ПРИЛОЖЕНИЕ № 2
УТВЕРЖДЕНО
Приказом «Об утверждении внутренних нормативных
актов по защите информации в информационных системах
по организации ГАУЗ "ККЦ СВМП"
от « 22 » января 2024 г. № 44 »
(М.П.)

Политика информационной безопасности в ГАУЗ "ККЦ СВМП"

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее - Политика) утверждается главным врачом ГАУЗ "ККЦ СВМП" и определяет мероприятия, процедуры и правила по защите информации в информационных системах ГАУЗ "ККЦ СВМП" (далее – ИС).

1.2. Положения настоящей Политики обязательны к исполнению для всех пользователей ИС (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

1.3. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в ГАУЗ "ККЦ СВМП" 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 (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

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

1.4. Целями настоящей Политики 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.

1.5. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

1.6. Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:

– Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о 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.

2. ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИС, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ИС

2.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ГАУЗ "ККЦ СВМП", допущенному к работе с ресурсами ИС, присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

2.2. Под учетной записью Пользователя понимается учетная запись операционной системы для доступа к информационной системе.

2.3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИС запрещено.

2.4. Процедура регистрации (создания учетной записи и выдачи, при необходимости, электронного ключа) пользователя ИС для сотрудника ГАУЗ "ККЦ СВМП" и предоставления ему (или изменения его) прав доступа к ресурсам ИС инициируется заявкой руководителя подразделения, в котором работает этот сотрудник. Форма заявки приведена в Приложении № 1 к настоящей Политике. В заявке указывается:

– содержание запрашиваемых изменений (регистрация нового пользователя ИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИС ранее зарегистрированного пользователя);

– должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;

– полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИС);

– заявку визирует администратор безопасности, утверждая тем самым возможность допуска (изменения прав доступа) данного сотрудника к ресурсам ИС, необходимым для решения им указанных задач.

2.5. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации в ИС. Допуск Пользователей к обработке информации в ИС производится на основании завизированной Администратором заявки, составленной по форме, приведенной в Приложении № 1 к настоящей Политике. При визировании очередной заявки Администратор осуществляет актуализацию следующих документов:

– Положение о разграничении прав доступа в ИС (при необходимости, Приложение № 2 к настоящей Политике);

– Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ИС.

2.6. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки СЗИ от НСД, и формирует учетную запись и первичный пароль. Дает ознакомиться с инструкцией Пользователя ИС под роспись, сообщает пользователю идентификационные данные и допускает к работе в ИС. После допуска к работе в ИС, Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями раздела 3 Инструкции Пользователя ИС.

2.7. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания. Исполненная заявка хранится у Администратора и может быть использована для восстановления полномочий пользователей после сбоев в работе ИС, а также для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИС при разборе инцидентов безопасности.

2.8. Для проведения сотрудниками сторонних организаций временных работ в ИС предусмотрена гостевая временная учетная запись «Guest». Данная учетная запись отключена и активируется (наделяется необходимыми полномочиями) только при необходимости. Все работы от имени такой учетной записи проводятся только под контролем Администратора.

2.9. В качестве модели разграничения доступа к ресурсам ИС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от

необходимости по доступу к тем или иным ресурсам ИС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации в ИС. Описание всех возможных ролей в ИС приведено в Приложении № 2 к настоящей Политике. Помимо учетных записей Пользователей, доступ к системе получают различные системные службы и процессы.

2.10. Администратор обеспечивает оперативное обновление и актуальность:

– Перечня лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами ИС.

– Перечня лиц, допущенных в помещения ГАУЗ "ККЦ СВМП".

2.11. 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 ГАУЗ "ККЦ СВМП" 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.

2.12. Пользователям запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации в системе. Администратору разрешается ряд действий до прохождения идентификации и аутентификации в ИС в ряде случаев. Условия, при которых разрешаются такие действия, и перечень разрешенных действий для Администратора, до прохождения процедуры идентификации и аутентификации в ИС, перечислены в пункте 5.9 инструкции Администратора.

3. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

3.1. С целью определения разрешенных маршрутов прохождения информации между пользователями, устройствами, сегментами в рамках, а также между информационными системами и при взаимодействии с сетью Интернет устанавливаются правила и процедуры управления информационными потоками.

