ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИНЯТО
Решением Ученого совета университета
от 25.04.2018, протокол № 9

УТВЕРЖДАЮ
Ректор
_____В.И. Кошель

Приказ от 27.04.2018 № 490-ОД

ПОЛОЖЕНИЕ ОБ УПОЛНОМОЧЕННОМ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОБЕСПЕЧЕНИЮ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об уполномоченном по информационной безопасности и обеспечению защиты конфиденциальной информации федерального государственного бюджетного образовательного учреждения высшего образования «Ставропольский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее соответственно – Положение, ФГБОУ ВО СтГМУ Минздрава России, университет) определяет основные обязанности, права и ответственность должностного лица, отвечающего за безопасность информации, обрабатываемой в университете.

1.2. Уполномоченный по информационной безопасности и обеспечению защиты конфиденциальной информации (далее – Уполномоченный по ИБ и ОЗКИ) назначается и освобождается от выполнения обязанностей, предусмотренных настоящим Положением, на основании приказа ректора из числа работников ФГБОУ ВО СтГМУ Минздрава России.

1.3. Уполномоченный по ИБ и ОЗКИ подчиняется непосредственно ректору ФГБОУ ВО СтГМУ Минздрава России.

1.4. Уполномоченный по ИБ и ОЗКИ является лицом, ответственным за проведение работ по технической защите информации и поддержанию достигнутого уровня защиты автоматизированных систем и их ресурсов на этапах эксплуатации и модернизации в целях обеспечения режима конфиденциальности при обработке защищаемой информации с использованием средств автоматизации.

1.5. Уполномоченный по ИБ и ОЗКИ определяет политику оператора (ФГБОУ ВО СтГМУ Минздрава России) в отношении обработки конфиденциальной информации, в том числе содержащей персональные данные.

1.6. На Уполномоченного по ИБ и ОЗКИ возлагаются следующие задачи:

– контроль организации эксплуатации и поддержание работоспособности средств защиты информации (далее – СЗИ);

– контроль действий работников ФГБОУ ВО СтГМУ Минздрава России, являющихся пользователями автоматизированных рабочих мест (далее – АРМ) из состава автоматизированных систем и участвующих в рамках выполнения своих должностных обязанностей в процессах автоматизированной обработки информации конфиденциального

характера (далее – Пользователи) в части выполнения ими установленных мер по защите информации;

– защита автоматизированных систем ФГБОУ ВО СтГМУ Минздрава России от несанкционированного доступа (далее – НСД) к защищаемой информации, в том числе выявление и регистрация попыток НСД к защищаемым информационным ресурсам и техническим средствам автоматизированных систем;

– разработка единой политики (концепции) обеспечения информационной безопасности университета, определение требований к системе защиты информации университета и документообороту на бумажных и электронных носителях;

– организация мероприятий и координация работ всех подразделений университета по комплексной защите информации на всех этапах технологических циклов ее создания, переноса на носитель (бумажный или электронный), обработки и передачи в соответствии с единой политикой обеспечения информационной безопасности университета;

– исполнение контрольно-надзорных функций по вопросам соблюдения правил безопасной эксплуатации автоматизированных систем университета;

– контроль за соблюдением требований технических условий и сертификатов на приобретенные программных и аппаратных средств (в том числе средства защиты информации);

– организация и контроль за разрешительной системой допуска исполнителей к работе с защищаемой информацией;

– определение порядка учета, хранения и обращения с защищаемой информацией (документами и носителями информации);

– контроль сохранности конфиденциальных документов и носителей информации;

– разработка единой политики университета по вопросам обработки конфиденциальной информации, в том числе содержащей персональные данные граждан Российской Федерации;

– определение порядка допуска должностных лиц университета к обработке конфиденциальной и иной охраняемой законом информации;

– разработка нормативных документов в части, касающиеся вопросов обеспечения информационной безопасности, включая документы, регламентирующие деятельность сотрудников подразделений Университета;

