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
_____ марта _____ 2023 г.

ПОЛОЖЕНИЕ

ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОмГМУ

КОНТРОЛЬНЫЙ

Омск 2023

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНО заведующим сектором информационной безопасности С.В. Хабаровым.

2. ПРИНЯТО ученым советом от 16.03.2023 г., протокол №2.

3. ВВЕДЕНО в действие с 20.03.2023 г. распоряжением от 20.03.2023 г. впервые.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее Положение регламентирует мероприятия, процедуры и правила по защите информации в информационных системах в федеральном государственном бюджетном образовательном учреждении высшего образования «Омский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – ФГБОУ ВО ОмГМУ Минздрава России).

1.2 Целями настоящего Положения являются:

– обеспечение конфиденциальности, целостности, доступности защищаемой информации;

– предотвращение утечек защищаемой информации;

– мониторинг событий безопасности и реагирование на инциденты безопасности;

– нейтрализация актуальных угроз безопасности информации;

– выполнение требований действующего законодательства по защите информации.

1.3 В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года действие Положения распространяется к сведениям конфиденциального характера, в ФГБОУ ВО ОмГМУ Минздрава России к таким сведеньям относятся:

– сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами.

– сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

1.3 Действие настоящего положения распространяется на пользователей (далее - Пользователи) и администраторов (далее - Администраторы) информационных систем персональных данных ФГБОУ ВО ОмГМУ Минздрава России.

1.4 Настоящее Положение является локальным нормативным актом Университета, выполнение требований которого обязательно для всех структурных подразделений Университета, должностных лиц и сотрудников, участвующих в обработке персональных данных.

2 НОРМАТИВНЫЕ ССЫЛКИ

2.1 Настоящее Положение разработано 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»;

– Указ Президента Российской Федерации № 188 от 6 марта 1997 года "Об утверждении перечня сведений конфиденциального характера";

– Постановление Правительства РФ № 1119 от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России № 17 от 11 февраля 2013 года «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ ФСТЭК России № 21 от 18 февраля 2013 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при обработке в информационных системах персональных данных;

– 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 настоящем положении применяются следующие обозначения и сокращения:

ИСПДн – информационная система персональных данных;

ПО – программное обеспечение;

СЗИ – средств защиты информации;

ТС – технические средства;

НСД – несанкционированный доступ;

ФЗ – федеральный закон;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ФСБ – Федеральная служба безопасности;

ФАПСИ – Федеральное агентство правительственной связи и информации;

ГРИИБ – Группа реагирования на инциденты информационной безопасности.

4 ОБЩИЕ ПОЛОЖЕНИЯ

4.1 Настоящее положение об информационной безопасности (далее – Положение) утверждается ректором ФГБОУ ВО ОмГМУ Минздрава России.

4.2 Все, что не предусмотрено условиями настоящего Положения, определяется нормами законодательства Российской Федерации, актами уполномоченных органов власти и локальными актами ОмГМУ. В случае изменения законодательства Российской Федерации, принятия уполномоченными органами власти актов, отменяющих или изменяющих нормы, регулируемые Положением, или изменения Устава ОмГМУ настоящее Положение действует в части, им не противоречащей.

5 ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИСПДН, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ИСПДН

5.1 С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ФГБОУ ВО ОмГМУ Минздрава России, допущенному к работе с ИСПДн присваивается учетная запись пользователя. Процедура регистрации (создания учетной записи и выдачи при необходимости электронного ключа) Пользователя ИСПДн для сотрудника и предоставления/изменения ему прав доступа к ресурсам ИСПДн инициируется приказом ректора.

5.2 Использование одного и того же имени пользователя несколькими Пользователями (или группового имени для нескольких пользователей) в ИСПДн запрещено.

5.3 Администратор перед визированием приказа осуществляет верификацию Пользователя (подтверждает его личность).

5.4 После визирования Администратор определяет права доступа для учетной записи и производит необходимые настройки СЗИ от НСД и формирует учетную запись, персональный идентификатор и пароль.

5.5 По окончании внесения изменений в списки пользователей в приказе делается отметка о выполнении задания. Приказ хранится у Администратора и может быть использована для восстановления полномочий Пользователей после сбоев в работе ИСПДн, а также для контроля правомерности наличия у конкретного Пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе инцидентов безопасности.

5.6 Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только Администраторам безопасности, системным Администраторам и сотрудникам сторонней организации, производящим работы в сети ФГБОУ ВО ОмГМУ Минздрава России на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.

5.7 Пользователям запрещены любые действия в ИСПДн до прохождения процедуры идентификации и аутентификации в системе.

6 ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1 В ИСПДн разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей Пользователями.

6.2 Пользователь имеет право подать заявку Администратору, в виде служебной записки, на включение установку дополнительного программного обеспечения, необходимого ему для выполнения служебных (должностных) обязанностей.