3.2. С целью управления информационными потоками в ИС на всех сетевых устройствах (включая сетевые адаптеры АРМ Пользователей и серверов) прописываются статические маршруты. Список статических сетевых маршрутов фиксируется в Перечне статических сетевых маршрутов в ИС.

3.3. Администратор осуществляет контроль неизменности статических маршрутов, а также добавляет необходимые маршруты в случае необходимости и документирует изменения.

3.4. Контроль и фильтрация информационных потоков между ИС и внешними телекоммуникационными сетями осуществляется с помощью сертифицированного средства межсетевого экранирования (далее - МЭ).

3.5. Для контроля и фильтрации информационных потоков между ИС и внешними телекоммуникационными сетями выбирается политика «Блокировать все, кроме явно разрешенного». Такая политика выбрана с целью исключения возможности доступа Пользователей к сайтам с вредоносным содержимым, а также к фишинговым сайтам (сайты, имитирующие другие легальные сайты с целью кражи аутентификационной и/или личной информации Пользователей). Также такая политика выбрана исходя из практической невозможности блокировки всех фишинговых сайтов и ресурсов с вредоносным содержимым при выборе политики «Разрешено все, кроме явно запрещенного».

3.6. С целью реализации политики контроля и фильтрации информационных потоков между ИС и внешними телекоммуникационными сетями «Блокировать все, кроме явно разрешенного» утверждается Перечень разрешающих правил взаимодействия с внешними телекоммуникационными сетями в ИС. Данный список может быть дополнен на основании служебной записки Администратору с указанием обоснования добавления того или иного ресурса/сайта/протокола/порта в список разрешенных.

3.7. Администратор обеспечивает соответствие настроек МЭ, приведенному в Перечне разрешающих правил взаимодействия с внешними телекоммуникационными сетями в ИС, списку разрешительных правил.

4. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

4.1. В ИС 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.

4.2. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Перечнем разрешенного программного обеспечения в ИС. Пользователям запрещена установка любого ПО в ИС.

4.3. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей, программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

4.4. Администратор ежемесячно проводит проверку соответствия состава программного обеспечения в ИС списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

5. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, КОНТРОЛЬ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

5.1. Одной из основных целей злоумышленников являются машинные носители информации, используемые в ИС для хранения и обработки защищаемой информации. Исходя из этого, защита машинных носителей информации (как в стационарных АРМ и серверах, так и мобильных/съемных) является ключевым звеном политики информационной безопасности.

5.2. Учет машинных носителей осуществляется Администратором в соответствующих журналах. Администратор несет ответственность, за достоверность и своевременность сведений, отраженных в журнале учета машинных носителей информации.

5.3. В ИС учету подлежат:

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные подобные устройства);

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

5.4. 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.

5.5. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

5.6. Администратор маркирует съемные машинные носители, использование которых разрешено за пределами контролируемой зоны и информационной системы, и делает соответствующую отметку в журнале. Использование немаркированного соответствующим образом носителя информации за пределами контролируемой зоны и/или информационной системы является инцидентом информационной безопасности и расследуется в установленном порядке.

5.7. Использование неучтенных съемных носителей и портативных устройств (в том числе личных) в ИС запрещено.

5.8. Невозможность использования неучтенных съемных носителей информации обеспечивается путем программных настроек сертифицированного средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД). Настройками СЗИ от НСД неучтенные носители информации блокируются на всех стационарных устройствах ИС. Попытки использования неучтенных съемных носителей информации фиксируются средствами СЗИ от НСД. Такие попытки являются инцидентами безопасности и расследуются в установленном порядке.

5.9. Невозможность использования неучтенных портативных вычислительных устройств обеспечивается путем организации аутентификации в системе не только пользователя ИС, но и самого устройства по нескольким параметрам (имя устройства, IP-адрес, MAC-адрес и другие).

5.10. Невозможность использования неучтенных машинных носителей в стационарных устройствах обеспечивается путем физического контроля доступа в соответствии с инструкциями Пользователя и Администратора, а также путем проведения периодических мероприятий по инвентаризации ресурсов ИС и комплектности технических средств.

5.11. Гарантированное уничтожение (стирание) информации на машинных носителях организовывается Администратором в случаях:

– возвращения учтенного съемного носителя информации Администратору;

– при вводе в эксплуатацию нового машинного носителя или технического средства со встроенными носителями информации;

– при передаче носителя информации в сторонние организации (в том числе и для проведения ремонта технического средства);

– при утилизации технических средств.