– сбор информации от сотрудников подразделений университета по вопросам применения технологий обработки информации и эксплуатации автоматизированных систем;

– организацию текущего контроля соблюдения сотрудниками университета требований Планов защиты автоматизированных систем и других организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– исполнение контрольно-надзорных функций за выполнением специальных требований по размещению технических средств автоматизированных систем, прокладке кабельных трасс и инженерных систем, за организацией резервного дублирования и архивирования информации, а также созданием и использованием эталонных копий программного обеспечения в части обеспечения безопасности информации и процессов ее обработки;

– определение и пересмотр порядка установки и модернизации аппаратных и программных средств автоматизированных систем университета в части обеспечения безопасности информации и процессов ее обработки;

– исполнение контрольной надзорных функций по вопросам обработки конфиденциальной информации на материальных носителях, с использованием и без использования средств вычислительной техники;

– принятие решений об установлении грифа конфиденциальности на материальных носителях конфиденциальной информации.

1.7. Уполномоченный по ИБ и ОЗКИ в своей работе руководствуется Конституцией Российской Федерации, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями Правительства Российской Федерации, решениями и нормативными правовыми актами Федеральной службы по техническому и экспортному контролю Российской Федерации, иными нормативными правовыми актами Российской Федерации по вопросам обеспечения информационной безопасности и защиты информации, локальными нормативными актами ФГБОУ ВО СтГМУ Минздрава России, настоящим Положением.

1.8. Уполномоченный по ИБ и ОЗКИ осуществляет общее и методическое руководство в вопросах обеспечения безопасности информации конфиденциального характера, обрабатываемой как с использованием, так и без использования средств автоматизации.

1.9. Во всех случаях, не урегулированных настоящим Положением или другими нормативными документами ФГБОУ ВО СтГМУ Минздрава России, необходимо руководствоваться действующим законодательством Российской Федерации.

1.10. Настоящее Положение вступает в силу с момента его утверждения и действует до замены его новым Положением.

1.11. Все изменения в Положение вносятся приказом ректора ФГБОУ ВО СтГМУ Минздрава России на основании решения Ученого совета.

1.12. Настоящее Положение и изменения к нему являются обязательными для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

II. ОБЯЗАННОСТИ УПОЛНОМОЧЕННОГО ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Уполномоченный по ИБ обязан:

2.1. знать и выполнять требования действующих нормативных и руководящих документов Российской Федерации, локальных нормативных документов ФГБОУ ВО СтГМУ Минздрава России, регламентирующих порядок действий по обеспечению информационной безопасности;

2.2. знать перечень технических средств, входящих в состав автоматизированных систем, перечень используемого программного обеспечения, перечень задач, решаемых с использованием таких технических средств и программного обеспечения, структуру и топологию локальной вычислительной сети (далее – ЛВС) ФГБОУ ВО СтГМУ Минздрава России;

2.3. контролировать соответствие документально утвержденного состава аппаратной и программной части автоматизированных систем реальной конфигурации, принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию автоматизированных систем;

2.4. контролировать соответствие состава и расположения основных и вспомогательных технических средств и систем техническому паспорту объекта информатизации и не допускать их изменения, не допускать внесение несанкционированных изменений в системы электроснабжения, заземления и других коммуникаций;

2.5. проводить работу по выявлению возможных каналов утечки защищаемой информации и НСД к ней, каналов вмешательства в процесс функционирования технических средств автоматизированных систем и готовить предложения по устранению таких каналов;

2.6. осуществлять установку, настройку, обеспечивать функционирование и поддерживать работоспособность СЗИ, вести документацию на СЗИ в соответствии с требованиями нормативных документов;

2.7. обеспечивать сохранность эталонных вариантов общесистемного, прикладного и специального программного обеспечения автоматизированных систем, выполнять

резервное копирование программного обеспечения, настроек и параметров СЗИ и восстановление таких данных в случае отказа средств и систем защиты информации;

2.8. вести учет состава пользователей и их прав доступа к защищаемым информационным ресурсам автоматизированных систем (согласовывать матрицы доступа);

