Приложение № 1

УТВЕРЖДЕНО
Приказом ГБУ РО «ОКЦФП»
от 24.11.2025г. №36

ПОЛИТИКА
информационной безопасности ГБУ РО «ОКЦФП»

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ....4
1.1. Назначение документа....4
1.2. Цель документа....4
1.3. Область применения документа....4
1.4. Основные виды и способы обработки защищаемой информации....5
1.5. Категории субъектов ПДн....5
1.6. Состав обрабатываемых ПДн и основания их обработки....5
2. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕРОПРИЯТИЯ....6
2.1. Основные мероприятия по защите информации....6
3. ПРАВИЛА И ПРОЦЕДУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ....7
3.1. Общие положения....7
3.2. Идентификация и аутентификация....8
3.3. Управление доступом....9
3.4. Защита носителей информации....13
3.5. Уничтожение информации и обезличивание ПДн....14
3.6. Антивирусная защита....15
3.7. Обнаружение и предотвращение вторжений....16
3.8. Обеспечение целостности и доступности....17
3.9. Защита помещений и технических средств....18
3.10. Защита информационной системы, систем связи и передачи данных....19
3.11. Защита среды виртуализации и контейнеризации....20
3.12. Защита мобильных рабочих мест....20
3.13. Управление конфигурацией....23
3.14. Ограничение программной среды....25
3.15. Анализ защищенности и управление уязвимостями....27
3.16. Управление событиями и инцидентами безопасности....28
4. ВЫВОД ИЗ ЭКСПЛУАТАЦИИ....32
5. ВНУТРЕННИЙ КОНТРОЛЬ И АУДИТ....32
5.1. Общие положения....32
5.2. Порядок проведения внутреннего контроля....33
5.3. Порядок проведения внутреннего аудита....33
6. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ....33
6.1. Общие положения....33
6.2. Регламент работ внешних подрядчиков....34
6.3. Правила работы в сети Интернет....35

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
БВТ	Бездисковый видеодисплейный терминал
ЗИ	Защита информации
ИБП	Источник бесперебойного питания
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ОРД	Организационно-распорядительная документация
ПДн	Персональные данные
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
РД	Руководящий документ
СЗИ	Система защиты информации
СрЗИ	Средство защиты информации
СПО	Системное программное обеспечение
ССОП	Сети связи общего пользования
СУБД	Система управления базами данных
ТС	Технические средства
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение документа

1.1.1. Настоящий документ определяет набор правил и процедур обеспечения информационной безопасности в ГБУ РО «ОКЦФП».

1.1.2. Нарушение правил и процедур обеспечения информационной безопасности, определенных настоящей Политикой, влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность.

1.2. Цель документа

1.2.1. Основной целью Политики является создание условий для безопасного и бесперебойного функционирования объектов инфраструктуры ГБУ РО «ОКЦФП» в соответствии с требованиями действующего законодательства.

1.3. Область применения документа

1.3.1. Настоящая Политика применяется в отношении автоматизированной системы (АС) ГБУ РО «ОКЦФП» предназначенной для автоматизации процессов оказания и учета медицинской помощи, информационной поддержки медицинских работников, при взаимодействии с сервисами информационных систем в сфере здравоохранения по модели SaaS (software as a service). К объектам защиты АС ГБУ РО «ОКЦФП», относятся:

- защищаемая информация;
- средства защиты информации;
- средства криптографической защиты информации;
- среда функционирования средств защиты информации (средства вычислительной техники, системное и прикладное ПО);
- любая информация, относящаяся к системе защите информации;
- документы, дела, журналы, картотеки, издания, технические документы, видео -, кино - и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация;
- носители защищаемой информации и мобильные устройства;
- используемые информационной системой каналы (линии) связи, включая кабельные системы;
- помещения, в которых находятся компоненты АС ГБУ РО «ОКЦФП».

1.3.2. К защищаемой информации в АС ГБУ РО «ОКЦФП» относятся сведения, отнесенные к категории конфиденциальных в соответствии с Указом Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера», в том числе информация, содержащая персональные данные (ПДн) касающиеся состояния здоровья субъектов персональных данных (врачебная тайна). Также, к защищаемой информации, относится следующая сопутствующая информация:

- перечень составных частей АС ГБУ РО «ОКЦФП», участвующих в обработке защищаемой информации;

- состав возможных уязвимостей АС ГБУ РО «ОКЦФП», возможных последствий от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальность, целостность, доступность);
- структурно-функциональные характеристики, включающие структуру и состав АС ГБУ РО «ОКЦФП», физические, функциональные и технологические взаимосвязи между составными частями и взаимосвязи с иными системами, режимы обработки информации в целом и в отдельных составных частях;
- меры и средства защиты информации, применяемые в ГБУ РО «ОКЦФП»;
- сведения о реализации системы защиты информации в ГБУ РО «ОКЦФП»
- закрытые ключи шифрования и электронной подписи.

1.3.3. Настоящей Политикой руководствуются сотрудники ГБУ РО «ОКЦФП», замещающие должности, предусматривающие осуществление доступа к объектам защиты.

1.4. Основные виды и способы обработки защищаемой информации

1.4.1. Обработка защищаемой информации производится как с использованием средств вычислительной техники (автоматизированная обработка) так и без использования таких средств.

1.4.2. Основными способами обработки защищаемой информации являются: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение.

1.5. Категории субъектов ПДн

1.5.1. Основными категориями субъектов ПДн являются физические лица, обратившиеся за медицинскими услугами, не являющиеся сотрудниками ГБУ РО «ОКЦФП», а также сотрудники ГБУ РО «ОКЦФП».

1.6. Состав обрабатываемых ПДн и основания их обработки

1.6.1. Обработка ПДн осуществляется в соответствии с учредительными документами ГБУ РО «ОКЦФП», Федеральным законом от 21.11.2011 №323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных".

1.6.2. Состав ПДн определяется требованиями к оформлению медицинской документации на основании распорядительных документов, а также функционалом сервисов информационных систем в сфере здравоохранения, при выполнении следующих задач:

- персонифицированный учет оказанных медицинских услуг и медикаментов:
- ведение электронной медицинской карты гражданина;
- запись к врачу в электронном виде;
- обмен телемедицинскими данными;
- проведение лабораторных исследований;
- внедрение систем электронного документооборота;
- ведение единого регистра медицинских работников;

- ведение электронного паспорта медицинского учреждения и паспорта системы здравоохранения субъекта Российской Федерации.

1.6.3. Массивы информации, используемые при реализации вышеуказанных задач, содержат специальные категории персональных данных касающиеся состояния здоровья субъектов ПДн, подлежащие защите в соответствии с действующим законодательством.

2. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕРОПРИЯТИЯ

2.1. Основные мероприятия по защите информации

2.1.1. Руководством ГБУ РО «ОКЦФП» назначается ответственный за обеспечение информационной безопасности (далее, ответственный за обеспечение ИБ), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, уровня не ниже заместителя руководителя ГБУ РО «ОКЦФП».

2.1.2. Руководством ГБУ РО «ОКЦФП» назначается администратор(ы) информационной безопасности (далее Администратор(ы) ИБ), осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты из числа штатных специалистов ГБУ РО «ОКЦФП», наиболее компетентных в этой области.

2.1.3. Ответственным за обеспечение ИБ формируется, а руководством ГБУ РО «ОКЦФП» утверждается перечень объектов защиты и ответственных лиц.

2.1.4. Ответственным за обеспечение ИБ формируется, а руководством ГБУ РО «ОКЦФП» утверждается план мероприятий по защите информации в АС ГБУ РО «ОКЦФП» на следующий календарный год.

2.1.5. Ответственным за обеспечение ИБ формируется, а руководством ГБУ РО «ОКЦФП» утверждается перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

2.1.6. В целях исполнения требований законодательства и соблюдения принципа персональной ответственности, ответственным за обеспечение ИБ организуется ознакомление под роспись всех лиц допущенных к обработке защищаемой информации с *Основными нормативно-правовыми актами и организационно–распорядительной документацией регулирующими порядок обработки и защиты информации в автоматизированной системе государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии» (Приложение 1)*, при необходимости организуется обучение указанных сотрудников.

2.1.7. Ответственным за обеспечение ИБ организуется оформление между лицами (как физическими, так и юридическими) допущенными к работам в АС ГБУ РО «ОКЦФП» и оператором в лице ГБУ РО «ОКЦФП», *Соглашения о соблюдении правил обеспечения информационной безопасности в автоматизированной системе государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии» (Приложения 2 и 3)*.

2.1.8. Ответственным за обеспечение ИБ организуется уведомление уполномоченного органа по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн. Уведомление осуществляется через официальный портал Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) http://pd.rsoc.ru/operators-registry/notification/form/.

2.1.9. Ответственным за обеспечение ИБ организуется заключения договора - поручения на обработку персональных данных третьими лицами, в случае если принятая информационная технология подразумевает такую обработку.

2.1.10. Ответственным за обеспечение ИБ формируется, а руководством ГБУ РО «ОКЦФП» утверждаются правила рассмотрения запросов субъектов персональных данных или их представителей.

2.1.11. Ответственным за обеспечение ИБ формируется, а руководством ГБУ РО «ОКЦФП» утверждается политика в отношении обработки персональных данных, с последующим опубликованием на официальном сайте в течение 10 дней после утверждения.

3. ПРАВИЛА И ПРОЦЕДУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Общие положения

3.1.1. Технологический процесс обработки информации полностью определяется составом и функциональными возможностями прикладных программных компонентов и функционалом сервисов внешних информационных систем при обработке информации по модели SaaS, технических и программных средств, правилами эксплуатации технических и программных средств и навыками пользователей, реализующих и управляющих основными операциями обработки данных в АС ГБУ РО «ОКЦФП».

3.1.2. Для предотвращения действий злоумышленников, случайных и преднамеренных действий пользователей, приводящих к утрате документов и утечке защищаемой информации, нарушениям целостности и доступности, а также к отказам в обслуживании программных и аппаратных средств, ответственным за обеспечение ИБ организуется работа по созданию системы защиты информации, в том числе персональных данных в АС ГБУ РО «ОКЦФП».

3.1.3. Создание системы защиты информации подразумевает внедрение в действующий технологический процесс ряда подсистем защиты информации:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управления доступом субъектов доступа к объектам доступа;
- ограничения программной среды;
- регистрации событий безопасности;
- антивирусной защиту;
- обнаружения (предотвращение) вторжений;
- контроля (анализа) защищенности информации;
- целостности информационной системы и информации;
- доступности информации;

- защиты среды виртуализации и контейнеризации;
- защиты технических средств;
- защиты информационной системы, ее средств, систем связи и передачи данных.

