УТВЕРЖДЕНО

приказом ФГБОУ ВО СтГМУ
Минздрава России
от 27.02.2023 № 119-ОД

ПРИНЯТО

решением ученого совета
от 22.02.2023, протокол № 7

ПОЛОЖЕНИЕ
об отделе организации и технологии защиты информации центра обеспечения технической поддержки и информационной безопасности

I. Общие положения

1.1. Настоящее Положение об отделе организации и технологии защиты информации центра обеспечения технической поддержки и информационной безопасности (далее – Положение) определяет цели, задачи и функции отдела организации и технологии защиты информации центра обеспечения технической поддержки и информационной безопасности (далее – Отдел), обеспечивающего информационную безопасность федерального государственного бюджетного образовательного учреждения высшего образования «Ставропольский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее - университет).

1.2. Отдел является структурным подразделением центра обеспечения технической поддержки и информационной безопасности университета (далее – центр), которое создается, реорганизуется и ликвидируется на основании решения ученого совета университета приказом ректора.

1.3. 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, локальными нормативными актами университета и настоящим положением.

II. Цели и задачи деятельности отдела

2.1. Деятельность отдела направлена:

на исключение или существенное снижение негативных последствий (ущерба) в отношении уенивеситета вследствие нарушения функционирования информационных систем и информационно-телекоммуникационных сетей в результате реализации угроз безопасности информации;

на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

на повышение защищенности органа университета от возможного нанесения 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. Основными задачами деятельности отдела являются:

планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в университете;

контроль соблюдения требований законодательства Российской Федераций в сфере обеспечения информационной безопасности;

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 производственных процессов в случае проведения компьютерных атак;

взаимодействие с Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ);

обеспечение нормативно-правового обеспечения использования информационных ресурсов, в части информационной безопасности.

III. Функции отдела

3.1. Отдел 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 ректору;

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 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;

выполнение иных функций, исходя из поставленных ректором целей и задач в рамках обеспечения информационной безопасности в университете;

обеспечение своевременного предоставления соответствующей информации и документов для формирования закупок, необходимых для осуществления деятельности Отдела.

IV. Права отдела

4.1. С целью реализации функций Отдел имеет право:

запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений университета, необходимым для принятия решений по всем вопросам, отнесенным к компетенции Отдела;

готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности;

контролировать деятельность любого структурного подразделения университета по выполнению требований к обеспечению информационной безопасности;

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 ректору университета о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

вносить представления ректору университета в отношении работников университета при обнаружении фактов нарушения работниками установленных требований безопасности информации в университете, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности;

вносить на рассмотрение руководству органа (организации) предложения по вопросам деятельности подразделения;

иметь необходимое техническое оснащение рабочих мест и необходимое оборудование для осуществления своей деятельности, а также пользоваться информационными ресурсами, транспортными средствами университета для осуществления функций, возложенных на Отдел.

V. Организационная структура отдела

5.1. Отдел подчиняется непосредственно проректору по информатизации и стратегическому развитию и руководителю центра обеспечения технической поддержки и информационной безопасности.

5.2. Руководство Отделом осуществляет начальник, назначаемый на должность приказом ректора университета по представлению руководителя центра обеспечения технической поддержки и информационной безопасности и согласованию с проректором по информатизации и стратегическому развитию.

5.3. Другие работники Отдела назначаются на должность приказом ректора по представлению начальника Отдела и согласованию с проректором по информатизации и стратегическому развитию и руководителем центра обеспечения технической поддержки и информационной безопасности.

5.4. Структура, численность и штатное расписание отдела, изменения к нему утверждаются ректором университета в установленном порядке, исходя из объёма решаемых задач.

VI. ВЗАИМООТНОШЕНИЯ И СВЯЗИ ОТДЕЛА

6.1. Взаимодействие Отдела со структурными подразделениями ениверситета, в том числе с филиалами, по вопросам, входящим в компетенцию Отдела, осуществляется, исходя из производственной необходимости.

6.2. По указанию ректора ениверситета Отдел осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации по вопросам информационной безопасности.

VII. Обязанности отдела

7.1. Работники Отдела обязаны:

качественно и в полном объеме выполнять возложенные на них должностные обязанности;

исполнять решения ученого совета университета, поручения руководства университета и проректора по информатизации и стратегическому развитию;

давать разъяснения по направлениям деятельности Отдела;

нести ответственность за выполнение возложенных на них обязанностей в соответствии с должностными инструкциями, утверждаемыми ректором университета.

_____