2.9. производить необходимые настройки и сопровождать в процессе эксплуатации, установленные на АРМ пользователей СЗИ от НСД:

– в целях обеспечения усиленной идентификации и аутентификации пользователей выдавать им персональные идентификаторы;

– в соответствии с матрицами доступа автоматизированных систем устанавливать и актуализировать в базе данных СЗИ от НСД права доступа пользователей к защищаемым информационным ресурсам (файлам, каталогам), устройствам, программным средствам обработки и защиты информации;

– своевременно удалять учетные записи пользователей и установленные им права доступа из базы данных СЗИ от НСД при изменении списка пользователей;

– формировать для каждого Пользователя перечень программного обеспечения, разрешенного для запуска на АРМ;

– разграничивать доступ пользователей к принтерам и осуществлять контроль за соблюдением установленных правил и параметров регистрации и маркирования распечатываемых документов;

– вводить в базу данных СЗИ от НСД описания событий, подлежащих регистрации в системном журнале и журнале СЗИ от НСД;

– периодически проводить анализ системных журналов и журналов СЗИ от НСД для выявления попыток НСД к защищаемым информационным ресурсам;

– настраивать подсистему контроля целостности обрабатываемой информации конфиденциального характера, программных средств автоматизированных систем и системы защиты и определять варианты реагирования на возникающие ситуации нарушения целостности;

– централизовано управлять установленными на АРМ пользователей СЗИ от НСД;

– проводить оперативный мониторинг и аудит безопасности ФГБОУ ВО СтГМУ Минздрава России, своевременно реагировать на события НСД;

2.10. контролировать регулярность смены аутентификационной информации для Пользователей в соответствии с установленной периодичностью, пресекать действия пользователей, которые могут привести к компрометации паролей и персональных идентификаторов;

2.11. осуществлять контроль за соблюдением установленного порядка и своевременностью обновления программного обеспечения элементов автоматизированных систем и системы защиты информации конфиденциального характера по мере появления таких обновлений;

2.12. осуществлять контроль за соблюдением установленного порядка антивирусной защиты информации, организацией и обеспечением эксплуатации средств антивирусной защиты, в том числе контролировать соблюдение Пользователями порядка и правил проведения антивирусного тестирования АРМ;

2.13. осуществлять контроль за соблюдением установленного порядка резервного копирования и восстановления данных, резервирования технических средств АС;

2.14. обеспечивать выполнение требований по обеспечению безопасности информации при подключении АС ФГБОУ ВО СтГМУ Минздрава России к информационно-телекоммуникационной сети «Интернет», в том числе осуществлять мониторинг работы пользователей в информационно-телекоммуникационной сети «Интернет»;

2.15. разрабатывать решения по определению информационных связей между сегментами ЛВС и требованиями к изоляции сегментов с использованием СЗИ, разработке

порядка пользования электронной почтой и ресурсами информационно-телекоммуникационной сети «Интернет»;

2.16. осуществлять текущий и периодический контроль работоспособности и неизменности состояния СЗИ, в том числе контролировать целостность файлов СЗИ с помощью специализированного программного обеспечения;

2.17. с установленной периодичностью проводить анализ защищенности и обнаружение уязвимостей автоматизированных систем, в том числе связанных с ошибками в конфигурации программного обеспечения автоматизированных систем, с помощью специальных программных средств (систем) анализа защищенности;

2.18. производить необходимые настройки и сопровождать в процессе эксплуатации специальные программные средства (системы) обнаружения вторжений в целях обнаружения и (или) блокирования основных угроз безопасности информации, относящихся к вторжениям (атакам), в том числе угроз преднамеренного НСД или специальных воздействий на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе информационно-телекоммуникационной сети «Интернет», и со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к ресурсам автоматизированных систем;

2.19. осуществлять с помощью специализированного программного обеспечения периодический контроль защищенности информации, обрабатываемой в автоматизированных системах, в том числе:

– контролировать эффективность применения СЗИ;