5.12. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации. Контроль невозможности восстановления уничтоженной информации производится Администратором с помощью специализированных утилит по восстановлению информации.

5.13. При возвращении учтенного съемного носителя информации Пользователем, а также при вводе в эксплуатацию нового машинного носителя, информация уничтожается путем использования механизма СЗИ от НСД затирания файлов случайной битовой последовательностью.

5.14. При передаче носителя информации в сторонние организации (не с целью передачи на нем информации), в том числе и для ремонта носителя или технического средства, информация уничтожается путем полной многократной перезаписи машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации. Затем производится очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти, специализированными программами или утилитами производителя.

5.15. В случаях уничтожения информации способами, описанными в пунктах 5.13 и 5.14 настоящей Политики, Администратор фиксирует факт уничтожения информации, а также факт контроля уничтожения информации в Журнале учета мероприятий по защите информации в ИС.

5.16. При утилизации технических средств, а также при возникновении необходимости уничтожения информации на неперезаписываемых машинных носителях (например, CD-R), физически уничтожается сам машинный носитель.

5.17. В случае физического уничтожения машинного носителя информации, составляется акт уничтожения. Акт уничтожения машинных носителей подписывается назначенной приказом руководителя комиссией по уничтожению персональных данных и по форме утвержденного акта уничтожения персональных данных.

6. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ)

6.1. Администратор запрещает доступ пользователей внешних информационных систем к ресурсам ИС.

6.2. Администратор обеспечивает управление информационными потоками при взаимодействии с внешними информационными системами в соответствии с правилами и процедурами, описанными в разделе 4 настоящей инструкции.

6.3. Порядок обработки, хранения и передачи информации с использованием внешних информационных систем определяются технологическими процессами обработки информации в ИС.

6.4. Взаимодействие ИС с информационными системами возможно только при выполнении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

– при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

7. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

7.1. Для выявления уязвимостей в ИС привлекается Организация-лицензиат ФСТЭК России. Организация-лицензиат ФСТЭК России проводит полное сканирование ИС на выявление уязвимостей, применяя при этом сертифицированный сканер уязвимости.

7.2. Сканирование ИС на наличие уязвимостей проводится с периодичностью, необходимой и достаточной для должной обработки отчета по результатам сканирования и принятия мер по устранению выявленных уязвимостей, но не реже одного раза в квартал.

7.3. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ИС необходимо организовать внеплановое полное сканирование информационной системы.

7.4. 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.

7.5. 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 ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

7.6. 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.

7.7. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом Временно исполняющего обязанности главного врача ГАУЗ "ККЦ СВМП".

8. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

8.1. С целью противодействия эксплуатации известных уязвимостей, в ГАУЗ "ККЦ СВМП" устанавливаются правила и процедуры контроля установки обновлений системного и прикладного программного обеспечения.

8.2. В программном обеспечении, поддерживающем автоматические обновления, таких как Java, Acrobat Reader и т. д. автоматические обновления не отключаются.

8.3. Общесистемное программное обеспечение и основное прикладное программное обеспечение обновляется во внерабочее время. Администратор перед обновлениями создает образы системы, точки восстановления и резервные копии баз данных.

8.4. Администратор контролирует источники обновлений программного обеспечения. Обновления должны осуществляться из доверенных источников, в соответствии с документацией на программное обеспечение.

8.5. Обновления общесистемного и основного прикладного программного обеспечения осуществляются не реже одного раза в неделю. Экстренные обновления осуществляются в случае поступления информации о критичных уязвимостях, для которых существует обновление безопасности.

8.6. Администратор в соответствии с эксплуатационной документацией на программное обеспечение осуществляет проверку установки обновлений, а также корректность установки обновлений. В ГАУЗ "ККЦ СВМП" должно применяться только такое программное обеспечение, которое поддерживает проверку целостности файлов обновлений.

8.7. Обновление антивирусных баз, сигнатур уязвимостей, баз решающих правил средств защиты информации осуществляется в соответствии с эксплуатационной документацией на СЗИ и разделами настоящей Политики.

8.8. Обновление микропрошивок и программного обеспечения BIOS/UEFI производится только при поступлении информации о критичных уязвимостях в таком программном обеспечении, применяемом в ГАУЗ "ККЦ СВМП".

