Федеральное государственное бюджетное образовательное учреждение
высшего образования «Воронежский государственный
медицинский университет имени Н.Н. Бурденко»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО ВГМУ им. Н.Н. Бурденко Минздрава России)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 29DA63E73B264EA326A68D5EC1676813
Владелец: Есауленко Игорь Эдуардович
Действителен: с 18.07.2024 до 11.10.2025

УТВЕРЖДЕНО
приказом ректора
ФГБОУ ВО ВГМУ
им. Н.Н. Бурденко
Минздрава России
«27» февраля 2023 года № 141

ПОЛОЖЕНИЕ О ЦЕНТРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ ИМ. Н.Н.БУРДЕНКО» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ.

Воронеж, 2023

1. РАЗРАБОТАНО

Центром информационной безопасности и инженерно-технических средств защиты

полное наименование структурного подразделения, ответственного за разработку документа

2. ПРИНЯТО НА ЗАСЕДАНИЯ УЧЁНОГО СОВЕТА ФГБОУ ВО ВГМУ им. Н.Н. Бурденко Минздрава России

16.02.2023 г., протокол № 6.

3. ВЕРСИЯ I.

Один экземпляр принят на хранение:

Должность _____ Л.А. Гришина

1. Общие положения

1.1 Центр информационной безопасности и инженерно-технических средств защиты (далее – Центр) является структурным подразделением ФГБОУ ВО ВГМУ им. Н.Н. Бурденко Минздрава России (далее – Университет).

1.2 В своей деятельности Центр 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, постановлениями, приказами, инструктивными письмами Минздрава России, Уставом Университета, коллективным договором, приказами и распоряжениями ректора Университета, решениями Ученого Совета, правилами внутреннего трудового распорядка и настоящим Положением.

1.3 Центр в своей деятельности подчиняется проректору по цифровой трансформации и возглавляется начальником центра.

1.4 Контроль за деятельностью Центра осуществляет ректор.

1.5 Центр осуществляет свою деятельность во взаимодействии с другими структурными подразделениями Университета, а также в пределах своей компетенции со сторонними организациями. По указанию руководства 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, Министерством здравоохранения РФ, Министерством науки и высшего образования РФ по вопросам информационной безопасности

1.6 Настоящее Положение утверждается приказом ректора.

2. Структура

2.1 Начальник и другие работники Центра назначаются на должности и освобождаются от занимаемых должностей приказом ректора в соответствии с действующим трудовым законодательством Российской Федерации.

2.2 Квалификационные требования, функциональные обязанности, права, ответственность начальника и других работников Центра регламентируются должностными инструкциями, утверждаемыми ректором.

2.3 Изменения и дополнения в структуру Центра, штатное расписание и настоящее Положение вносятся ректором Университета в установленном порядке.

3. Основные задачи

3.1 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;

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

3.3 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;

3.4 Обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры Университета;

3.5 Обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры Университета;

3.6 Планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в Университете;

3.7 Выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств;

3.8 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;

3.9 Поддержание стабильной деятельности Университета и его производственных процессов в случае проведения компьютерных атак;

3.10 Взаимодействие с Национальным координационным центром по компьютерным инцидентам;

3.11 Обеспечение нормативно-правового обеспечения использования информационных ресурсов;

3.12 Обеспечение безопасности значимых объектов критической информационной инфраструктуры Университета;

3.13 Обеспечение работоспособности систем видеонаблюдения и системы контроля и управления доступом на территории Университета.

4. Основные функции

4.1 Разработка, координация, управление и контроль за реализацией плана (стратегии) работ по обеспечению информационной безопасности в Университете;

4.2 Разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Университете и представление их ректору Университета;

4.3 Выявление и проведение анализа угроз безопасности информации в Университете, уязвимостей информационных систем, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;

4.4 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;

4.5 Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

4.6 Представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах;

4.7 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";

4.8 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;

4.9 Подготовка отчетов о состоянии работ по обеспечению информационной безопасности в Университете;

4.10 Организация развития навыков безопасного поведения в Университете, в том числе проведение занятий с руководящим составом и специалистами Университета по вопросам обеспечения информационной безопасности;

4.11 Выполнение иных функций, исходя из поставленных руководством Университета целей и задач в рамках обеспечения информационной безопасности в Университете;

4.12 Составление заявок на приобретение товаров, работ, услуг для выполнения задач и функций Центра;

4.13 Обеспечение безопасности значимых объектов критической информационной инфраструктуры Университета и разработка необходимой документации.

4.14 Разработка, координация, управление и контроль за реализацией плана (стратегии) работ по обеспечению работоспособности систем видеонаблюдения и системы контроля и управления доступом на территории Университета.

5. Права

5.1 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;

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

5.3 Контролировать деятельность любого структурного подразделения Университета по выполнению требований к обеспечению информационной безопасности;

5.4 Постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности;

5.5 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;

5.6 Участвовать в работе комиссий Университета при рассмотрении вопросов обеспечения информационной безопасности и вопросов обеспечения видео фиксации, контроля и управления доступом;

5.7 Вносить предложения руководству Университета о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

5.8 Вносить представления руководству Университета в отношении сотрудников Университета при обнаружении фактов нарушения сотрудниками установленных требований безопасности информации в Университете, в том числе ходатайствовать о привлечении указанных сотрудников к административной или уголовной ответственности;

5.9 Вносить на рассмотрение руководству Университета предложения по вопросам деятельности подразделения;

5.10 Согласовывать договоры на закупку товаров, работ, услуг, направленных на выполнение задач и функций Центра;

5.11 Участвовать в подготовке проектов документов, связанных с деятельностью Центра.

5.12 Осуществлять иные права в соответствии с законодательными и нормативными актами.

6. Взаимоотношения с другими подразделениями Университета

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

6.2 По указанию руководства Университета 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, Министерством здравоохранения РФ, Министерством науки и высшего образования РФ по вопросам информационной безопасности.

6.3 Взаимодействие Центра со структурными подразделениями Университета регулируется соответствующими Регламентами.

7. Ответственность

7.1 За ненадлежащее и несвоевременное выполнение Центром функций, предусмотренных настоящим Положением ответственность несет начальник Центра.

7.2 Ответственность сотрудников Центра устанавливается их должностными инструкциями.

8. Заключительные положения

8.1. Положение вступает в силу с момента утверждения приказом ректора.

8.2. Проект Положения с листом согласования хранится в ученом совете, утвержденный экземпляр Положения - в управлении кадров, на официальном сайте в сети Интернет - в виде электронного документа, подписанного электронной подписью в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».