3.1.4. Для реализации вышеуказанных подсистем используются сертифицированные ФСТЭК и ФСБ России средства защиты информации имеющие сертификат на соответствие средствам защиты информации не ниже 5 класса и 5 уровня доверия, средства вычислительной техники не ниже 5 класса, а также средства криптографической защиты информации имеющие сертификат на соответствие классу КС1 и выше.

3.2. Идентификация и аутентификация

3.2.1. Общие положения

3.2.1.1. Парольная защита осуществляется с целью предотвращения несанкционированного, в том числе случайного доступа к защищаемой информации и интерфейсу настроек оборудования. Парольная защита применяется для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

3.2.1.2. В целях реализации многофакторной политики аутентификации учетные записи пользователей (логины) составляют личный секрет пользователя.

3.2.1.3. Учетная информация (логины и пароли) является конфиденциальной.

3.2.1.4. К основным и обязательным видам паролей относятся:

- пароли BIOS;
- пароли на доступ к средам операционных систем и интерфейсам систем управления, включая подсистемы виртуализации и контейнеризации;
- пароли доступа к антивирусным средствам;
- пароли доступа к средствам обнаружения вторжений;
- пароли доступа к средствам межсетевого экранирования;
- пароли доступа к средствам анализа защищенности;
- пароли доступа к файлам архивов и образов дисков;
- пароли доступа к коммутационному оборудованию (коммутаторы, маршрутизаторы и т.п).

3.2.1.5. Логины и пароли доступа, первично назначаются Администратором ИБ, в соответствии со следующими требованиями:

- длина всех видов логинов и паролей пользователей, вводимых с клавиатуры должна быть не менее 6 символов буквенно-цифрового множества в верхнем и нижнем регистрах;
- длина пароля для всех видов административных логинов должна быть не менее 8 символов буквенно-цифрового множества, в верхнем и нижнем регистрах;
- срок действия логинов и паролей не должен превышать 90 дней;

- запрещено использовать последние 4 использовавшихся логина и пароля;
- запрещено использовать логины и пароли, установленные по умолчанию (например пароли доступа по умолчанию для коммутирующего и сетевого оборудования).

3.2.1.6. Введение строгой политики логинов и паролей направлено на запрет использования легко вычисляемых сочетаний символов (имена, фамилии, дни рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, общепринятые сокращения [ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.], закономерные порядки [123456, qwerty и т. п.]) и другие данные, которые могут быть подобраны путем анализа.

3.2.1.7. Пользователи обязаны своевременно сообщать Администратору ИБ о всех нештатных ситуациях, нарушениях работы подсистемы идентификации и аутентификации, возникающих при работе с логинами и паролями.

3.2.1.8. При организации парольной защиты запрещается:

- записывать свои логины и пароли в очевидных местах (внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.п.);
- хранить логины и пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги;
- сообщать посторонним лицам свои логины и пароли, а также сведения о применяемой системе защиты от НСД.

3.2.1.9. На Администратора ИБ возлагаются следующие задачи:

- обеспечение функционирования системы парольной защиты и оказание помощи пользователям в ее реализации;
- контроль за реализацией требований парольной защиты пользователями.

3.2.2. Порядок применения парольной защиты

3.2.2.1. Защита с применением логинов и паролей осуществляется в соответствии с эксплуатационной документацией на технические и программные средства.

3.2.2.2. В случае отсутствия технической возможности реализовать требования к длине логинов и паролей, необходимо использовать максимально допустимую длину, предусмотренную программным обеспечением технических средств.

3.2.2.3. Плановая смена логинов и паролей проводится регулярно Администратором ИБ, не реже одного раза в 90 дней.

3.2.2.4. Внеплановая смена логина и пароля должна производиться в следующих случаях:

- компрометация логина и пароля;
- в случае прекращения полномочий пользователя (увольнение, переход на другую работу, не связанную с обработкой защищаемой информации);
- по указанию ответственного за обеспечение ИБ.

3.2.2.5. Компрометация действующих логинов и паролей является нештатной ситуацией, о чем пользователи сообщают Администратору ИБ. Под компрометацией понимается хищение,

утрата действующих логинов и паролей, передача или сообщение их лицам, не имеющим на то право, другие действия сотрудников, приведшие к получению его учетной информации лицами, не имеющими на то права.

3.2.3. Защита обратной связи

3.2.3.1. Вывод последних использованных логинов пользователей при проведении всех видов идентификации и аутентификации запрещается.

3.3. Управление доступом

3.3.1. Общие положения

3.3.1.1. Управление доступом обеспечивается организационными и техническими мерами.

3.3.1.2. Доступ к защищаемой информации и ее носителям разрешается только лицам, прошедшим процедуру допуска. При этом указанные лица должны иметь доступ только к той информации, которая необходима для выполнения их функциональных обязанностей.

3.3.1.3. До начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств). Перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации определяется Администратором ИБ. Способ реализация данного функционала зависит от возможностей коммутационного оборудования.

3.3.1.4. Процедура допуска сотрудников ГБУ РО «ОКЦФП» (в том числе и находящихся на испытательном сроке) и сотрудников внешних организаций к объектам защиты АС ГБУ РО «ОКЦФП», включает в себя следующие мероприятия:

- оформление основания для допуска однозначно определяющего физическое лицо, допускаемое к работам в АС ГБУ РО «ОКЦФП». Таким основанием для штатных сотрудников ГБУ РО «ОКЦФП» является приказ о назначения сотрудника на должность подразумевающую доступ к персональным данным. Основанием для допуска сотрудников внешних организаций является официальное письмо с просьбой о предоставлении допуска сотрудникам внешней организации с указанием ФИО и паспортных данных допускаемого лица, с указанием основания допуска (например осуществление технической поддержки по договору №____) или оформление предписания на выполнение работ, с указанием основания допуска (например осуществление технической поддержки по договору №____) или служебное удостоверение предоставляющее право допуска к объектам защиты в соответствии с действующим законодательством.
- оформление *Соглашения о соблюдении правил обеспечения информационной безопасности в автоматизированной системе государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»;*
- ознакомление под роспись с *Основными нормативно-правовыми актами, регулирующими порядок обработки и защиты информации в автоматизированной*

системе государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»;

- инструктаж по порядку работы в защищенной информационной системе у Администратора ИБ.

3.3.2. Порядок использования учетных записей устройств (технических средств)

3.3.2.1. Каждое сетевое устройство, в соответствии со стандартом IEEE MAC-48 использует уникальный MAC-адрес, который должен использоваться в качестве идентификатора устройства в АС ГБУ РО «ОКЦФП».

3.3.2.2. Аутентификация устройств в АС ГБУ РО «ОКЦФП» должна осуществляться на основе механизма аутентификации портов коммутаторов, которая позволяет проверять права доступа клиентов к портам коммутатора с использованием сервера аутентификации или функции “port security”. Рекомендуется использовать коммутаторы предусматривающие проверку прав доступа (аутентификацию) к портам с использованием MAC-адреса в соответствии со стандартом 802.1X.

3.3.3. Порядок использования учетных записей пользователей

3.3.3.1. Каждому лицу, допущенному к работам в АС ГБУ РО «ОКЦФП» сопоставляется уникальная учетная запись пользователя (логин), под которой он будет регистрироваться, и работать. Значение учетной записи не должно совпадать с ранее использованной в течении последнего года.

3.3.3.2. В случае производственной необходимости, некоторым лицам могут быть сопоставлены несколько уникальных имен (учетных записей).

3.3.3.3. Использование несколькими лицами общей учетной записи запрещено.

3.3.4. Управление учетными записями пользователей.

3.3.4.1. Основанием для создания, блокирования или удаления учетной записи штатного сотрудника (пользователя) служат копии приказов или любые другие распоряжения по персоналу, касающиеся изменения статуса пользователя при условии прохождения пользователем процедуры допуска согласно п. 3.3.1.4. Возможные статусы по персоналу:

- принят на должность;
- уволен;
- отпуск, командировка и т.п.

3.3.4.2. Копии документов, являющихся основаниями для допуска (распоряжений, приказов по кадрам и т.п.), в соответствии с которыми незамедлительно производится настройка учетных записей, предоставляются Администратору ИБ ежедневно.

3.3.4.3. Сотруднику, зарегистрированному в качестве нового пользователя, сообщается имя соответствующего ему пользователя и начальное значение пароля.

3.3.4.4. Блокирование учетной записи производится в случае планируемого отсутствия пользователя на срок более 90 суток.

3.3.4.5. Программные средства настраиваются Администратором ИБ на блокирование учетных записей пользователя и администратора не менее чем на 10 минут при достижении максимально допустимого количества неуспешных попыток входа с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль). Допускается не более 8 неуспешных попыток входа.

3.3.4.6. Учетные записи пользователей должны состоять в группе «Пользователи» и быть ограниченными в праве установки, удаления и настройки системного и прикладного программного обеспечения и оборудования.

3.3.4.7. Не допускается присутствие активных неиспользуемых учетных записей.

3.3.5. Управление правами доступа

3.3.5.1. Администратором ИБ, любым доступным способом, производится отключение беспроводных интерфейсов, а также интерфейсов взаимодействия с мобильными технических средствами с функцией модема, на технических средствах где такой интерфейс связи не является основным (мобильные устройства), таким образом, чтобы пользователь не имел возможности их включить повторно.

3.3.5.2. Должна быть исключена несанкционированная удаленная активация видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, а при их активации должно производиться оповещение пользователей об активации таких устройств.

3.3.5.3. Системы BIOS всех технических средств настраиваются Администратором ИБ на запрет загрузки с внешних носителей, путем определения приоритетов загрузочных устройств.

3.3.5.4. При наличии штатного функционала преобразования данных (шифрования) операционной системы или средства защиты информации Администратором ИБ может задействоваться данный функционал в качестве компенсирующей меры, в целях обеспечения недоступности информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы.

3.3.5.5. Коммутационное оборудование настраивается на разрешение доступа только для тех MAC адресов, которые успешно прошли аутентификацию.

3.3.5.6. Пользователи должны обладать минимальными необходимыми для исполнения должностных обязанностей правами доступа к файлам и каталогам АС ГБУ РО «ОКЦФП».