– контролировать соответствие прав пользователей по доступу к защищаемым информационным ресурсам АРМ и серверов, описанных в матрице доступа автоматизированных систем, реальным правам доступа, предоставляемым установленными на АРМ пользователей СЗИ от НСД;

– осуществлять поиск и гарантированное уничтожение информации конфиденциального характера на машинных носителях информации;

2.20. обеспечивать выполнение требований по обеспечению безопасности информации при организации технического обслуживания технических средств автоматизированных систем и отправке их в ремонт (контролировать гарантированное уничтожение информации конфиденциального характера на машинных носителях информации);

2.21. определять состав регистрируемых событий автоматизированных систем, обеспечивать своевременное архивирование журналов событий автоматизированных систем и надлежащий режим хранения данных архивов;

2.22. своевременно анализировать содержимое журналов учета событий автоматизированных систем, регистрируемых СЗИ, операционными системами, прикладным программным обеспечением, с целью выявления возможных нарушений и своевременно реагировать на возникающие нештатные ситуации;

2.23. в случае возникновения нештатных ситуаций (сбоев), фактов неправомерных действий пользователей, приводящих к нарушению установленных требований по защите информации, немедленно информировать ректора ФГБОУ ВО СтГМУ Минздрава России;

2.24. проводить работы по восстановлению работоспособности технических средств и программного обеспечения системы защиты информации в случае их отказа (сбоя), принимать меры по выявлению причин, приведших к отказу работоспособности;

2.25. вести Журнал учета нештатных ситуаций, выполнения профилактических работ, установки и модификации аппаратных и программных средств автоматизированных рабочих мест согласно приложению 1 к настоящему Положению, учитывать факты несоблюдения установленных требований по защите информации, условий хранения носителей информации, использования СЗИ, другие факты, приводящие к снижению уровня защищенности информации конфиденциального характера, факты

выполнения профилактических работ, установки и модификации аппаратных и программных средств АРМ;

2.26. участвовать в проведении служебных проверок по фактам НСД к защищаемой информации, фактам несоблюдения установленных требований при автоматизированной обработке такой информации, условий эксплуатации средств защиты информации, технических средств автоматизированных систем, а также иным фактам, которые могут привести к нарушению или угрозе нарушения безопасности защищаемой информации;

2.27. принимать участие в разработке нормативных документов ФГБОУ ВО СтГМУ Минздрава России, связанных с функционированием автоматизированных систем и применением СЗИ, выполнением мероприятий по обеспечению информационной безопасности;

2.28. осуществлять контроль за выполнением работниками ФГБОУ ВО СтГМУ Минздрава России требований локальных нормативных актов по вопросам автоматизированной обработки и технической защиты информации конфиденциального характера;

2.29. консультировать пользователей по вопросам обеспечения информационной безопасности и ответственности за нарушение установленного порядка автоматизированной обработки и технической защиты информации конфиденциального характера, обучать пользователей правилам работы с СЗИ, в том числе на основе разрабатываемых инструкций, памяток;

2.30. составлять отчеты по результатам своей деятельности, вести Журнал учета мероприятий по контролю защищенности информации конфиденциального характера, обрабатываемой в автоматизированных системах согласно приложению 2 к настоящему Положению;

2.31. вести Журнал учета средств защиты информации согласно приложению 3 к настоящему Положению.

Уполномоченному по ИБ и ОЗКИ запрещается:

2.32. создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к защищаемой информации и предоставлять его другим лицам с целью ее модификации, копирования, уничтожения;

2.33. использовать ставшие доступными в ходе исполнения обязанностей идентификационные и аутентификационные данные пользователей (имена, пароли, ключи) для маскирования своих действий;

2.34. вносить вредоносные изменения в настройки серверной части автоматизированной системы;

2.35. использовать в своих или чьи-либо личных интересах ресурсы автоматизированных систем, предоставлять такую возможность другим;

2.36. передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, конфигурационные настройки;

2.37. производить действия, приводящие к сбою, остановке, замедлению работы автоматизированной системы, блокированию и потере информации;

2.38. нарушать правила эксплуатации технических средств автоматизированных систем;

2.39. подключать технические средства автоматизированных систем к другим техническим средствам, не определенным в обосновании подключения;

2.40. корректировать, удалять журналы событий автоматизированных систем;

2.41. используя служебное положение, выполнять иные действия, приводящие к нарушению или угрозе нарушения безопасности защищаемой информации.

