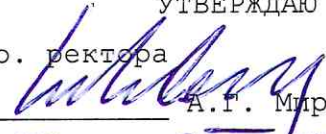


МИНЗДРАВ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего
образования «Южно-Уральский
государственный медицинский университет»
Министерства здравоохранения
Российской Федерации
(ФГБОУ ВО ЮУГМУ Минздрава России)

УТВЕРЖДАЮ
И.о. ректора

А.Г. Мирошниченко
07 сентября 2023 г.

№ 47

ПОЛОЖЕНИЕ
Об отделе информационной безопасности

І. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Отдел информационной безопасности является структурным подразделением федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – университет).

1.2. Отдел информационной безопасности является самостоятельным структурным подразделением.

1.3. Создание, ликвидация и реорганизация отдела информационной безопасности осуществляется приказом ректора университета.

1.4. Руководство отделом информационной безопасности осуществляет начальник отдела, назначаемый и освобождаемый от должности приказом ректора университета. Начальник отдела информационной безопасности непосредственно подчиняется проректору по стратегическому развитию, науке и инновациям.

1.5. В своей деятельности отдел информационной безопасности руководствуется законодательством Российской Федерации, в том числе федеральным законом от 27.06.2006 №152-ФЗ «О персональных данных», федеральным законом от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи», Трудовым кодексом РФ, Уставом федерального государственного бюджетного образовательного учреждения высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации, Коллективным договором, приказами и распоряжениями ректора университета, распоряжениями проректоров университета, решениями ученого совета университета, требованиями системы менеджмента качества, распространяющимися на деятельность отдела информационной безопасности, правилами эксплуатации вычислительной техники, правилами по соблюдению производственной санитарии, правилами по охране труда, настоящим положением и другими локальными нормативными актами университета.

1.6. Отдел информационной безопасности печати не имеет.

1.7. В области действия системы менеджмента качества университета отдел участвует в процессе «Управление инфраструктурой в части связи и информационных систем».

II. СТРУКТУРА ПОДРАЗДЕЛЕНИЯ

2.1. Структура отдела информационной безопасности определяется штатным расписанием, которое утверждается ректором университета.

III. ЦЕЛИ И ЗАДАЧИ

3.1. Целями деятельности отдела информационной безопасности являются:

- исключение или существенное снижение негативных последствий (ущерба) в отношении университета вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;
- обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;
- повышение защищенности университета от возможного нанесения ей материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем университета или несанкционированного доступа к циркулирующей в них информации и её несанкционированного использования;
- обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры университета;
- обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры университета.

3.2. Основными задачами деятельности отдела информационной безопасности являются:

- планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в университете;
- выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств;
- предотвращение утечки информации по техническим каналам, не санкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;
- поддержание стабильной деятельности университета и производственных процессов в случае проведения компьютерных атак;
- взаимодействие с Национальным координационным центром по компьютерным инцидентам;
- обеспечение нормативно-правового обеспечения использования информационных ресурсов.

IV. ФУНКЦИИ

4.1. Отдел информационной безопасности выполняет следующие функции:

- разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в университете;
- разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в университете и представление их руководству;
- выявление и проведение анализа угроз безопасности информации в отношении университета, уязвимостей информационных систем, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;
- обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения невозможности реализации негативных последствий, разработки и реализации организационных мер и применения средств обеспечения информационной безопасности;

- обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;
- представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах;
- исполнение указаний, данных Федеральной службой безопасности Российской Федерации и её территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих организации либо используемых организацией, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет";
- проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов организации в целях обеспечения информационной безопасности в университете;
- подготовка отчетов о состоянии работ по обеспечению информационной безопасности в университете;
- организация развития навыков безопасного поведения в университете, в том числе проведение занятий с работниками по вопросам обеспечения информационной безопасности;
- контроль безопасного поведения работников университета по вопросам обеспечения информационной безопасности.
- выполнение иных функций, исходя из поставленных руководством университета целей и задач в рамках обеспечения информационной безопасности в университете.

V. ПРАВА И ПОЛНОМОЧИЯ

Работники отдела информационной безопасности обладают следующими правами и полномочиями:

- принимать в пределах своей компетенции меры по обеспечению выполнения, возложенных на них задач;
- вносить предложения по улучшению деятельности университета;
- осуществлять взаимодействие с руководителями всех структурных подразделений университета по вопросам, относящимся к компетенции отдела информационной безопасности;
- запрашивать информацию от структурных подразделений университета для осуществления функций, возложенных на отдел информационной безопасности;
- давать разъяснения, рекомендации и указания по вопросам, входящим в компетенцию отдела информационной безопасности;
- доводить до сведения руководства информацию о выявленных случаях нарушения информационной безопасности.

VI. ВЗАИМОТНОШЕНИЯ. СВЯЗИ

Работники отдела информационной безопасности взаимодействуют со всеми структурными подразделениями и должностными лицами университета.

VII. ОТВЕТСТВЕННОСТЬ

Работники отдела информационной безопасности несут ответственность в случае:

- ненадлежащего исполнения или неисполнения своих обязанностей в пределах, определенных действующим трудовым законодательством Российской Федерации, уставом университета, а также правилами внутреннего трудового распорядка университета и должностными инструкциями;
- причинения материального ущерба в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации;

- правонарушений, совершенных в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

Начальник отдела
информационной безопасности



Е.В. Зосим

СОГЛАСОВАНО

Проректор стратегическому развитию,
науке и инновациям



А.Н. Наркевич

Ведущий юрисконсульт

Е.В. Маркова

Рассмотрено на заседании ученого совета 29.08 2023 (протокол № 1)
Введено впервые