3.3.5.7. Максимальное разрешенное количество одновременно установленных сеансов связи не должно превышать 2.

3.3.5.8. Межсегментное взаимодействие должно осуществляться исключительно с применением средств межсетевого экранирования и обнаружения вторжений, при этом должно осуществляться управление информационными потоками при передаче информации между устройствами, включающее:

- фильтрацию информационных потоков в соответствии с установленными правилами управления потоками по совокупности критериев TCP пакетов;

- разрешение передачи информации в информационной системе только по заданному маршруту;
- изменение (перенаправление) маршрута передачи информации в необходимых случаях;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в необходимых случаях.

3.3.5.9. Должно обеспечиваться блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя 15 минут или по требованию пользователя, с необходимостью повторной аутентификации.

3.3.5.10. Конкретные права пользователей по доступу к защищаемым ресурсам, правила межсегментного (сетевого) доступа определяются Администратором ИБ и отражаются в *Матрице доступа (Приложение 4).*

3.3.5.11. Матрица доступа должна поддерживаться Администратором ИБ в актуальном состоянии. Допускается ведение матрицы доступа в электронной форме.

3.3.6. Действия до идентификации и аутентификации

3.3.6.1. До прохождения процедур идентификации и аутентификации пользователям АС ГБУ РО «ОКЦФП» запрещаются любые действия, не связанные со штатной технологией эксплуатации задач.

3.3.6.2. Администратору ИБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые исключительно в целях восстановления функционирования АС ГБУ РО «ОКЦФП» в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

3.3.6.3. Удаленный доступ в АС ГБУ РО «ОКЦФП» запрещен, за исключением доступа по защищенным каналам связи сети VPN.

3.4. Защита носителей информации

3.4.1. Общие положения

3.4.1.1. Носители защищаемой информации независимо от формы их представления (машинные носители, мобильные технические средства или носители на бумажной основе) подлежат учету. Система учета должна однозначно определять сотрудника, обладающего в текущий момент времени носителем защищаемой информацией и несущего за него ответственность.

3.4.1.2. Ответственный сотрудник хранит носители защищаемой информации в недоступном для посторонних лиц месте (сейф, металлический шкаф и т.д.), исключающем несанкционированный доступ и пользование ими.

3.4.1.3. Оснащение подразделений защищенными хранилищами осуществляется по инициативе начальников структурных подразделений в которых обрабатывается защищаемая информация, путем подачи служебной записки в адрес ответственного за обеспечение ИБ.

3.4.1.4. Создаваемые документы, как в бумажном, так и в электронном виде, над которыми работа еще не закончена, должны храниться таким же образом, как и готовые.

3.4.1.5. Передача носителей защищаемой информации в пределах одной организации осуществляется только среди сотрудников, допущенных к ее обработке, в пределах их компетенций.

3.4.1.6. Работа с носителями защищаемой информации производится только ответственным сотрудником, только в рабочее время и только на своем рабочем месте.

3.4.1.7. Об утрате или недостаче документов, носителей информации, ключей от помещений, хранилищ, сейфов, металлических шкафов, личных печатей, а также о причинах и условиях возможной утечки защищаемой информации сотрудник обязан немедленно сообщить ответственному за обеспечение ИБ.

3.4.2. Мобильные технические средства

3.4.2.1. В качестве мобильных технических средств (далее, МТС) рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

3.4.2.2. Учет МТС в АС ГБУ РО «ОКЦФП» осуществляет Администратор ИБ в *Журнале учета мобильных технических средств и носителей информации(МТС) (Приложение 5)*.

3.4.2.3. При нарушениях функционирования, поломке МТС они подлежат передаче Администратору ИБ.

3.4.2.4. На каждом рабочем месте, предназначенном для работы с МТС производится контроль использования интерфейсов ввода (вывода) с применением средств защиты информации. Средства защиты информации настраиваются на разрешение использования конкретного МТС на конкретном рабочем месте, а использование любых других МТС запрещается. Попытки использования интерфейсов ввода (вывода) как успешные, так и не успешные регистрируются в журнале средств защиты информации.

3.4.2.5. На серверном оборудовании, Администратором ИБ, обеспечивается дополнительная защита от несанкционированного использования портов ввода/вывода при помощи их опечатывания или отключения путем применения соответствующих настроек базовой системы ввода-вывода.

3.4.2.6. На МТС, предназначенных для взаимодействия с внешними системами и которые, следовательно, могут быть перемещены за пределы контролируемой зоны проставляется соответствующая отметка (маркер). Вынос МТС, не предназначенных для взаимодействия с внешними системами за пределы контролируемой зоны запрещен.

3.4.2.7. Передача МТС между сотрудниками осуществляется путем сдачи/выдачи носителя защищаемой информации Администратору ИБ под роспись.

3.4.3. Носители информации на бумажной основе (защищаемые документы)

3.4.3.1. Учет защищаемых документов может производится на листах описи документов хранящихся в папках-регистраторах с соответствующими пояснительными надписями (например «Списки», «Реестры» и т.п).

3.4.3.2. Папки-регистраторы учитываются в журналах учета дел в соответствующем подразделении.

3.4.3.3. Необходимо обособлять друг от друга документы, содержащие открытую информацию, документы для служебного пользования, ПДн, а также ПДн, различающиеся по целям их обработки.

3.4.3.4. Операции копирования и сканирования документов, содержащих ПДн, допускаются только с разрешения руководителя подразделения, с внесением соответствующей записи *в Журнал регистрации копировально-множительных работ (Приложение 6)* с указанием количества сделанных копий. Данный журнал должен быть расположен рядом с копировально-множительным устройством. Работа с копиями производиться так же, как и с оригиналом. Запрещается оставлять оригиналы и копии документов в копировальных аппаратах.

3.5. Уничтожение информации и обезличивание ПДн

3.5.1. Уничтожение информации

3.5.1.1. Уничтожение (стирание) информации на машинных носителях производится в обязательном порядке в следующих случаях:

- при их передаче между пользователями, в сторонние организации для ремонта или утилизации;
- перед подключением новых устройств, после их приобретения или после возвращения из ремонта;
- при первичном подключении после использовании в иных информационных системах.

3.5.1.2. В ходе мероприятий по анализу защищенности, Администратором ИБ осуществляется контроль уничтожения (стирания) информации.

3.5.1.3. При уничтожении защищаемой информации составляется *Акт об уничтожении защищаемой информации (Приложение 7)*, в котором указывается перечень уничтожаемых документов, файлов, носителей и т.д. Акт составляется комиссией сформированной из ответственного за обеспечение ИБ, Администратора ИБ и сотрудника обрабатывающего эти данные. В акте все члены комиссии подписями подтверждают уничтожение защищаемой информации.

3.5.1.4. Уничтожение документов производится любым способом, в результате которого документ приходит в состояние, когда его невозможно даже частично восстановить (сжигание, измельчение специальными механическими устройствами и т.д).

3.5.1.5. Уничтожение данных с носителей информации производится путем их затирания не менее чем в 1 проход случайной последовательностью, с использованием программных средств гарантированного уничтожения данных в составе сертифицированных средств защиты информации. Допускается физическое уничтожение носителей информации.

3.5.1.6. Акты об уничтожении мобильных технических средств и данных, хранятся у ответственного за обеспечение ИБ.

3.5.2. Обезличивание ПДн

3.5.2.1. Обезличивание персональных данных производится в соответствии с Приказом Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных», в тех случаях когда данный метод защиты персональных данных является наиболее приемлемым с учетом принятого технологического процесса.

3.6. Антивирусная защита

3.6.1. Общие положения

3.6.1.1. Для организации антивирусной защиты используются сертифицированные ФСТЭК России лицензионные антивирусные средства.

3.6.1.2. Средства антивирусной защиты устанавливаются на всех ТС оснащённых накопителем информации и настраиваются Администратором ИБ на работу по единому и согласованному сценарию.

3.6.1.3. Антивирусный контроль образов операционных систем размещаемых в оперативной памяти устройств, предназначенных для сетевой загрузки на бездисковые терминалы и мобильные USB загрузочные устройства осуществляется в местах их постоянного хранения - серверах управления сетевой загрузкой.

3.6.1.4. Обновление антивирусных средств должно производиться из официальных источников, ежедневно в автоматическом режиме. Для обновления антивирусных баз может использоваться соединение с официальным сервером обновлений или соединение со специально созданным каталогом обновлений на локальном сервере.

3.6.1.5. Администратор ИБ обязан проводить дополнительный антивирусный контроль в отношении любых входящих и исходящих данных поступающих в систему независимо от канала их передачи.

3.6.1.6. Необходимо проводить контроль подозрительного ПО в изолированной, тестовой среде (песочница). Наибольшую опасность могут представлять файлы с исполняемыми расширениями (часто вредоносное ПО, включая вирусы-крипторы, могут являться обычными скриптами выполняющими последовательности рутинных операций и обладают «чистым» кодом с точки зрения антивируса. Существенное значение для нейтрализации угроз вредоносного ПО имеет запрет на вхождение в периметр безопасности исполняемых файлов, а также осведомленность пользователей о недопустимости их запуска без предварительного контроля Администратором ИБ).

3.6.1.7. Администратором ИБ должны быть произведены настройки направленные на проведение антивирусного контроля системных областей в автоматическом режиме при загрузке всех узлов АС ГБУ РО «ОКЦФП».

3.6.1.8. Пользователи АС ГБУ РО «ОКЦФП» не должны обладать возможностью отключения, изменения настроек или временной остановки антивирусного средства.

3.6.1.9. Пользователи обязаны передать любое незапрашиваемое или подозрительное сообщение Администратору ИБ для комплексного контроля. Администратор ИБ должен периодически информировать пользователей об этой обязанности.

3.6.1.10. Ответственному за обеспечение ИБ необходимо проводить системную работу с пользователями направленную на повышение их осведомленности в области ЗИ. Эффективной мерой контроля при этом являются внезапные проверки на предмет соблюдения принятых в организации политик безопасности.

3.7. Обнаружение и предотвращение вторжений

3.7.1.1. В АС ГБУ РО «ОКЦФП» используются сертифицированные средства обнаружения и предотвращения вторжений. Обнаружение вторжений осуществляется на уровне межсегментного взаимодействия.

3.7.1.2. Право по управлению (администрированию) системой обнаружения вторжений предоставляется Администратору ИБ или уполномоченному лицу.

