеспечению информационной безопасности;
- проводить проверки структурных подразделений Университета в части, касающейся функций отдела;
- контролировать деятельность работников Университета в области обеспечения информационной безопасности.

5.2 Сотрудники ОЗИ обязаны:

- определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения информационной безопасности, включая документы, регламентирующие деятельность работников других подразделений Университета;
- обеспечивать необходимый уровень информационной безопасности Университета в соответствии с поставленными задачами;
- исполнять функции, указанные в законодательстве по вверенному направлению, настоящем Положении и иных локальных актах Университета;

- участвовать в расследовании событий, связанных с нарушением информационной безопасности Университета;
- координировать действия всех подразделений Университета в области обеспечения информационной безопасности;
- выполнять иные обязанности, предусмотренные должностной инструкцией и трудовым договором.

6. ОТВЕТСТВЕННОСТЬ

6.1 Ответственность за надлежащее и своевременное выполнение отделом информационной безопасности функций, предусмотренных настоящим Положением и организацию защиты информации в Университете, в том числе за предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты несет начальник отдела.

6.2 Сотрудники ОЗИ несут ответственность за выполнение возложенных на них обязанностей в соответствии с должностными инструкциями.

6.3 Сотрудники ОЗИ несут ответственность за нарушение норм, регулирующих получение, обработку и защиту служебной информации (персональных данных) и могут быть привлечены к дисциплинарной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.

7. ВЗАИМООТНОШЕНИЯ С ДРУГИМИ ПОДРАЗДЕЛЕНИЯМИ

7.1 Сотрудники ОЗИ получают информацию, необходимую для своевременного и качественного выполнения своих должностных обязанностей, а также реализации предоставленных им прав, от руководителей и работников управлений и служб университета в сроки, установленные регламентом работ ОЗИ.

7.2 Сотрудники ОЗИ в рамках, предоставленных им компетенций, предоставляют информацию, необходимую для своевременного и качественного выполнения другими работниками Университета своих должностных обязанностей, а также реализации предоставленных им прав, в сроки, установленные регламентом работ ОЗИ.

8. КРИТЕРИИ ОЦЕНКИ ДЕЯТЕЛЬНОСТИ ОТДЕЛА

8.1. Эффективность и результативность деятельности подразделения определяются по итогам выполнения поставленных целей и задач по обеспечения информационной безопасности.

8.2. Качественное выполнение функциональных обязанностей.

Разработал:

Начальника отдела по защите информации — Семенов С.В.

Согласовано:

Проректор по реализации национальных проектов и развитию регионального здравоохранения — А. В. Соловьева

Начальник управления комплексной безопасности — К. Ф. Горецкий

Заместитель начальника управления кадров — Е.Е. Лучникова

Начальник управления правового и документационного обеспечения — А.А. Кожуховский

С положением и должностными обязанностями ознакомлен(а), принял(а) к руководству и исполнению:

№ п/п	Ф.И.О.	Подпись	Дата