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

9.1. Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ИС фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

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

9.3. Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

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

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

9.6. 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 СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом руководству ГАУЗ "ККЦ СВМП", который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

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

10.1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ИС осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 3 к настоящей Политике.

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

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

10.4. Нештатными ситуациями являются:

– разглашение информации ограниченного доступа сотрудниками ГАУЗ "ККЦ СВМП", 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.

– неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
  - несанкционированное изменение информации;
  - несанкционированное копирование информации;

– несанкционированный доступ к защищаемой информации:
  - несанкционированное подключение технических средств к средствам и системам ИС;
  - использование закладочных устройств;
  - использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ИС;
  - использование злоумышленником уязвимостей программного обеспечения ИС;
  - использование злоумышленником программных закладок;
  - заражение ИС 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;
  - дефекты, сбои, отказы, аварии технических средств и систем ИС;
  - дефекты, сбои, отказы программного обеспечения ИС;
  - сбои, отказы и аварии систем обеспечения ИС;

– 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.).

10.5. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.

10.6. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 4 настоящей Политики.

10.7. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления, по результатам тренировок, изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

10.8. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении 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.

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

– корректное отключение технических средств ИС 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 ИС, 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.

10.10. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями, выполняются следующие действия:

– Пользователи корректно отключают и обесточивают свои рабочие места;

– системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;

– Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;

– в случае нарушения корректной работы технических средств в ИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;

– в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;

– в случае стихийных бедствий/природных явлений, опасных для жизни человека, в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

Приложение № 1 к Политике информационной безопасности
в ГАУЗ "ККЦ СВМП", утвержденной приказом
от «22 » января 2024 г. № 44-о

ЗАЯВКА

на внесение изменений в списки пользователей

и наделение пользователей полномочиями доступа к ресурсам

_____

(наименование информационной системы)

Прошу зарегистрировать пользователя (исключить из списка пользователей, изменить полномочия пользователя)

(нужное подчеркнуть)

_____

(должность с указанием подразделения)

_____

(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, излишних)

(нужное подчеркнуть)

для решения задач:

_____

(список задач)

_____

_____

_____

Начальник

_____

(наименование заказывающего подразделения)

«___» _____ 20__ г. _____ _____

(подпись) (фамилия)

Администратор безопасности

Согласовано

«___» _____ 20__ г. _____ _____

(подпись) (фамилия)

ЗАДАНИЕ

на внесение изменений в списки пользователей

_____

(наименование информационной системы)

Администратору безопасности информации

_____

(фамилия и инициалы исполнителя)

Произвести изменения в списках пользователей

Временно исполняющий обязанности главного врача

ГАУЗ "ККЦ СВМП"

_____ И.С. Зеленкова

«___» _____ 20___ г.

Обратная сторона заявки

Присвоено имя _____ (персональный идентификатор) и предоставлены полномочия, необходимые для решения следующих задач:

Наименование задач

Администратор безопасности _____

(подпись, фамилия)

Имя учетной записи и начальное значение пароля получил, о порядке смены пароля при первом входе в систему проинструктирован, с инструкцией Пользователя информационных систем ГАУЗ "ККЦ СВМП" ознакомлен

Пользователь _____

(подпись, фамилия)

«___» _____ 20___ г.

Приложение № 2 к Политике информационной безопасности
в ГАУЗ "ККЦ СВМП", утвержденной приказом
от «22 » января 2024 г. № 44-о

Положение о разграничении прав доступа в информационных системах ГАУЗ "ККЦ СВМП"

Исходя из характера и режима обработки защищаемой информации в информационных системах ГАУЗ "ККЦ СВМП" (далее - ИС) определяется следующий перечень групп Пользователей, служб и процессов, участвующих в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам ИС приведен в таблице.

Роль	Описание параметров доступа к ресурсам ИС для данной роли
Администратор безопасности	Доступ на запись и чтение защищаемой информации, настройкам операционной системы и СЗИ. Полный доступ к системным журналам, журналам средств защиты информации и другим электронным журналам сообщений.
Системный администратор	Доступ на запись и чтение защищаемой информации, настройкам операционной системы. Полный доступ к системным журналам и другим электронным журналам сообщений, за исключением журналов средств защиты информации.
Пользователь	Доступ на запись и чтение защищаемой информации при работе с прикладным программным обеспечением. Из под учетных записей с этой ролью разрешен запуск всех не системных процессов, необходимых для выполнения служебных обязанностей.
Средство анализа защищенности	Доступ на чтение к системному реестру Windows. Доступ на чтение файловой структуры и папок на жестких дисках. Доступ на запись во временную директорию %SystemRoot%\Temp.