3.7.1.3. Обновление баз решающих правил системы обнаружения вторжений производится с официального ресурса в автоматическом режиме.

3.7.1.4. В целях минимизации ложных срабатываний системы обнаружения вторжений Администратором ИБ производится редактирование правил с учетом структурно-функциональных характеристик АС, с тем чтобы выявить аномальный трафик не присущий принятой информационной технологии, в частности должны обнаруживаться и блокироваться протоколы, используемые для скрытого управления вредоносным ПО или эксфильтрации, такие как ICMP, DNS и т.п. в полях данных пакетов которых содержатся не нормальные для данных протоколов данные по содержанию и размеру (например управляющие команды).

3.7.1.5. Администратором ИБ контролируется содержание (производится анализ) и работоспособность системы распознавания компьютерных атак (анализаторы), а также своевременность обновления баз решающих правил.

3.8. Обеспечение целостности и доступности

3.8.1. Общие положения

3.8.1.1. В АС ГБУ РО «ОКЦФП» применяются следующие способы резервного копирования и восстановления доступности:

- резервирование настроек программного обеспечения и оборудования (экспорт настроек);
- регулярное резервное копирование данных, включая образы виртуальных машин и образы контейнеров приложений;
- создание точек восстановления системы через механизм мгновенных снимков (снэпшоты);

- восстановление программы или драйвера путем переустановки, без восстановления системы полностью;
- восстановление или создание новой копии системы из полного образа системы с эталонных шаблонов.

3.8.1.2. К каждому сервису АС ГБУ РО «ОКЦФП», их программному обеспечению и оборудованию применяется экспорт настроек. При отсутствии такой функции, параметры настроек, параметры окон, панелей инструментов и панелей меню резервируются при помощи снимков экрана.

3.8.1.3. Резервные копии систем и данных могут хранится как в RAID массиве, так и на внешних учтенных носителях. В случае повышения вероятности аварий, Администратор ИБ должен организовать хранение резервных копий в отдельном помещении, оснащенном соответствующими системами вентиляции, кондиционирования и отопления.

3.8.2. Резервирование системной информации

3.8.2.1. Планирование и реализацию работ по резервированию информации осуществляет Администратор ИБ.

3.8.2.2. Резервные копии файлов конфигурации описывающие настройки средств защиты информации и телекоммуникационного оборудования, включая правила маршрутизации между различными физическими и логическими (VLAN) сегментами имеют статус защищаемых электронных документов и хранятся соответствующим образом. Доступ к этим файлам имеет только Администратор ИБ.

3.8.2.3. Для каждого узла АС ГБУ РО «ОКЦФП» создается образ системы путем клонирования жесткого диска (физического или виртуального), включающий все необходимое программное обеспечение и настройки безопасности

3.8.3. Резервирование данных

3.8.3.1. Резервное копирование информационных ресурсов осуществляется по двухуровневой схеме ротации:

- полное резервное копирование информационных ресурсов выполняется в конце каждого месяца. Архив хранится в течение года и является архивом Уровня 1;
- инкрементальное резервное копирование информационных ресурсов выполняется в конце каждой недели (в пятницу или субботу). Архив хранится в течение календарного месяца и является архивом Уровня 2;

3.8.3.2. Администратор ИБ настраивает задания резервного копирования, путем настройки штатного планировщика задач операционных систем на автоматическое выполнение резервирования данных в соответствии с *«Планом резервного копирования информационных ресурсов» (Приложение 8).* Резервные копии при необходимости должны подвергаться архивированию путем сжатия, с использованием штатных утилит операционных систем. Система именования файлов резервных архивных копий должна соответствовать правилу именования: *backup-`date '+%d-%B-%Y'`.*

3.8.4. Контроль программного обеспечения и данных

3.8.4.1. Любое программное обеспечение планируемое к внедрению, проверяется Администратором ИБ на соответствие функционалу указанному в официальной документации, совместимости с имеющимися программно-аппаратными платформами, соответствие контрольных сумм дистрибутивов, публикуемым на официальных сайтах производителя.

3.8.4.2. Для контроля целостности файлов не подлежащих изменению, Администратором ИБ генерируются и сохраняются контрольные суммы указанных файлов.

3.8.4.3. Контроль целостности реализуется штатными средствами СЗИ от НСД или средствами операционных систем, с помощью которых вычисляются и сравниваются с эталоном контрольные суммы в целевых каталогах.

3.9. Защита помещений и технических средств

3.9.1. Общие положения

3.9.1.1. Помещения в которых размещаются компоненты АС ГБУ РО «ОКЦФП», серверные комнаты (стойки) и помещения, предназначенные для автоматизированной и неавтоматизированной обработки защищаемой информации, являются режимными объектами. Сотрудники ответственные за соблюдение мер защиты на режимных объектах определяются приказом руководителя ГБУ РО «ОКЦФП». Необходимо контролировать физический доступ ко всем техническим средствам и коммутирующему оборудованию АС ГБУ РО «ОКЦФП».

3.9.1.2. Доступ в режимные помещения в нерабочее время должен быть заблокирован дверью, закрытой на ключ. В рабочее время доступ в помещение контролируется ответственным сотрудником, находящимся в помещении. При отсутствии персонала, нахождение в режимном помещении посторонних лиц запрещается, а дверь должна быть закрыта на ключ.

3.9.1.3. Все работы по обслуживанию (ремонту) технических средств внешними организациями проводятся только под контролем Администратора ИБ.

3.9.1.4. В качестве меры контроля вскрытия технических средств, шкафов и помещений, должно использоваться их опечатывание.

3.9.1.5. Размещение дисплеев, клавиатур, принтеров должно исключать их несанкционированный просмотр посторонними лицами и посетителями.

3.9.1.6. Размещение и режим эксплуатации устройств вывода аудиоинформации должны исключать несанкционированное прослушивание информации, в частности рабочие места предназначенные для оказания телемедицинских консультаций должны быть расположены в отдельных помещениях, а вывод аудио информации должен осуществляться в гарнитуру пользователя в случае невозможности исключения несанкционированного прослушивания информации организационными мерами.

3.9.1.7. Режимные помещения рекомендуется оснащать средствами охранной и пожарной сигнализации.

3.10. Защита информационной системы, систем связи и передачи данных

3.10.1. Защита информационной системы

3.10.1.1. Питание ключевых узлов АС ГБУ РО «ОКЦФП», включая серверы и активное оборудование необходимо осуществлять через источники бесперебойного питания.

3.10.1.2. Доступ к интерфейсам обновления BIOS (локальным, сетевым) запрещается.

3.10.1.3. В дополнение к мерам указанным в п.п. 3.3.5.8 в АС ГБУ РО «ОКЦФП» при использовании средств межсетевого экранирования. Администратором ИБ должны реализовываться и постоянно контролироваться на неизменность следующие параметры управления информационными потоками:

- запрещены все соединения кроме тех, которые разрешены и являются минимально необходимыми (белый список);
- установление соединений через сеть Интернет с серверами обновления антивирусных средств, системного и прикладного программного обеспечения разрешается только с использованием протокола https на время этого обновления, и блокируется после его окончания;
- сетевое взаимодействие АС ГБУ РО «ОКЦФП» с ЛВС ГБУ РО «ОКЦФП» разрешено, в объеме минимально необходимом и достаточном для функционирования АС ГБУ РО «ОКЦФП», при этом обеспечивается запрет доступа к защищаемой информации из ЛВС ГБУ РО «ОКЦФП».

3.10.2. Защита каналов связи

3.10.2.1. Для организации межсегментного взаимодействия в АС ГБУ РО «ОКЦФП» должны использоваться сертифицированные программные и программно-аппаратные комплексы шифрования.

3.11. Защита среды виртуализации и контейнеризации

3.11.1.1. Право установки и настройки среды виртуализации и контейнеризации предоставляется только Администратору ИБ.

3.11.1.2. Доступ к интерфейсу настроек среды виртуализации и контейнеризации должен осуществляться после прохождения процедур идентификации и аутентификации в соответствии с требованиям к этим подсистемам установленными настоящей Политикой.

3.11.1.3. Доступ к интерфейсу управления средой виртуализации и контейнеризации допускается только локальный.

3.11.1.4. Доступ к файлам конфигурации среды виртуализации и контейнеризации, разрешается только Администратору ИБ путем соответствующей настройки системы разграничения доступа.

3.11.1.5. Внутренние сети среды виртуализации и контейнеризации (виртуальные сети) должны изолировать группы сервисов по функциональной принадлежности. Каждый защищаемый

сегмент виртуализированной сети должен контролироваться подсистемой межсетевого экранирования.

3.11.1.6. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин и контейнеров должны выполняться все требования настоящей Политики.

3.11.1.7. Подсистема регистрации событий должна регистрировать все события среды виртуализации и контейнеризации, а также события внутри виртуальных машин и контейнеров в соответствии с требованиям к подсистеме регистрации событий установленными настоящей Политикой.

3.12. Защита мобильных рабочих мест

3.12.1. Общие положения

3.12.1.1. Использование технологий беспроводного доступа ограничено применением в АС ГБУ РО «ОКЦФП» стандартов связи для мобильных устройств (рабочих мест) на базе планшетов. Другие реализации технологий беспроводного доступа не допускаются.

3.12.1.2. В АС ГБУ РО «ОКЦФП» запрещено использование личных мобильных устройств (BYOD), а также устройств для которых не определен текущий владелец.

3.12.1.3. На мобильных устройствах должна отсутствовать возможность несанкционированной удаленной активации любых периферийных устройств ввода (вывода) информации, и коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы). Запрет несанкционированной удаленной активации должен осуществляться через физическое исключение такой возможности и (или) путем управления программным обеспечением.

3.12.1.4. Контроль несанкционированного использования модулей реализующих технологии передачи речи и видеоинформации достигается через запрет использования этих модулей на программном уровне.

3.12.1.5. Администратором ИБ должны быть реализованы механизмы сбора лог-файлов приложений используемых на мобильных устройствах и непрерывный аудит этих лог-файлов в целях выявления несанкционированных действий.

3.12.1.6. Администратором ИБ должны проводится выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации).

3.12.2. Идентификация и аутентификация

3.12.2.1. Экран мобильного устройства должен блокироваться с необходимостью ввода пароля или PIN-кода для разблокирования.

3.12.2.2. Пароли, вводимые на мобильном устройстве должны скрываться, для чего Администратором ИБ осуществляется соответствующая настройка программного обеспечения.

