федеральное государственное бюджетное образовательное учреждение высшего образования
«Приволжский исследовательский медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО «ПИМУ» Минздрава России)

ПРИКАЗ

04 сентября 2023 г. № 487/осн

Нижний Новгород

Об утверждении Положения
«Об отделе информационной безопасности
ФГБОУ ВО «ПИМУ» Минздрава России»

В целях приведения локальных нормативных актов ФГБОУ ВО «ПИМУ» Минздрава России (далее – университет) в соответствии с законодательством,

п р и к а з ы в а ю:

1. Утвердить прилагаемое Положение «Об отделе информационной безопасности ФГБОУ ВО «ПИМУ» Минздрава России».

Ректор Н.Н. Карякин

федеральное государственное бюджетное образовательное учреждение высшего образования
«Приволжский исследовательский медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО «ПИМУ» Минздрава России)

УТВЕРЖДЕНО
Приказом ФГБОУ ВО «ПИМУ»
Минздрава России
от «__» декабря 2023 г. № 487/осн

ПОЛОЖЕНИЕ
Об отделе информационной безопасности ФГБОУ ВО «ПИМУ» Минздрава России

г. Нижний Новгород
2023

1. Общие положения

1.1. Отдел информационной безопасности (далее по тексту – Отдел) является структурным подразделением федерального государственного бюджетного образовательного учреждения высшего образования «Приволжский исследовательский медицинский университет» Министерства здравоохранения Российской Федерации (ФГБОУ ВО «ПИМУ» Минздрава России) (далее – Университет).

1.2. Отдел в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, уставом Университета, настоящим Положением, локальными нормативными актами Университета.

1.3. Отдел непосредственно подчиняется ректору и проректору по безопасности.

2. Цели, задачи и функции отдела информационной безопасности

2.1. Деятельность отдела информационной безопасности направлена:

- на 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;
- на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;
- на повышение защищенности Университета от возможного нанесения ему 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 ее несанкционированного использования;
- на обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры Университета;
- на обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры Университета.

2.2. Задачи отдела информационной безопасности:

- 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, несанкционированного 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 его процессов в случае проведения компьютерных атак;

- взаимодействие с Национальным координационным центром по компьютерным инцидентам (НКЦКИ);
- совершенствование нормативно-правовой базы обеспечения информационной безопасности Университета;
- организация материального учета, хранения материальных ценностей в части средств защиты информации (в т.ч. средств криптографической защиты информации);
- организация работ по технической защите информации, содержащей сведения, составляющие государственную тайну;
- участие в цифровой трансформации Университета.

2.3. Функции отдела информационной безопасности:

- разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в Университете;
- разработка и поддержание в актуальном состоянии регламентирующих и организационно-распорядительных документов по обеспечению информационной безопасности в Университете;
- контроль выполнения структурными подразделениями Университета и их работниками требований регламентирующих и организационно-распорядительных документов в части информационной безопасности;
- 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;
- при взаимодействии с центром информационных технологий обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;
- представление в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) информации о выявленных компьютерных инцидентах;
- исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих Университету либо используемых Университетом, 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 Университета 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 руководящим составом и специалистами Университета по вопросам обеспечения информационной безопасности;
- организация и проведение специальных мероприятий по противодействию иностранным техническим разведкам и технической защите информации;
- разработка совместно с работниками специальной части Университета и службой безопасности комплекса мероприятий по защите информации, содержащей сведения,

составляющие государственную тайну, при установлении и осуществлении научно-технических и торгово-экономических связей с зарубежными фирмами, а также при посещении Университета иностранными представителями;

- обеспечения участников электронного взаимодействия сертификатами ключей электронных подписей;
- организация выполнения требований по информационной безопасности при подключении пользователей к государственным информационным системам и системам финансового документооборота;
- выполнение иных функций, исходя из поставленных руководством Университета целей и задач в рамках обеспечения информационной безопасности в Университете.

3. Организационная структура отдела информационной безопасности

3.1. Руководство деятельностью отдела информационной безопасности осуществляет начальник отдела.

3.2. В состав отдела входят:

- специалисты по информационной безопасности;
- специалисты технической поддержки пользователей.

3.3. Состав и штатную численность отдела утверждает ректор Университета.

4. Права и обязанности отдела информационной безопасности

4.1. Отдел имеет право:

- разрабатывать и вносить предложения по совершенствованию мер по обеспечению информационной безопасности;
- запрашивать у руководителей структурных подразделений Университета, образовательных организаций-партнеров, регулирующих и надзорных федеральных органов информацию и документы, необходимые для осуществления своей деятельности;
- контролировать деятельность любого структурного подразделения Университета по выполнению требований к обеспечению информационной безопасности;
- готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности;
- постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности;
- участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;
- участвовать в работе комиссий Университета при рассмотрении вопросов обеспечения информационной безопасности;
- вносить предложения руководству Университета о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;
- вносить на рассмотрение руководству Университета предложения по вопросам деятельности подразделения.

4.2. Отдел обязан:

- содействовать работе ректора, ректората, проректоров Университета по реализации мер по обеспечению информационной безопасности;
- эффективно использовать, развивать и качественно улучшать систему мер по обеспечению информационной безопасности Университета, в т.ч. на основе регулярного повышения квалификации сотрудников отдела;
- использовать современные эффективные информационные, научно-исследовательские, технические и управленческие технологии при осуществлении своих функций;
- поддерживать положительный имидж кафедр, факультетов и других структурных подразделений Университета.

5. Взаимоотношения и связи отдела информационной безопасности

5.1. Отдел осуществляет свои полномочия во взаимодействии со структурными подразделениями Университета, а также в пределах своей компетенции с иными органами (организациями) и гражданами в установленном порядке.

5.2. По указанию ректора осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством здравоохранения Российской Федерации по вопросам информационной безопасности.

6. Ответственность

6.1. Всю полноту ответственности за деятельность, своевременное выполнение возложенных на отдел задач и функций несет начальник отдела информационной безопасности.

6.2. Сотрудники отдела несут персональную ответственность за:

- невыполнение своих должностных обязанностей, предусмотренных должностной инструкцией и действующими нормативными актами;
- необеспечение требований по обеспечению информационной безопасности, установленных законодательством Российской Федерации;
- несоблюдение конфиденциальности персональных данных сотрудников Университета и обучающихся.

7. Заключительные положения

7.1. В настоящее Положение могут вносится изменения и дополнения в соответствии с действующим законодательством Российской Федерации.

Проректор по безопасности _____ В.А. Грачев

Начальник управления кадрами _____ Ю.И. Китаева

Начальник юридического управления _____ А.В. Качко