федеральное государственное бюджетное образовательное учреждение высшего образования
«ОМСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Ректор ФГБОУ ВО ОмГМУ
Минздрава России
_____ М.А. Ливзан
«_19_» ____09_____ 2024 г.

ИНСТРУКЦИЯ

АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОНТРОЛЬНЫЙ

Омск 2024

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНА заведующим сектора информационной безопасности Ключенко А.А.

2. ПРИНЯТА ученым советом 19.09.2024 г., протокол № 10.

3. ВВЕДЕНА в действие с 23.09.2024 г. распоряжением от 20.09.2024 г. впервые.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящая Инструкция устанавливает правила и обязанности администратора информационной безопасности (далее – Администратор ИБ) при работе в информационных системах ФГБОУ ВО ОмГМУ Минздрава России.

1.2 Настоящая Инструкция является локальным нормативным актом Университета, выполнение требований которого обязательно для всех структурных подразделений Университета, должностных лиц и сотрудников, участвующих в работе с информационными системами.

2 НОРМАТИВНЫЕ ССЫЛКИ

2.1 Настоящая Инструкция разработана с учетом следующих положений, законодательных и нормативно-правовых актов:

– Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;

– Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;

– «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;

– методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

– «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;

– «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

3 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

3.1 В настоящей Инструкции применяются следующие обозначения и сокращения:

ФАПСИ – Федеральное агентство правительственной связи и информации при Президенте Российской Федерации;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ИСПДн – информационная система персональных данных;

СКЗИ – средство криптографической защиты информации;

АРМ – автоматизированное рабочее место;

СЗИ – средство защиты информации.

4 ОБЩИЕ ПОЛОЖЕНИЯ

4.1 Администратор ИБ назначается приказом руководителя ФГБОУ ВО ОмГМУ Минздрава России (далее – Организация), и обеспечивает правильность использования и нормальное функционирование установленной системы защиты ИС.

4.2 Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

4.3 В своей деятельности Администратор руководствуется настоящей Инструкцией, Положением об обработке и защите персональных данных, Политикой информационной безопасности и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.

4.4 Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах пользователей. Он несет ответственность за реализацию принятой политики безопасности.

5 ФУНКЦИИ И ОБЯЗАННОСТИ

5.1 Администратор ИБ обязан:

5.1.1 Осуществлять учет и периодический контроль за составом и полномочиями пользователей ИС.

5.1.2 Осуществлять оперативный контроль за работой пользователей ИС, анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных.

5.1.3 Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в ИС СЗИ.

5.1.4 Присутствовать при внесении изменений в конфигурацию (модификации) программно-технических средств ИС, обеспечивать и контролировать установку и настройку СЗИ.

5.1.5 Не реже одного раза в месяц проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

5.1.6 Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил в соответствии с Регламентом управления доступом субъектов доступа к объектам доступа в ИС Организации.

5.1.7 Управлять идентификаторами (осуществлять создание, присвоение и уничтожение идентификаторов пользователей и устройств) и средствами аутентификации (аутентификационной информацией) внутренних пользователей в ИС, обеспечивать соблюдение правил идентификации и аутентификации пользователей и устройств в соответствии с Регламентом идентификации и аутентификации субъектов доступа и объектов доступа в ИС Организации.

5.1.8 Осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации в соответствии с Регламентом идентификации и аутентификации субъектов доступа и объектов доступа в ИС Организации.

5.1.9 Осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в ИС программного обеспечения в соответствии с Регламентом ограничения программной среды в ИС Организации.

5.1.10 Настраивать параметры журналов регистрации событий безопасности в соответствии с Регламентом регистрации событий безопасности в ИС Организации.

5.1.11 Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже одного раза в неделю.

5.1.12 Управлять средствами антивирусной защиты в соответствии с Регламентом антивирусной защиты в ИС Организации.

5.1.13 Осуществлять контроль уровня защищенности информации, обрабатываемой в ИС, в соответствии с Регламентом контроля защищенности информации в ИС Организации.

5.1.14 Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.

5.1.15 Обеспечивать сохранность СЗИ, эксплуатационной и технической документации к СЗИ, а также порядок обращения с СЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации в соответствии с Инструкцией по порядку обращения со средствами защиты информации в ИС Организации.

5.1.16 Проводить не реже одного раза в три месяца контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в соответствии с Регламентом идентификации и аутентификации пользователей в ИС Организации и Регламентом контроля защищенности информации в ИС Организации.

5.1.17 Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ ИС .

5.1.18 Осуществлять поэкземплярный учет в соответствующем журнале:

- СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ);
- эксплуатационной и технической документации к СЗИ.

5.1.19 Осуществлять хранение:

- носителей дистрибутивов СЗИ;
- лицензий и сертификатов на СЗИ.

5.1.20 Не реже одного раза в месяц осуществлять проверки:

- состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);
- состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

5.1.21 Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ИС по вопросам работы с СЗИ.

5.1.22 Отвечать на вопросы обслуживающего и эксплуатирующего персонала ИС, связанные с работой СЗИ.

5.1.23 Составлять инструкции по работе с СЗИ.

5.1.24 Докладывать Руководителю Организации об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.

5.1.25 Участвовать в выявлении инцидентов информационной безопасности и реагировании на них.

5.1.26 Управлять конфигурацией ИС и ее системой защиты информации.

В ходе управления конфигурацией ИС и ее системы защиты информации осуществляются:

- поддержание конфигурации ИС и ее системы защиты информации (структуры системы защиты информации ИС, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИС и ее системы защиты информации);

- управление изменениями базовой конфигурации ИС и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИС и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИС и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИС и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации;
- анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС;
- определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС и ее системы защиты информации;
- внесение информации (данных) об изменениях в базовой конфигурации ИС и ее системы защиты информации в эксплуатационную документацию на систему защиты информации ИС.

5.1.27 В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий. Оперативно докладывать вышестоящему руководству о случаях возникновения внештатных ситуаций и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС. Предпринимаемые меры по возможности согласовывать с вышестоящим руководством.

6 ПРАВА

6.1 Администратор ИБ имеет право:

6.1.3 Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС.

6.1.4 Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ИС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

6.1.5 В пределах своей компетенции сообщать своему непосредственному руководителю обо всех недостатках в работе ИС и ее системы защиты.

6.1.6 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

6.1.7 Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.

6.1.8 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в т.ч. вести мониторинг действий пользователей и обслуживающего персонала ИС).

6.1.9 Вносить свои предложения по совершенствованию мер защиты информации в ИС.

7 ОТВЕТСТВЕННОСТЬ

7.1 Администратор ИБ несет ответственность:

7.1.3 За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской

Федерации.

7.1.4 За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

7.1.5 За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО
Проректор по последипломному образованию

_____ А.С. Колчин

«12» 09 2024 г.

СОГЛАСОВАНО
Начальник ОА и ИТ

_____ Р.А. Ахмеров

«09» 09 2024 г.

СОГЛАСОВАНО
Начальник юридического отдела

_____ О.В. Глевская

«09» 09 2024 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования

_____ С.В. Плоткина

«11» 09 2024 г.