3.12.3. Управление доступом

3.12.3.1. Перечень сотрудников которым разрешено использовать мобильные технические средства определяется руководителем ГБУ РО «ОКЦФП».

3.12.3.2. Мобильные устройства разрешенные к использованию в АС ГБУ РО «ОКЦФП» подлежат учету, который осуществляет Администратор ИБ в *«Журнале учета мобильных технических средств и носителей информации» (Приложение 5)*. Выдача мобильных устройств производится сотруднику под роспись, после ознакомления с настоящей Политикой.

3.12.3.3. Пользователи мобильных устройств должны иметь доступ только к разрешенным web-ресурсам для взаимодействия посредством штатного web-браузера.

3.12.3.4. Доступ к функциям геолокации должен быть предоставлен только тем приложениям, которые используют данную функцию в целях навигации и определения местонахождения пропавшего устройства.

3.12.4. Ограничение программной среды

3.12.4.1. На всех мобильных устройствах Администратором ИБ отключается возможность установки приложений из неизвестных источников. Допускается установка приложения только из официальных источников по согласованию с Администратором ИБ.

3.12.4.2. Администратором ИБ формируются списки разрешенных к использованию приложений (белый список). При формировании белого списка ПО должны учитываться конфигурационные настройки приложений, которые часто запрашивают права значительно превосходящие функциональность приложений. Такое ПО относится к потенциально опасному и рассматривается как нежелательное к установке, требующее установки аналогичного ПО, с адекватными правами.

3.12.4.3. Процесс обновления ПО мобильного устройства должен производится не реже чем в раз месяц (при условии наличия соответствующих обновлений и соответствия требованиям формуляров используемых на них средств защиты). Процесс обновления должен выполняться Администратором ИБ для всех мобильных устройств.

3.12.5. Защита встроенных носителей информации

3.12.5.1. Защита встроенных носителей информации направлена на нейтрализацию угроз утечки информации в случаях уничтожения, отправки в ремонт, передачи другому лицу (в том числе и несанкционированной) или утилизации. Во всех перечисленных случаях информация подлежит гарантированному уничтожению (затиранию не менее чем в 1 проход), допускается использование функции «сброс к заводским установкам», при наличии подтверждения ее эффективности для затирания данных в ходе контроля защищенности.

3.12.5.2. Данные хранящиеся на носителях информации мобильных устройствах шифруются с использованием штатных средств мобильных устройств на пароле пользователя. Учитывая, что штатные утилиты шифрования не позволяют работать с SD-картами, хранение конфиденциальной информации на SD-картах запрещается.

3.12.5.3. Резервное копирование информации выполняется только Администратором ИБ. Резервные копии данных мобильных устройств являются конфиденциальной информацией.

3.12.5.4. На мобильных устройствах активируются функции защиты от хищений, которые позволяют обнаружить местонахождение устройства и/или произвести дистанционное затирание информации.

3.12.5.5. Требования по защите распространяются на все виды носителей информации мобильных устройств, как встроенные, так и съемные карты памяти и в целом соответствуют требованиям к защите носителей информации.

3.12.6. Антивирусная защита

3.12.6.1. Эффективность антивирусной защиты напрямую связана с соблюдением требований к ограничению программной среды.

3.12.6.2. Основными признаками указывающими на заражение вредоносным ПО являются совершение мобильным устройством действий без участия пользователя (например рассылка sms) или необъяснимо высокое потребление ресурсов мобильным устройством (батарея слишком быстро разряжается). При обнаружении вышеперечисленных признаков, равно как и о фактах утери или кражи мобильного устройства следует незамедлительно сообщать Администратору ИБ.

3.12.7. Контроль (анализ) защищенности информации

3.12.7.1. Администратором ИБ должен проводиться периодический контроль защищенности мобильных ТС в целях выявления уязвимостей программного обеспечения и тестирование этих уязвимостей в случае наличия публичного эксплойта.

3.12.7.2. Администратором ИБ должен проводится контроль эффективности затирания информации путем применения ПО для дистанционного затирания данных (защиты от вора), путем попыток ее восстановления в ходе контроля эффективности принятых мер защиты.

3.12.8. Защита мобильных устройств и систем передачи данных

3.12.8.1. На мобильных устройствах должны отсутствовать сервисы позволяющие произвести подключение к командному процессору операционной системы. Отладка по USB должна быть отключена.

3.12.8.2. На мобильных устройствах должна выполняться синхронизация со временем сети.

3.12.8.3. Использование внешних облачных сервисов для хранения данных запрещено.

3.12.8.4. При использовании мобильных устройств в АС ГБУ РО «ОКЦФП» рекомендуется задействовать технологическое решение уровня предприятия, которое централизует управление мобильными устройствами (mobile device management - MDM), в целях создания единой точки контроля устройств, единообразия управления конфигурацией и безопасностью мобильных устройств. Для целей централизованного управления должны использоваться исключительно защищенные каналы связи.

3.12.8.5. MDM предназначена для подключения распространенных мобильных платформ. Администратором ИБ, с помощью MDM выполняются:

- настройка правил аутентификации согласно требованиям к парольной защите настоящей Политики;
- настройка белого и черного списка программного обеспечения;
- обновление конфигурации мобильного устройства и поддержка неизменности конфигурации мобильных устройств;
- настройка правил сетевого взаимодействия;
- мониторинг журналов событий мобильного устройств в целях обнаружения взломанных (jailbreak или root) мобильных устройств.

3.12.8.6. Администратором ИБ должны документироваться аномалии, такие как несанкционированные изменения конфигурации для мобильных устройств.

3.13. Управление конфигурацией

3.13.1. Общие положения

3.13.1.1. Под управлением конфигурацией понимается формализованная процедура поддержания в неизменном виде конфигурации АС ГБУ РО «ОКЦФП» и системы защиты информации.

3.13.1.2. Под изменением конфигурации понимается внесение ранее не оговоренных изменений в состав программных и аппаратных средств АС ГБУ РО «ОКЦФП». Таким образом, обновление версий (замена) ранее учтенных программных и технических средств не является изменением конфигурации.

3.13.1.3. Все изменения в конфигурации технических и программных средств на объекте информатизации должны производиться в строгом соответствии с эксплуатационной документацией на них. Необходимо проводить предварительные стендовые испытания программного обеспечения и технических средств перед вводом в эксплуатацию.

3.13.2. Технический паспорт

3.13.2.1. Базовая конфигурация (профиль) АС ГБУ РО «ОКЦФП» отражается в «Техническом паспорте».

3.13.2.2. Технической паспорт разрабатывается Администратором ИБ и описывает базовую конфигурацию (профиль) АС ГБУ РО «ОКЦФП», состава установленных программных средств и системы защиты информации (структуру системы защиты информации, состав, места установки средств защиты информации, программного обеспечения и технических средств).

3.13.2.3. Перечень разрешенного к эксплуатации программного обеспечения разрабатывается Администратором ИБ с учетом минимально необходимого набора ПО необходимого для реализации заданной информационной технологии.

3.13.2.4. Все изменения в конфигурации отражаются Администратором ИБ в *Техническом паспорте.*

3.13.3. Процедура внесения изменений в конфигурацию

3.13.3.1. Внесение изменений в конфигурацию производятся Администратором ИБ, на основании служебной записки ответственного за обеспечение ИБ. Ответственным за обеспечение ИБ могут быть приняты следующие решения:

- установка, замена устройства (узла, блока);
- изъятие устройства (узла, блока);
- установка (развертывание) новых программных средств, необходимых для решения определенной задачи (добавление новой возможности решения задачи);
- удаление программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи).

3.13.3.2. Изъятие средств вычислительной техники содержащей носители информации на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор ИБ произведет удаление защищаемых данных или носителей информации, на основании служебной записки ответственного за обеспечение ИБ.

3.13.3.3. Установка программного обеспечения производится Администратором ИБ с оригинальных дистрибутивов или их носителей (компакт дисков и т.п.), полученных установленным порядком из официальных источников. Для верификации дистрибутивов должно выполняться сравнение контрольных сумм полученных дистрибутивов с эталонными значениями контрольных сумм. Доступ к исходным файлам и дистрибутивам должен быть предоставлен только Администратору ИБ.

3.13.3.4. При изменении конфигурации Администратором ИБ производятся настройки всех подсистем защиты информации в соответствии с требованиями настоящей Политики, проверяется работоспособность ПО и правильность настройки средств защиты. В ходе проверки производится контроль назначения прав доступа на системные файлы и каталоги, а также сканирование системы с помощью сканеров уязвимостей.

3.13.4. Контроль конфигурации

3.13.4.1. Администратором ИБ еженедельно осуществляется контроль конфигурации системы, путем автоматизированной генерации графической карты сети с указанием всех подключенных устройств. Для автоматизации данного процесса могут использоваться сканеры сетей, входящие в состав сертифицированных средств анализа защищенности.

3.13.4.2. Администратором ИБ ежедневно осуществляется контроль конфигурации системы защиты информации, путем сканирования внешних интерфейсов пограничного оборудования и интерфейсов коммутационного оборудования. Для автоматизации данного процесса могут использоваться сканеры сетей, входящие в состав сертифицированных средств анализа защищенности.

3.14. Ограничение программной среды

3.14.1. Общие положения

3.14.1.1. Любые изменения в состав аппаратного или программного обеспечения вносятся только на основании «Технического паспорта», перечня разрешенного к эксплуатации ПО (белый

список) и в целях устранения уязвимостей . В противном случае данные изменения считаются изменением конфигурации. Экстренное изменение конфигурации запрещается.

3.14.2. Плановое внесение изменений

3.14.2.1. Обновление (замена) программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ) производятся Администратором ИБ на основании служебной записки ответственного за обеспечение ИБ. Заявка на обновление (замену) программных средств может подаваться пользователями в любой форме на имя ответственного за обеспечение ИБ.

3.14.2.2. Обновление системного и прикладного ПО на серверах и рабочих станциях, прошивок СВТ производятся Администратором ИБ на основании информации о выявленных уязвимостях, при этом критические обновления (устраняющие уязвимости с высоким уровнем риска) внедряются в течение 24 часов после выхода патча, а стандартные обновления (снижающие средний или низкий риск) планируются в ежемесячный оконный период обслуживания.

3.14.3. Экстренное внесение изменений

3.14.3.1. В исключительных случаях (сбой, не позволяющий продолжить работу), требующих безотлагательного обновления или переустановки ПО, допускается экстренное внесение изменений без участия Администратора ИБ. В данной ситуации пользователь инициирует экстренное внесение изменений путем обращения к ответственному за обеспечение ИБ.

