ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«Камчатский краевой противотуберкулезный диспансер»
(ГБУЗ ККПТД)

ПРИКАЗ № 1036

г. Петропавловск-Камчатский «30» 12 2020 года

О назначении ответственного за организацию обработки персональных данных и администратора безопасности в информационной системе персональных данных «Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана»

В целях исполнения положений Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» и Приказа ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

ПРИКАЗЫВАЮ:

1. Ответственным за организацию обработки персональных данных в филиале №1 «ГБУЗ ККПТД» - пгт.Палана назначить Винокурову И.Н.
2. Юрисконсульту Пожарской О.В. внести в должностную инструкцию Винокуровой И.Н дополнение.
3. Ответственному за организацию обработки персональных данных обеспечить автоматизированную обработку персональных данных на объектах информатизации, удовлетворяющих действующему законодательству.
4. Утвердить прилагаемую инструкцию ответственного за организацию обработки персональных данных.
5. Ответственному за организацию обработки персональных данных руководствоваться инструкцией ответственному за организацию обработки персональных данных.
6. Ответственному за организацию обработки персональных данных обеспечить неавтоматизированную обработку персональных данных в соответствии с действующим законодательством.
7. Администратором безопасности информации в филиале № 1 "ГБУЗ ККПТД" - пгт. Палана назначить Малышева М.Н.
8. Утвердить прилагаемую инструкцию администратора безопасности.
9. Администратору безопасности в своей работе руководствоваться инструкцией администратора безопасности Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана.
10. Администратору безопасности организовать проведение работ по защите информации в соответствии с руководящими документами ФСТЭК России и ФСБ России.
11. Допуск к обработке персональных данных осуществлять в соответствии с внутренними документами, регламентирующими разграничение прав доступа к персональным данным.
12. Лицам, допущенным к обработке персональных данных при неавтоматизированной их обработке и хранении руководствоваться документом «Правила обработки персональных данных без использования средств автоматизации».

13.Лицам, допущенным к обработке персональных данных при автоматизированной их обработке руководствоваться следующими внутренними документами:

- политика информационной безопасности;
- инструкция пользователя.

14.Осуществлять регистрацию обращений субъектов персональных данных в Журнале учета обращений субъектов персональных данных о выполнении их законных прав.

15. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач А. В. Громов

УТВЕРЖДЕНА
Приказом о назначении ответственного за организацию обработки персональных данных и администратора безопасности в информационной системе персональных данных «Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана»
от «30» 12 2020г. № 1036

Инструкция администратора безопасности в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана (далее – Администратор) назначается приказом главного врача Камчатского краевого противотуберкулезного диспансера и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) и другой конфиденциальной информации (далее – КИ) в процессе ее обработки в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана.

1.2. Администратор обязан поддерживать в актуальном состоянии свои знания законодательных, нормативно-правовых актов Российской Федерации и методических материалов в сфере обработки и защиты ПДн и КИ.

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

1.4. Администратор безопасности подчиняется напрямую главному врачу в части вопросов информационной безопасности и имеет право требовать от пользователей ИС выполнения указаний и инструкций, связанных с защитой информации.

1.5. Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

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

2. ФУНКЦИИ И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ В ФИЛИАЛЕ № 1 "ГБУЗ ККПТД" - ПГТ. ПАЛАНА

2.1. Изучение особенностей технологических процессов обработки информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана с целью принятия решения о необходимости защиты информации и классификации, либо поиск специализированных организаций, производящих на договорной основе такой анализ. В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации сотрудниками сторонней организации. По окончании аналитических работ Администратор обязан ознакомиться с их результатами и подписать отчетные документы, либо составить мотивированный отказ в подписании таких документов и отправить их на доработку сторонней организации.

2.2. Определение актуальных угроз безопасности информации и разработка документа «Модель угроз безопасности», либо привлечение на договорной основе сторонних организаций для таких работ.

2.3. Периодический пересмотр актуальных угроз безопасности информации в следующих случаях:

- ежегодный плановый пересмотр актуальных угроз безопасности информации;
- появление в общедоступных источниках информации о новых угрозах и уязвимостях, имеющих предпосылки;
- существенное изменение условий функционирования, внедрение новых технологий;
- изменение нормативной документации, касающейся моделирования угроз безопасности информации;
- в результате инцидента безопасности.

2.4. Разработка проектной документации на систему защиты информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана (Техническое задание, Технический проект), либо привлечение на договорной основе сторонних организаций для таких работ.

2.5. Участие в подготовке технических заданий для конкурсов и аукционов, связанных с закупкой технических средств, программного обеспечения или средств защиты информации для Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана.

2.6. Участие в реализации проекта по защите информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана (тестирование системы защиты информации, внедрение системы защиты информации, аттестация по требованиям к защите информации, ввод в действие аттестованной ИС).

2.7. Выработка предложений главному врачу Камчатского краевого противотуберкулезного диспансера по совершенствованию системы защиты информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана.

2.8. Ведение учета применяемых в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана средств защиты информации (в том числе криптосредств), эксплуатационной и технической документации к ним.

2.9. Знание состава, структуры, назначения и выполняемых задач Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана, а также состава информационных технологий и технических средств, позволяющих осуществлять обработку ПДн и иной конфиденциальной информации.

2.10. Обеспечение передачи конфиденциальной информации и персональных данных через сети связи общего пользования в зашифрованном виде.

2.11. Разработка плана мероприятий по обеспечению безопасности защищаемой информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана и по защите периметра информационной системы. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости.

2.12. Осуществление контроля неизменности состояния аттестованной ИС (расположение и состав технических средств, состав программного обеспечения, физическое и логическое строение сети). В случае планирования изменения условий функционирования ИС, Администратор должен связаться с аттестующим органом и получить указания к дальнейшим действиям.