III. ПРАВА УПОЛНОМОЧЕННОГО ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Уполномоченный по ИБ и ОЗКИ имеет право:

3.1. в установленном порядке изменять конфигурацию элементов системы защиты информации;

3.2. в установленном порядке отключать любые элементы системы защиты информации при регламентном техническом обслуживании или устранении неисправностей;

3.3. получать доступ к программным и аппаратным средствам автоматизированных систем, средствам их защиты, а также просмотру прав доступа пользователей к ресурсам на АРМ и серверах автоматизированных систем;

3.4. требовать от работников ФГБОУ ВО СтГМУ Минздрава России соблюдения установленного порядка автоматизированной обработки защищаемой информации и выполнения требований локальных нормативных документов, регламентирующих вопросы обеспечения безопасности информации и технической защиты информации;

3.5. вносить на рассмотрение руководителя ФГБОУ ВО СтГМУ Минздрава России предложения о приостановлении обработки защищаемой информации при обнаружении случаев нарушения установленного порядка автоматизированной обработки защищаемой информации, невыполнения установленных требований по защите информации, нарушения функционирования СЗИ;

3.6. вносить на рассмотрение руководителя ФГБОУ ВО СтГМУ Минздрава России предложения по вопросам совершенствования работы, связанной с предусмотренными настоящей Инструкцией обязанностями;

3.7. инициировать проведение служебных проверок по фактам НСД к защищаемой информации, фактам нарушения установленных требований по защите информации, утраты, порчи технических средств автоматизированных систем, а также иным фактам, которые могут привести к нарушению или угрозе нарушения безопасности защищаемой информации.

IV. ОТВЕТСТВЕННОСТЬ

Уполномоченный по ИБ и ОЗКИ несет ответственность за:

4.1. ненадлежащее исполнение или неисполнение обязанностей и требований, предусмотренных настоящим Положением;

4.2. невыполнение решений и постановлений, приказов, распоряжений и других локальных нормативных документов ФГБОУ ВО СтГМУ Минздрава России, регламентирующих вопросы использования информационных ресурсов ФГБОУ ВО СтГМУ Минздрава России и организации работ по защите информации;

4.3. неприятие мер по устранению выявленных каналов утечки защищаемой информации и НСД к ней, пресечению выявленных нарушений установленных требований по защите информации;

4.4. разглашение информации конфиденциального характера, ставшей ему известной в ходе выполнения предусмотренных настоящим Положением обязанностей.

Приложение № 1

ЖУРНАЛ

учета нештатных ситуаций, выполнения профилактических работ, установки и модификации аппаратных и программных средств автоматизированных рабочих мест

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО и должности исполнителей	Подписи исполнителей	ФИО и должность администратора информационной безопасности	Принятые меры и выполненные действия (в случае нештатной ситуации)	Подпись администратора информационной безопасности	Примечание
		3	4	5	6	7	8	9

Приложение № 2

ЖУРНАЛ
учета мероприятий по контролю защищенности информации конфиденциального характера (персональных данных), обрабатываемой в автоматизированных системах

№ п/п	Дата	Краткое описание проведенного мероприятия	Исполнитель (ФИО и должность администратора информационной безопасности)	Результат мероприятия (отчет, принятые меры, выполненные действия – при наличии)	Подпись исполнителя	Примечание
		3	4	5	6	7

Приложение № 3

ЖУРНАЛ
учета средств защиты информации

№ п/п	Название	Модель, тип	Зав. номер (номер знака соответствия)	Сертификат	Место и дата установки	Примечание
	2	3	4	5	6	7