3.14.3.2. Факт экстренного внесения изменений фиксируется актом за подписями пользователя и ответственного за обеспечение ИБ. В акте указывается причина модификации, перечисляются программы подвергшиеся изменению, и указывается лицо, проводившее изменения.

3.14.3.3. В течение следующего дня после составления акта, Администратор ИБ совместно с ответственным за обеспечение ИБ при участии пользователя выясняют причины и состав проведенных экстренных изменений и принимается решение о сохранении или удалении произведенных изменений.

3.14.3.4. Для реализации возможности экстренного изменения, Администратором ИБ создается резервная учетная запись с правами администратора. Реквизиты доступа к данной учетной записи хранятся у руководителя ГБУ РО «ОКЦФП» и ответственного за обеспечение ИБ. Требования к защите данной учетной записи аналогичны требованиям, предъявляемым к учетным записям группы администраторов.

3.14.4. Установка программного обеспечения

3.14.4.1. Администратором ИБ осуществляется описание этапов процесса установки программного обеспечения, при этом фиксируются параметры настроек установщика. Описание может осуществляться в свободной форме, в виде руководств, допускается также осуществлять снимки экрана на разных этапах установки. Созданные таким образом описания должны позволять задокументировать процесс установки того или иного программного обеспечения в виде инструкции.

3.14.4.2. Установке подлежат только те компоненты, которые необходимы для реализации информационной технологии.

3.14.4.3. Для каждого сценария (типа операционной системы) установки программного обеспечения Администратором ИБ создается стенд (например с использованием технологии виртуализации), на который первоначально устанавливается программное обеспечение в различных вариантах конфигурации, в целях выбора оптимальной конфигурации.

3.14.5. Управление запуском программного обеспечения

3.14.5.1. Администратором ИБ составляется перечень (список) программного обеспечения предоставляющей серверные функции, запускаемого автоматически при загрузке операционной системы конкретного узла сети. Необходимо поддерживать в актуальном состоянии информацию о том какой узел предоставляет тот или иной сетевой сервис и для каких целей.

3.14.5.2. Сетевые сервисы должны настраиваться на функционирование в изолированной части файловой системы, который позволяет задать для определенного процесса (и его потомков) каталог, который они будут рассматривать как корневой, тем самым ограничивая для них область видимости иерархии файловой системы отдельной ветвью.

3.14.5.3. Сетевые сервисы не должны функционировать с правами администратора. Для запуска служб должны использоваться специальные учетные записи операционных систем.

3.14.5.4. Администратором ИБ автоматизируется процесс сверки списка автоматически запускаемого ПО.

3.15. Анализ защищенности и управление уязвимостями

3.15.1. Общие положения

3.15.1.1. Целью анализа защищенности является анализ угроз безопасности информации в АС ГБУ РО «ОКЦФП».

3.15.1.2. В качестве средства анализа защищенности используется сертифицированные ФСТЭК России средства анализа защищенности.

3.15.1.3. Запрещается проводить анализ защищенности средствами, не обновленными на дату такого анализа в части эксплуатации уязвимостей.

3.15.1.4. Полный плановый анализ защищенности осуществляется Администратором ИБ ежемесячно. Анализ проводится как в пределах сегментов, так и со стороны смежных сегментов АС ГБУ РО «ОКЦФП» (логическая граница), а так же со стороны ССОП (физическая граница). В ходе анализа осуществляется:

- контроль актуальности обновлений безопасности операционных систем и приложений;
- контроль актуальности антивирусных баз;
- контроль топологии и инвентаризация ресурсов сети, сетевых портов и связанных с ними сетевых сервисов, выявление неизвестных сетевых узлов;

- контроль уязвимостей операционных систем и прикладных программ, по актуальным базам уязвимостей;
- контроль защищенности в тестовой среде с использованием соответствующих эксплоитов (например: https://www.exploit-db.com/) для локальных уязвимостей (например, связанных с повышением привилегий);
- контроль загруженности систем и выявление приложений потребляющих и удерживающих значительные вычислительные ресурсы;
- контроль отравления кэша маршрутных таблиц;
- контроль исполнения требований парольной политики, локальный и сетевой аудит паролей (для коммутационного оборудования, сервисов HTTP, SMTP, POP, FTP, SSH и др.);
- контроль неизменности настроек средств защиты информации, в первую очередь обеспечивающих сетевую безопасность (правила межсетевого экранирования);
- контроль установленного программного обеспечения и оценка его соответствия перечню разрешенного к эксплуатации ПО;
- контроль учтенных записей (актуальность списка блокированных и неблокированных пользователей, принадлежность к группам и т.д);
- контроль прав доступа к каталогам хранящим файлы-идентификаторы сессий, файлам отчетов об ошибках, регистрации событий, конфигурационным файлам, интерфейсам доступа к настройкам всего без исключения сетевого оборудования;
- контроль использования мобильных технических средств и попыток несанкционированного их подключения;
- контроль наличия на рабочих станциях функционирующих модулей подключения к беспроводным сетям и возможности подключения мобильных устройств передачи данных.

3.15.1.5. По результатам анализа защищенности Администратором ИБ создается отчет на имя ответственного за обеспечение ИБ, с кратким описанием результатов по каждому из указанных пунктов.

3.15.1.6. При выявлении новых уязвимостей, Администратором ИБ пересматривается модель актуальных угроз безопасности информации.

3.15.1.7. Установка обновлений безопасности или изменение настроек в целях устранения уязвимостей производится Администратором ИБ незамедлительно после опубликования информации об уязвимости в соответствующих источниках (например: https://bdu.fstec.ru/vul). Перед установкой обновления безопасности Администратором ИБ проводится анализ информации о возникающих в связи с этим обновлением новых уязвимостях и ошибках. Необходимо проводить предварительное тестирование результатов установки обновлений.

3.15.1.8. Установка обновлений безопасности производится в строгом соответствии с Методическими документами ФСТЭК России 28 октября 2022 г. «Методика тестирования обновлений безопасности программных, программно-аппаратных средств» и «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств»,

с учетом критериев для принятия решения по обновлению критичного ПО, не относящегося к open-source опубликованных НКЦКИ 15 апреля 2022 г. № ALRT-20220415.1

3.15.1.9. Процесс управления уязвимостями выстраивается на основе Методического документа ФСТЭК России от 17 мая 2023 г. «Руководство по организации процесса управления уязвимостями в органе (организации)».

3.15.1.10. Рекомендуется применение средств автоматизации управления уязвимостями в целях обеспечения непрерывности этой деятельности, в связи с существенными рисками которые порождают уязвимости.

3.15.1.11. Внеплановый анализ защищенности производится в рамках подсистемы управления инцидентами.

3.16. Управление событиями и инцидентами безопасности

3.16.1. Общие положения

3.16.1.1. Под событием информационной безопасности понимается идентифицированный случай, указывающий на возможное нарушение системы защиты информации или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности.

3.16.1.2. Под инцидентом информационной безопасности понимается единичное событие (включая компьютерные атаки) или ряд нежелательных и непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации системы защиты.

3.16.1.3. Система управления событиями и инцидентами включает в себя:

- сбор сведений о событиях и инцидентах;
- регистрацию событий и инцидентов;
- реагирование на события и инциденты;

3.16.2. Сбор сведений о событиях и инцидентах

3.16.2.1. Сбор данных о событиях и инцидентах производится в автоматическом режиме, централизованно и непрерывно, механизмами регистрации событий. Срок хранения журналов событий безопасности не менее трех месяцев

3.16.2.2. В информационной системе подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в АС ГБУ РО «ОКЦФП» и загрузки (останова) операционных систем;
- подключение мобильных технических средств и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа;
- все действия от имени привилегированных учетных записей (администраторов), с сохранением полнотекстовой записи привилегированных команд (команд, управляющих системными функциями);
- передача видео и аудио информации;
- попытки изменения привилегий учетных записей.

3.16.2.3. Состав и содержание информации о событиях безопасности должен обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности. Таким образом все события должны содержать:

- дату и время события (начала и окончания) события;
- результат события (успешно или неуспешно);
- идентификатор субъекта инициировавшего событие;
- реквизиты задействованных в событии объектов (наименования и пути программ и аппаратных компонентов, их номера и другие реквизиты).

3.16.2.4. Доступ пользователей к системе сбора данных о событиях и инцидентах запрещается.

3.16.2.5. Сбор событий осуществляется со всех узлов АС ГБУ РО «ОКЦФП». Основными источниками событий являются журналы:

- регистрации событий операционных систем серверов и рабочих станций;
- регистрации событий всех подсистем безопасности;
- регистрации событий приложений конечного пользователя;
- не журнальные источники событий безопасности (сообщения пользователей, партнеров, контрагентов и т.п).

3.16.2.6. Дополнительно, в ручном или автоматизированном режиме, Администратором ИБ осуществляется сбор событий с коммутационного оборудования АС ГБУ РО «ОКЦФП».

3.16.2.7. Из системы сбора, путем применения фильтров, исключаются обычные, повторяющиеся для заданных условий функционирования, события (шум). Перед исключением события из системы сбора Администратор ИБ предварительно убеждается, что оно не представляет угрозы. Рекомендуется внедрение и использование SIEM (Security information and event management).

3.16.3. <u>Регистрация инцидента</u>

3.16.3.1. Администратором ИБ в ходе анализа событий делается вывод о возможности наступления инцидента (выявление инцидента), при наличии следующих признаков:

- сообщение об инциденте поступают одновременно из нескольких источников (пользователи, журнальные файлы);
- система сбора событий сигнализирует о множественном повторяющемся событии (например множественные неудачные попытки авторизации);
- средства защиты информации выдают ошибку запуска или функционирования;
- пользователи сообщают об уведомлении антивирусной программы;
- пользователи сообщают о поступлении незапрашиваемых сообщений;
- пользователи сообщают о нетипичном поведении прикладных программ (например файл не открывается приложением);
- пользователи сообщают о крайне низкой скорости работы приложения или сети;
- пользователи сообщают о предупреждениях проверки подлинности сертификата сервера;
- пользователи или администратор фиксируют наличие файлов с нечитабельными названиями;
- фиксируется подключение устройства с неизвестным IP/MAC-адресом;
- администратор фиксирует резкое увеличение сетевого трафика, и.т.д.

