УТВЕРЖДЕНО

приказом ФГБОУ ВО СтГМУ
Минздрава России
от 30.12.2022 № 1043-ОД

ПРИНЯТО

решением ученого совета
от 21.12.2022, протокол № 5

ПОЛОЖЕНИЕ
о центре обеспечения технической поддержки и информационной безопасности

I. Общие положения

1.1. Настоящее Положение о центре обеспечения технической поддержки и информационной безопасности (далее – Положение) определяет цели, задачи и функции центра обеспечения технической поддержки и информационной безопасности (далее – Центр), обеспечивающего вопросы информатизации и технического обеспечения, техническую поддержку информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Ставропольский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее - университет).

1.2. Центр является структурным подразделением университета, которое создается, реорганизуется и ликвидируется на основании решения ученого совета университета и приказа ректора.

1.3. Центр 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 информатизации, технического обеспечения, информационной безопасности и требований к ней, другими нормативными правовыми документами, локальными нормативными актами университета и настоящим положением.

II. Цели и задачи деятельности центра

2.1. Деятельность центра направлена на:

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

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

повышение защищенности органов управления 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;

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;

обеспечение структурных подразделений университета необходимыми средствами вычислительной и организационной техники в целях осуществления уставной деятельности университета;

совершенствование материально-технической базы университета;

развитие сетевой телекоммуникационной инфраструктуры университета, системы телеконференций;

совершенствование системы технической поддержки и эксплуатации средств информатизации;

на изучение, внедрение, сопровождение новых информационных технологий;

развитие направлений деятельности, входящих в компетенцию центра;

формирование предложений по совершенствованию ЛВС университета;

участие в обучении работников университета и проведение консультаций, относящихся к компетенции центра.

2.2. По поручению вышестоящего руководства центр может заниматься решением иных задач, для реализации которых необходимо применение знаний, навыков и опыта работников центра.

2.3. Основными задачами деятельности центра 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;

поддержка локально-вычислительной сети университета (далее - ЛВС) в работоспособном состоянии;

обеспечение технико-эксплуатационного обслуживания средств вычислительной и организационной техники;

внедрение и сопровождение программного обеспечения;

модернизация и замена программного обеспечения;

администрирование корпоративной сети университета, структурированных кабельных сетей, телефонных сетей;

организация работ по диагностике, техническому обслуживанию, ремонту компьютерной техники;

участие в оказании помощи в настройке и сопровождении средств автоматизации применяемых продуктов другими подразделениями университета;

участие в организации и проведении образовательного процесса в рамках компетенции центра;

поддержка структурных подразделений университета при реализации проектов по направлениям деятельности.

III. Функции центра

3.1. Центр 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 центра;

анализ потребностей структурных подразделений университета в дополнительных средствах вычислительной техники и обработки информации;

подготовка отчетной документации по расходам в части деятельности центра;

совместно с руководителями структурных подразделений определение задач в целях автоматизации рабочего процесса;

обеспечение работоспособности и бесперебойного функционирования аппаратной и программной составляющей серверного, коммутационного, телекоммуникационного (в том числе АТС), сетевого периферийного оборудования, кабельной системы ЛВС университета;

организация работ по оказанию услуг в сфере информатизации и связи, выполняемых сторонними организациями;

подготовка, оценка проектной и сметной документации, контроль и прием выполненных работ и оказанных услуг;

изучение, внедрение, формирование предложений по применению новых информационных технологий;

участие в определении потребностей по подготовке и переподготовке кадров в соответствии с планами внедрения и развития автоматизированной информационной

системы;

организация компьютерного, информационного и иного необходимого обеспечения совещаний, видеоконференций, селекторов и иных мероприятий, проводимых университетом;

разработка и внедрение порядков, инструкций, регламентов и стандартов использования программного и аппаратного обеспечения;

разработка (совместно с соответствующими структурными подразделениями) мероприятий по совершенствованию форм и методов работы с информационными ресурсами;

содействие в проведении (совместно с другими структурными подразделениями) мероприятий по обеспечению и совершенствованию форм и методов дистанционного обучения; разграничение доступа пользователей к сетевым информационным ресурсам, базам данных, периферийному оборудованию в соответствии с установленным регламентом.

ведение учета существующих лицензий на программное обеспечение пользователей;

подготовка проектов документов по вопросам, входящим в компетенцию отделов центра, ответы на письма и запросы государственных органов, предприятий, учреждений, организаций и граждан;

осуществление учета и хранения контрольных версий дистрибутивов и документации на используемые прикладные информационные системы;

подготовка информационных и иных материалов по вопросам, относящимся к компетенции университета и центра;

взаимодействие и обеспечение в пределах своей компетенции защиты сведений, относящихся к персональным данным, и иных сведений ограниченного распространения;

взаимодействие с сервисными центрами и поставщиками по вопросам гарантийного и послегарантийного обслуживания вычислительной и оргтехники, мультимедийного и интерактивного оборудования;

обеспечение информационного и телекоммуникационного взаимодействия с образовательными, научными учреждениями, предприятиями и организациями Российской Федерации и ведущими зарубежными научно-исследовательскими центрами;

осуществление иных функций по поручению вышестоящего руководства.

IV. Права центра

4.1. С целью реализации функций Центр 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 Центра;

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 Центр.

V. Организационная структура центра

5.1. Центр подчиняется непосредственно проректору по информатизации и стратегическому развитию, Ректору университета.

5.2. Руководство Центром осуществляет руководитель, назначаемый на должность приказом ректора университета по согласованию с проректором по информатизации и стратегическому развитию.

5.3. Другие работники Центра 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 центра, изменения к нему утверждаются ректором университета в установленном порядке, исходя из объема решаемых задач.

5.5. Руководитель Центра в пределах своей компетенции:

5.5.1. Руководит деятельностью Отделов, входящих в состав Центра, и несет персональную ответственность за качество и своевременность выполнения возложенных на Центр задач и функций, правильность и объективность принимаемых решений, соблюдение исполнительской и служебной дисциплины, правил пожарной безопасности и охраны труда работниками.

5.5.2. Обеспечивает качественное выполнение в установленные сроки поручений руководства университета.

5.5.3. Разрабатывает Положение о Центре, положения об отделах и функциональные обязанности для работников подчиненных подразделений.

5.5.4. Представляет проректору по информатизации и стратегическому развитию университета предложения о назначении на должность и освобождения от должности работников подчиненных подразделений, о применении к ним мер поощрения и наложения на них дисциплинарных взысканий, а также о выплате им материальной помощи.

5.5.5. Вносит проректору по информатизации и стратегическому развитию университета предложения о совершенствовании материально-технического и кадрового обеспечения Центра.

5.6. Деятельность по направлениям Центра осуществляют работники Отдела организации технологии и зашиты информации и Отдела информатизации и технического обеспечения, назначаемые и освобождаемые от должности приказом ректора университета.

VI. Взаимоотношения и связи центра

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

6.2. По указанию ректора университета, проректора по информатизации и стратегическому развитию Центр 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 и основной деятельности центра.

VII. Обязанности центра

7.1. Работники центра 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 центра и входящих в него Отделов;

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