6.3 Администратор ежеквартально проводит проверку используемого пользователем ИСПДн программного обеспечения

7 ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

7.1 Администратором должен быть обеспечен учет и контроль перемещения машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Учет носителей ведется в соответствующем журнале учета. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

7.2 Администратором должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения

(стирания) информации. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между Пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

8 ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

8.1 В ФГБОУ ВО ОмГМУ Минздрава России в качестве средства выявления уязвимостей необходимо использовать сертифицированный сканер уязвимостей.

8.2 Администратор не реже одного раза в месяц проводит полное сканирование системы на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ИСПДн производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.

8.3 Администратор изучает отчеты по результатам сканирования и принимает решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться ГРИИБ.

8.4 Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИСПДнО/МЭК 27005-2010

«Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

8.5 При выявлении уязвимостей, Администратор анализирует системные журналы и журналы средств защиты информации, на предмет выявления эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.

8.6 В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом руководителя ФГБОУ ВО ОмГМУ Минздрава России.

9 ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.1 Администратором осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение.

9.2 Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение производится Администратором из доверенных источников.

9.3 При возможности Администратор осуществляет проверку корректности функционирования обновлений в тестовой среде, перед обновлением программного обеспечения производится резервное копирования для обеспечения возможности восстановления данных.

10 ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

10.1 Состав технических средств, программного обеспечения и средств защиты информации ИСПДн фиксируется в техническом паспорте на информационную

систему. Технический паспорт является эталоном состава ТС, ПО и СЗИ, по которому осуществляется периодический контроль.

10.2 В случае добавления новых ТС, ПО и СЗИ в состав ИСПДн или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

10.3 Администратор осуществляет контроль состава ТС, ПО и СЗИ не реже одного раза в месяц.

10.4 Выявление несоответствия состава ТС, ПО и СЗИ техническому паспорту ИСПДн является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

10.5 В случае выявления несоответствия состава ТС, ПО и СЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

10.6 Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СЗИ, то Администратор сообщает об этом руководителю ФГБОУ ВО ОмГМУ Минздрава России, который принимает решение об организации самостоятельной сертификации использующегося СЗИ, либо об обновлении использующегося СЗИ до актуальной версии, либо о замене использующегося СЗИ на другое аналогичное сертифицированное СЗИ.

11 ПРАВИЛА И ПРОЦЕДУРЫ РЕЗЕРВИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ ВОССТАНОВЛЕНИЯ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

11.1 Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ИСПДн осуществляется в соответствии с инструкцией администратора безопасности.

11.2 Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. При выявлении проблем с системой резервирования принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ИСПДн.

11.3 Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ИСПДн.

11.4 Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

11.5 Нештатными ситуациями являются:

1) разглашение информации ограниченного доступа сотрудниками ФГБОУ ВО ОмГМУ Минздрава России, имеющими к ней право доступа, в том числе:

– разглашение информации лицам, не имеющим права доступа к защищаемой информации;

– передача информации по незащищенным каналам связи;

– обработка информации на незащищенных технических средствах обработки информации;

– опубликование информации в открытой печати и других средствах массовой информации;

– передача носителя информации лицу, не имеющему права доступа к ней;

– утрата носителя с информацией.

2) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

– несанкционированное изменение информации;

– несанкционированное копирование информации;

3) несанкционированный доступ к защищаемой информации:

– несанкционированное подключение технических средств к средствам и системам ИСПДн;

– использование закладочных устройств;

– использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ИСПДн;

– использование злоумышленником уязвимостей программного обеспечения ИСПДн;

– использование злоумышленником программных закладок;

– заражение ИСПДн злоумышленником программными вирусами;

– хищение носителей информации;

– нарушение функционирования технических средств обработки информации;

– блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

4) дефекты, сбои, отказы, аварии технических средств и систем ИСПДн;

5) дефекты, сбои, отказы программного обеспечения ИСПДн;

6) сбои, отказы и аварии систем обеспечения ИСПДн;

7) природные явления, стихийные бедствия:

– термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);

– механические факторы (повреждения зданий, землетрясения и т. д.);

– электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

11.6 Инциденты безопасности информации также являются нештатной ситуацией. При выявлении Администратором безопасности нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

11.7 В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

– корректное отключение технических средств ИСПДн до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;

– предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ИСПДн, а также меры по замене/ремонту вышедших из строя средств и систем;

– в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

11.8 В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями, выполняются действия, описанные в инструкции Администратора и Пользователя ИСПДН.

12 ПРАВИЛА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ И ЗАЩИТЫ ОТ СПАМА

12.1 Пользователи и Администраторы в своей работе с электронной почтой руководствуются регламентом работы с электронной почтой.

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО
Первый проректор
_____ Д.Г. Штейнборм
«09» марта 20 23 г.

СОГЛАСОВАНО
Начальник юридического отдела
_____ О.В. Глевская
«09» марта 20 23 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования
_____ С.В. Плоткина
«09» марта 20 23 г.

СОГЛАСОВАНО
Начальник отдела АТ и ИТ
_____ С.Ю. Иванов
«09» марта 20 23 г.