3.16.3.2. Для обеспечения достоверности сведений о событиях и инцидентах, используется единый сервер синхронизации времени для всех узлов АС ГБУ РО «ОКЦФП».

3.16.4. Реагирование на события и инциденты

3.16.4.1. Процедура реагирования на события и инциденты информационной безопасности состоит из нескольких фаз:

- обучение пользователей в части обнаружения инцидентов;
- сбора необходимого инструментария, для проведения анализа инцидента;
- реализация процессного подхода к управлению инцидентами ;

3.16.4.2. Обучение персонала производится на этапе допуска пользователей к автоматизированной обработке данных, в ходе инструктажа, Администратором ИБ. Пользователь обязан сообщать о любом событии безопасности или инциденте, произошедшем на рабочем месте.

3.16.4.3. Первоочередные меры противодействия инцидентам включают в себя:

- приостановку обработки информации или мониторинг ситуации;
- устранение причин инцидента.

3.16.4.4. Устранение причин и последствий инцидента производятся Администратором ИБ любыми доступными методами. Процедуры устранения причин инцидента применяются отдельно для каждого конкретного инцидента и зависят от его типа.

3.16.4.5. Необходимый инструментарий для проведения расследования инцидента содержит:

- открытый или анонимный канал связи для сообщений о подозрительных действиях;
- испытательные стенды для анализа возможного развития инцидента;
- программное обеспечение для анализа защищенности, включающее снифферы и анализаторы протоколов для анализа сетевого трафика;
- средства восстановления информации с дисковых систем.

3.16.4.6. Расследование инцидента производится путем реконструкции действий до и после произошедшего события или инцидента. В ходе анализа изучаются записи всех журналов, для получения полной картины произошедшего. Анализ событий производится путем выдвижения предположения о том или ином событии безопасности и последующем исследовании журналов, чтобы подтвердить или опровергнуть это предположение. Предположения соотносятся с вероятными нарушителями и актуальными угрозами безопасности информации для АС ГБУ РО «ОКЦФП».

3.16.4.7. Подлежат хранению события, зарегистрированные как минимум за последние три месяца.

3.16.4.8. Для анализа событий и инцидентов руководством ГБУ РО «ОКЦФП» создается группа, состоящая из:

- руководителя группы – ответственного за обеспечение ИБ ;
- технического специалиста – Администратора ИБ и (или) сторонних привлекаемых специалистов;
- участников инцидента – пользователей (при необходимости).

3.16.4.9. В процессе анализа изучаются:

- состояния портов серверных сервисов;
- события на наиболее критичных устройствах о работе операционных систем, приложений, протоколов, систем межсетевого экранирования, антивирусов;
- журналы активности приложений;
- информация доступная в сети Интернет о наступивших событиях, их значениях и последствиях.

3.16.4.10. Документирование результатов реагирования на инцидент производится в целях сбора свидетельств злонамеренных действий и оценки остаточных рисков. Документированию подлежат все факты и доказательства злонамеренного воздействия, в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007.

3.16.4.11. По результатам расследования инцидента разрабатываются и включаются в настоящую Политику меры по противодействию инцидентам.

3.16.4.12. Документированные результаты реагирования на инцидент хранятся у ответственного за обеспечение ИБ.

3.16.4.13. В ГБУ РО «ОКЦФП» разрабатывается План мероприятий, реализуемых при установлении в отношении объектов критической информационной инфраструктуры проведения целевых компьютерных атак, устанавливающий различные уровни их опасности.

4. ВЫВОД ИЗ ЭКСПЛУАТАЦИИ

4.1.1. Вывод из эксплуатации автоматизированной системы или окончание обработки защищаемой информации осуществляется на основании приказа, после принятия соответствующего решения руководством ГБУ РО «ОКЦФП».

4.1.2. Вывод из эксплуатации системы защиты информации АС ГБУ РО «ОКЦФП» осуществляется путем деинсталляции и/или демонтажа средств защиты информации Администратором ИБ в соответствии с эксплуатационной документацией на эти средства.

4.1.3. При необходимости дальнейшего использования информации в деятельности ГБУ РО «ОКЦФП» осуществляется архивирование информации на учтенный съемный машинный носитель информации, и передача указанного носителя на хранение руководителю ГБУ РО «ОКЦФП».

4.1.4. При необходимости передачи компонентов информационной системы в другие подразделения (другому пользователю) или в сторонние организации для ремонта, технического обслуживания осуществляется уничтожение (стирание) данных и остаточной информации с мобильных технических средств, в соответствии с требованиями п. 3.5 настоящей Политики.

4.1.5. При выводе из эксплуатации мобильных технических средств, на которых осуществлялись хранение и обработка информации, осуществляется уничтожение (стирание) данных и остаточной информации с мобильных технических средств, в соответствии с требованиями п. 3.5 настоящей Политики или физическое уничтожение этих средств.

4.1.6. Факт вывода из эксплуатации системы защиты информации АС ГБУ РО «ОКЦФП» путем деинсталляции и/или демонтажа средств защиты информации оформляется соответствующим актом. Акт составляется комиссией сформированной из ответственного за обеспечение ИБ, Администратора ИБ и утверждается руководителем организации.

5. ВНУТРЕННИЙ КОНТРОЛЬ И АУДИТ

5.1. Общие положения

5.1.1. Под внутренним контролем понимаются мероприятия, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных и оценку текущих недостатков системы защиты информации и технологического процесса обработки информации в АС ГБУ РО «ОКЦФП» и принятии оперативных решений о способе их устранения.

5.1.2. Под внутренним аудитом понимаются мероприятия, направленные на анализ системных недостатков системы защиты информации и технологического процесса обработки информации в АС ГБУ РО «ОКЦФП» и принятии новых технологических решений, способствующих повышению эффективности обработки и защиты информации.

5.1.3. В целях выявления и предотвращения нарушений законодательства Российской Федерации, в АС ГБУ РО «ОКЦФП» производятся внутренний контроль и аудит обработки ПДн. Для осуществления контрольных мероприятий приказом руководителя ГБУ РО «ОКЦФП» создается комиссия.

5.2. Порядок проведения внутреннего контроля

5.2.1. Плановый внутренний контроль проводится ежеквартально.

5.2.2. Внеплановый внутренний контроль проводится в случае выявления фактов несоблюдения требований действующего законодательства и (или) в случае возникновении инцидентов безопасности, и осуществляется в рамках реагирования на события и инциденты безопасности.

5.2.3. Внутренний контроль проводится по следующим направлениям:
- соблюдение правил безопасной обработки защищаемой информации при автоматизированной обработке;
- соблюдение правил безопасной обработки защищаемой информации при обработке без использования средств автоматизации.

5.2.4. По результатам внутреннего контроля ответственным за обеспечение ИБ принимаются решения об оперативном устранении выявленных недостатков.

5.3. Порядок проведения внутреннего аудита

5.3.1. В целях совершенствования системы обработки и защиты информации, проводится ежегодный плановый внутренний аудит по следующим направлениям:
- совершенствование правил безопасной обработки защищаемой информации при автоматизированной обработке;
- совершенствование правил безопасной обработки защищаемой информации при обработке без использования средств автоматизации.

5.3.2. По результатам внутреннего аудита, руководством ГБУ РО «ОКЦФП» могут приниматься решения о пересмотре действующей локальной нормативной базы, а также об изменениях конфигурации или модернизации АС ГБУ РО «ОКЦФП».

6. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

6.1. Общие положения

6.1.1. Организацию работ по защите информации производит ответственный за обеспечение ИБ.

6.1.2. При проведении проектных работ необходимо предусмотреть ответственность поставщика в соответствующем договоре и производить экспертную оценку проектной документации на предмет включения в проект не достоверно испытанных компонентов и наличия системной избыточности.

6.1.3. Все работы в АС ГБУ РО «ОКЦФП» выполняются под контролем Администратора ИБ. Работы должны выполняться в строгом соответствии с проектной (эксплуатационной) документацией.

6.1.4. Экспертиза проектной документации должна включать в себя анализ публикуемых в интернет отчетов об ошибках возникших в сходных условиях внедрения.

6.1.5. При планировании работ, в качестве коммутирующего оборудования следует выбирать управляемые коммутаторы с поддержкой стандартов сетевой аутентификации 802.1X и встроенными механизмами защиты от различных видов спуфинга и паразитного DHCP трафика (DHCP-snooping) и задействовать указанный защитный функционал в ходе внедрения.

6.1.6. При планировании строительных или ремонтных работ в серверных помещениях, следует учитывать требования Инструкции по проектированию зданий и помещений для электронно-вычислительных машин (СН 512-78).

6.1.7. При составлении договора оказания облачных услуг необходимо учитывать угрозы в соответствии с банком данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru/threat) и риски связанные с облачными услугами, а также предусмотреть компенсацию ущерба поставщиком облачных услуг в соответствующем договоре при недобросовестном или непрофессиональном исполнении обязательств.

6.2. Регламент работ внешних подрядчиков

6.2.1. Для выполнения работ по внедрению, сопровождению, обслуживанию СВТ и иного технологического оборудования могут привлекаться сторонние организации. При этом все работы по обслуживанию и ремонту СВТ и технологического оборудования должны быть предварительно согласованы с ответственным за обеспечение ИБ. Ответственным за обеспечение ИБ на имя руководителя оформляется служебный документ с перечнем задач, объёмом работ и сроками исполнения. Представители подрядчика допускаются к оборудованию только при наличии паспорта сотрудника, действующего договора на оказание услуг и одноразового пропуска, зарегистрированного в журнале пропускного режима (при наличии).

6.2.2. Перед началом работ Администратор ИБ совместно с представителем подрядчика проводят осмотр оборудования, отмечая его текущее состояние и наличие защитных средств (замки, пломбы, ярлыки). В процессе работ подрядчик обязан соблюдать требования по неразглашению и не менять конфигурацию систем без предварительного уведомления Администратора ИБ. Все манипуляции с аппаратной частью и подключениями к иным сетям осуществляются под контролем Администратора ИБ.

6.2.3. При необходимости демонтажа накопителей информации или модулей оперативной памяти сохранность данных обеспечивается созданием резервных копий с контролем целостности. Информация на основных накопителях подлежит гарантированному уничтожению путем затирания до передачи оборудования подрядчику. Любые снятые

компоненты маркируются и упаковываются в заводскую тару или иные контейнеры. После завершения ремонта производится верификация серийных номеров модулей.