Приложение № 3 к Политике информационной безопасности
в ГАУЗ "ККЦ СВМП", утвержденной приказом
от «22 » января 2024 г. № 44-о

Порядок резервирования информационных ресурсов в информационных системах ГАУЗ "ККЦ СВМП"

№ п/п	Наименование информационного ресурса	Место размещения ресурса в системе	Вид резервного копирования	Ответственный за резервное копирование	Место хранения резервной копии	Частота резервного копирования
1.	Образы операционных систем	Все АРМ	Образ системы, периодическое	Администратор информационной безопасности	Учтенные носители информации	По мере внесения существенных изменений в состав операционных систем
2.	Средство защиты информации	Все АРМ	Эталонный дистрибутив	Администратор информационной безопасности	Сейф администратора информационной безопасности	Единовременно

Приложение № 4 к Политике информационной безопасности
в ГАУЗ "ККЦ СВМП", утвержденной приказом
от «22 » января 2024 г. № 44-о

План обеспечения непрерывности функционирования информационных системах ГАУЗ "ККЦ СВМП"

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
1.	Разглашение защищаемой информации сотрудниками, имеющими легальные права доступа к ней	1	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
2.	Обнаружение несанкционированно скопированной или измененной конфиденциальной информации	1	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
3.	Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней	1	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	1 день
4.	Обнаружение подключения технических средств к средствам и системам объекта информатизации	1	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	3 часа
5.	Подключение технических средств к средствам и системам ГИС в текущий момент времени	1	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	3 часа
6.	Обнаружение закладочных устройств	1	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	Сразу после получения информации об инциденте	1 день
7.	Установка закладочных устройств злоумышленником в текущий момент времени	1	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
8.	Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
9.	Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки	1	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
10.	Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени	1	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
11.	Использование программных закладок внешним нарушителем в текущий момент времени	1	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
12.	Использование программных закладок внутренним злоумышленником или обнаружение факта использования	1	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
13.	Обнаружение программных вирусов	1	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
14.	Хищение носителя защищаемой информации	1	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 сутки	3 дня
15.	Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
16.	Обнаружение нарушения функционирования ТС обработки информации произведенного	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	злоумышленником	Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
17.	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней
18.	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
19.	Обнаружение произошедшего факта блокировки доступа к защищаемой информации	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
20.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации	-	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	1 день
21.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	20 минут	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	20 минут	1 день
22.	Дефекты, сбои, отказы, аварии ТС, программных средств и систем ГИС	Сбой ТС и систем ГИС	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	1 час	2 дня

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
		Отказ ТС и систем ГИС, затронувший работу группы пользователей	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день
		Отказ ТС и систем ГИС, затронувший работу одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	1 час	2 дня
		Авария ТС и систем ГИС	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
23.	Сбои, отказы и аварии систем обеспечения ГИС	Сбой систем обеспечения ГИС	Ответственному за материально- техническое обеспечение сразу после инцидента	Ответственному за материально- техническое обеспечение в первый рабочий день после инцидента	1 час	1 день
		Отказ систем обеспечения ГИС, затронувший работу группы пользователей	Ответственному за материально- техническое обеспечение и Администратору сразу после обнаружения инцидента	Ответственному за материально- техническое обеспечение и Администратору сразу после обнаружения инцидента	1 час	1 день
		Отказ систем обеспечения ГИС, затронувший работу одного пользователя	Ответственному за материально- техническое обеспечение сразу после инцидента	Ответственному за материально- техническое обеспечение в первый рабочий день после инцидента	1 час	2 дня
		Авария систем обеспечения ГИС	Ответственному за материально- техническое обеспечение, Администратору сразу после обнаружения инцидента	Ответственному за материально- техническое обеспечение, Администратору не позднее 8 часов после инцидента	1 час	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
24.	Природные явления, стихийные бедствия, несущие угрозу жизни человека	1	Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	10 минут	30 минут
25.	Природные явления, стихийные бедствия, не несущие угрозу жизни человека	1	Руководителю, заместителям Руководителя, Администратору	Руководителю, заместителям Руководителя, Администратору	10 минут	1 час