6.2.4. По окончании сервисного обслуживания подрядчик передаёт полный отчёт о проделанных работах, перечень заменённых компонентов и подтверждение соответствия настроек первоначальным параметрам. Администратор ИБ проверяет работоспособность оборудования, выполняет тестовые процедуры и фиксирует результаты в соответствующем Акте. Акт подписывается представителями подрядчика и ГБУ РО «ОКЦФП», копии документа хранятся у ответственного за обеспечение ИБ не менее трёх лет.

6.2.5. Для выполнения работ по разработке, внедрению, сопровождению, обслуживанию средств системы защиты информации могут привлекаться сторонние специализированные организации на условиях настоящего раздела. Кроме того в случае привлечения таких организаций необходимо соблюдение следующих требований к исполнителям работ:

- Для выполнения работ по установке, обслуживанию и ремонту средств криптографической защиты информации исполнитель должен иметь соответствующую лицензию ФСБ России;
- Для предоставления услуг связи исполнитель должен иметь лицензию на оказание услуг связи;
- Для проведения работ по установке, обслуживанию и ремонту средств защиты информации исполнитель должен иметь соответствующую лицензию ФСТЭК России.

6.3. Правила работы в сети Интернет

6.3.1. Сотрудники ГБУ РО «ОКЦФП» при доступе к ресурсам сети Интернет обязаны обеспечивать надёжную защиту персональных данных от несанкционированного доступа, утечки и вредоносного воздействия через глобальную сеть. Все пользователи обязаны строго соблюдать настоящие правила независимо от занимаемой должности и трудового статуса.

6.3.2. Доступ к Интернет-ресурсам для выполнения служебных задач предоставляется только к ресурсам белого списка отраслевых сервисов. Пароли и другие учётные данные этих сервисов не должны передаваться по незащищённым каналам или храниться в открытом виде на рабочих станциях.

6.3.3. Для предотвращения доступа к вредоносным, фишинговым и подозрительным ресурсам применяется централизованная система обнаружения вторжений и межсетевого экранирования. Пользователям запрещается отключать или обходить механизмы защиты. Администратором ИБ регулярно проводятся анализ и аудит логов с целью выявления аномалий и попыток несанкционированного доступа.

6.3.4. Передача конфиденциальной информации и персональных данных через публичные каналы Интернет возможна исключительно по защищённым каналам связи с с ипользованием сертифицированных СКЗИ (VPN, SSL/TLS) и только в рамках

утверждённого рабочего процесса. Использование сторонних облачных хранилищ и мессенджеров без соответствующей классификации данных и технического разрешения строго запрещено. Все загружаемые из Интернета файлы подлежат автоматическому сканированию антивирусными средствами до открытия пользователем.

6.3.5. Узлы с которых осуществляется доступ к сети Интернет должны быть настроены на автоматическое получение и установку обновлений операционных систем и антивирусных баз. Запрещено использование неавторизованного ПО, расширений браузеров или плагинов. Любые подозрительные уведомления о необходимости установки программного обеспечения через браузер требуют немедленного обращения к Администратору ИБ.

6.3.6. Пользователи обязаны проходить регулярное обучение по вопросам информационной безопасности и подтверждать своё ознакомление с актуальными версиями настоящей Политики. Нарушение правил влечёт дисциплинарную ответственность вплоть расторжения трудового договора. Ответственный за обеспечение ИБ осуществляет координацию мероприятий по повышению осведомлённости и готовности сотрудников к реагированию на инциденты, связанные с работой в сети Интернет.

Приложение 1 к Политике информационной безопасности государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

(ОБРАЗЕЦ)

ЛИСТ ОЗНАКОМЛЕНИЯ

с основными нормативно-правовыми актами и организационно-распорядительной документацией регулирующими порядок обработки и защиты информации в автоматизированной системе государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

№ п/п	Структурное подразделение	Должность	ФИО	Дата	Роспись об ознакомлении

Приложение 2 к Политике информационной безопасности государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

(ОБРАЗЕЦ)

СОГЛАШЕНИЕ
о соблюдении правил обеспечения информационной безопасности в автоматизированной системе государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

_____ в лице _____, действующего на основании ____, с одной стороны и

_____
(фамилия, имя, отчество)

_____
(должность)

именуемый (-ая) в дальнейшем РАБОТНИК, с другой стороны, заключили настоящее соглашение о том, что:

1. РАБОТНИКУ будет предоставлен доступ к объектам защиты ГБУ РО «ОКЦФП», в том числе к конфиденциальной информации, для выполнения РАБОТНИКОМ своих функциональных обязанностей, согласно занимаемой должности.
2. РАБОТНИК обязуется:
   - не раскрывать (не передавать) третьим лицам, данные о составе и структуре, методах и способах защиты информации, равно как и саму конфиденциальную информацию, полученную в ходе исполнения функциональных обязанностей (за исключением случаев, предусмотренных Федеральным законодательством);
   - соблюдать установленные правила обеспечения информационной безопасности направленные на обеспечение эффективного и бесперебойного функционирования автоматизированной системы ГБУ РО «ОКЦФП», а также на защиту персональных данных и иной конфиденциальной информации;
   - не нарушать своими действиями работоспособность системы защиты информации и технологический процесс в целом;
   - не извлекать из автоматизированной системы ГБУ РО «ОКЦФП» какие либо материалы, данные, документы и носители защищаемой информации.
3. РАБОТНИК подтверждает, что:
   - он (она) ознакомлен(-а) с правилами обеспечения информационной безопасности в автоматизированной системе ГБУ РО «ОКЦФП» отраженными в нормативно-правовых актах;
   - он (она) не имеет перед кем-либо никаких обязательств, которые входят в противоречие с настоящим СОГЛАШЕНИЕМ или ограничивают его (ее) деятельность в ГБУ РО «ОКЦФП».

Реквизиты сторон

Приложение 3 к Политике информационной безопасности государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

(ОБРАЗЕЦ)

СОГЛАШЕНИЕ
о соблюдении правил обеспечения информационной безопасности в автоматизированной системе государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

_____ в лице _____, действующего на основании _____, с одной стороны и _____, в лице _____, действующего на основании _____, с другой стороны, заключили настоящее соглашение о том, что:

При оказании услуг технической поддержки по договору №___ от _____, _____ будет предоставлен доступ к автоматизированной системе ГБУ РО «ОКЦФП».

_____ обязуется:

– не осуществлять попытки доступа к конфиденциальной информации, в том числе персональным данным, передачу конфиденциальной информации, в том числе персональных данных по незащищенным каналам связи;

– не раскрывать (не передавать) третьим лицам, данные о составе и структуре, методах и способах защиты информации, полученные в ходе исполнения своих обязательств (за исключением случаев, предусмотренных Федеральным законодательством);

– не нарушать своими действиями работоспособность автоматизированной системы ГБУ РО «ОКЦФП» и ее системы защиты информации;

– не извлекать из автоматизированной системы ГБУ РО «ОКЦФП» какие либо материалы, данные, документы и носители защищаемой информации.

Подписанием настоящего соглашения _____ выражает согласие со всеми требованиями защиты информации в автоматизированной системе государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии».

Реквизиты сторон

Приложение 4 к Политике информационной безопасности государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

(ОБРАЗЕЦ)

МАТРИЦА ДОСТУПА

Субъект доступа **Объект доступа**		ФИО	ФИО	ФИО	ФИО	ФИО	ФИО
Наименование	**Идентификатор**						
Средства криптографической защиты информации	Модель Заводской номер						
Коммутационное оборудование	Модель Заводской номер						
Используемые информационной системой каналы (линии) связи, включая кабельные системы	-						
Информация ограниченного доступа, в том числе врачебная тайна и персональные данные - защищаемая информация	Личный каталог пользователя						
Информация, о составе и структуре системы защиты информации, а также сведения относящиеся к эксплуатации системы защиты информации включая ключевую, парольную и аутентифицирующую информацию - защищаемая информация	Личный каталог Администратора ИБ						
Документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, включая документацию на средства защиты информации и на технические и программные компоненты	Дело уч.№ 1 дсп						
Мобильное техническое средство (флэш-накопитель, планшет, смартфон)	Модель Заводской номер						
Помещения, в которых находятся объекты защиты (режимные помещения)	Кабинет №___						

Приложение 5 к Политике информационной безопасности государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

(ОБРАЗЕЦ)

ЖУРНАЛ УЧЕТА МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ И НОСИТЕЛЕЙ ИНФОРМАЦИИ

Тип	Возможность перемещения за пределы КЗ	Учетный номер, пометка конфиденциальности	Расписка ответственного		Отметка об уничтожении (номер и дата акта, подпись, дата)
			Принял	Сдал	

Приложение 6 к Политике информационной безопасности государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

(ОБРАЗЕЦ)

ЖУРНАЛ УЧЕТА КОПИРОВАЛЬНО-МНОЖИТЕЛЬНЫХ РАБОТ

N п/п	Дата	Исполнитель	Наименование документа	кол-во листов	тираж	Роспись

Приложение 7 к Политике информационной безопасности государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

(ОБРАЗЕЦ)
АКТ № ___

УНИЧТОЖЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Комиссия в составе:

Председатель комиссии – ответственный за обеспечение информационной безопасности: _____

Члены комиссии:

- Администратор информационной безопасности: _____
- Пользователь: _____

составила настоящий акт о том, что перечисленные носители информации / данные с перечисленных носителей информации подлежат уничтожению / стиранию.

Учетный (инвентарный) номер.	Причина уничтожения или стирания информации	Тип МНИ, документа	Производимая операция (стирание, уничтожение)
1	2	3	4

Учетные данные носителей, перед уничтожением данных сверили с записями в акте. Защищаемая информация полностью уничтожена средствами гарантированного уничтожения данных в составе средства защиты информации от несанкционированного доступа _____. Контроль отсутствия остаточной информации произведен администратором ИБ с использованием средства анализа защищенности _____.

ИЛИ если бумажный носитель, то :

Учетные данные носителей, перед уничтожением данных сверили с записями в акте и полностью уничтожили путем сжигания.

ФИО Подпись

_____

_____

_____

Приложение 8 к Политике информационной безопасности государственного бюджетного учреждения Ростовской области «Областной клинический центр фтизиопульмонологии»

(ОБРАЗЕЦ)

ПЛАН РЕЗЕРВНОГО КОПИРОВАНИЯ

Информационные ресурсы	**Уровень копирования**	**Тип резервного носителя**	**Средства копирования**	**Время копирования**	**Место хранения копии**