2.13. Осуществление контроля физической сохранности и целостности технических средств ИС, а также контроль сохранности и целостности опечатывающих пломб на технических средствах ИС (в том числе и программно-аппаратных средствах защиты информации). Контроль неизменности состава технических средств в ИС.

2.14. Проведение инструктажей сотрудников, работающих с защищаемой информацией в ИС (далее – Пользователи ИС), по темам: правила работы в ИС, защита информации в ИС, положения законодательства в сфере защиты информации и персональных данных, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана в вопросах информационной безопасности.

2.15. Организация первоначального доступа пользователям ИС к ресурсам информационный системы в соответствии с утвержденным положением о разграничении прав доступа в ИС. Ввод в систему qMS штатной структуры филиала № 1 "ГБУЗ ККПТД" - пгт. Палана и присваивание сотрудникам соответствующих их должностным обязанностям ролей в системе.

2.16. Периодическое тестирование функций системы защиты от НСД согласно плану мероприятий по обеспечению безопасности информации, либо при изменении программной среды или полномочий Пользователей ИС.

2.17. Участие в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности, внесение по результатам таких расследований предложений по совершенствованию системы безопасности главному врачу филиала № 1 "ГБУЗ ККПТД" - пгт. Палана, КГКУЗ МИАЦ и/или Министерству здравоохранения Камчатского края. По мере возможности, Администратор должен восстанавливать ущерб, нанесенный информационной системе во время инцидента безопасности, а также восстанавливать ПДн и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента.

2.18. Контроль выполнения Пользователями ИС требований Инструкции пользователя ИС, а также других установленных требований для обеспечения безопасности ПДн и иной конфиденциальной информации.

2.19. В случае получения от Пользователей ИС информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, Администратор незамедлительно принимает все необходимые меры для обеспечения безопасности ПДн и иной конфиденциальной информации в пределах своих полномочий.

2.20. Обеспечение отсутствия на АРМ Пользователей ИС средств разработки и отладки программного обеспечения. Контроль за отключением на АРМ Пользователей и невозможностью самостоятельного включения пользователем технологий мобильного кода (JavaScript, Adobe Flash, макросы MS Office и т. д.), кроме случаев, когда использование таких технологий необходимо для выполнения служебных (должностных) обязанностей.

2.21. Выявление уязвимостей ИС посредством периодического сканирования системы сертифицированным сканером безопасности Max Patrol централизованно осуществляют администраторы безопасности КГКУЗ МИАЦ. Администраторы безопасности КГКУЗ МИАЦ в случае выявления уязвимостей направляют соответствующие отчеты Администратору филиала № 1 "ГБУЗ ККПТД" - пгт. Палана. Администратор филиала № 1 "ГБУЗ ККПТД" - пгт. Палана принимает меры по устранению выявленных уязвимостей.

2.22. Контроль сотрудников сторонних организаций, производящих ремонт/обслуживание технических средств ИС или настройку/установку программного обеспечения ИС.

2.23. Обеспечение непрерывности процессов в ИС. В случае нарушения работоспособности технических средств и программного обеспечения ИС, в том числе средств защиты ИС, Администратор принимает меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

2.24. Своевременное информирование Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ИС.

3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИС

Администратор имеет право:

3.1. Знакомиться с локальными нормативными актами филиала № 1 "ГБУЗ ККПТД" - пгт. Палана, регламентирующими процессы обработки и защиты ПДн и иной конфиденциальной информации.

3.2. Вносить предложения главному врачу филиала № 1 "ГБУЗ ККПТД" - пгт. Палана по совершенствованию существующей системы защиты информации.

3.3. Требовать от Пользователей ИС соблюдения требований Инструкции пользователя ИС и иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн и иной конфиденциальной информации.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн и иной конфиденциальной информации.

3.5. Требовать прекращения работы в ИС, как в целом, так и отдельных Пользователей ИС, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИС.

3.6. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

4. РАБОЧЕЕ МЕСТО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИС И ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Одним из ключевых элементов системы защиты информации в ИС Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана является АРМ Администратора.

4.2. АРМ Администратора устанавливается таким образом, чтобы исключался как преднамеренный, так и непреднамеренный несанкционированный доступ к техническим средствам АРМ Администратора.

4.3. По требованию Администратора КГКУЗ МИАЦ осуществляет централизованное управление политиками безопасности в ИС, обновлениями средств защиты информации, обновлениями антивирусных баз и сигнатур, конфигурацией информационной системы.

4.4. Администратор изучает журналы безопасности средств защиты информации на предмет выявления инцидентов безопасности.

4.5. Рабочее место администратора является объектом защиты и защищается согласно требованиям к тому же классу, по которому классифицирована ИС в целом.

5. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦАНИРОВАННОГО ДОСТУПА DALLAS LOCK 8.0-К

5.1. Администратор участвует в развертывании средства защиты информации от несанкционированного доступа (далее – СЗИ от НСД) в ИС и осуществляет управление и централизованный мониторинг этого средства с рабочего места Администратора.

5.2. Администратор производит настройку подсистемы регистрации, идентификации и аутентификации в СЗИ от НСД Dallas Lock 8.0-К согласно утвержденному Положению о разграничении доступа. Идентификации и аутентификации подлежат как пользователи, так и учетные записи служб, приложений, программных процессов.

5.3. Внешние пользователи проходят идентификацию и аутентификацию в рамках общего домена Acticve Directory. Внешними пользователями ИС Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана являются только администраторы безопасности КГКУЗ МИАЦ. Администратор обеспечивает наличие минимального количества точек входа внешних пользователей в ИС. Администратор производит мониторинг подключений и действий внешних пользователей в ИС. Администратор обеспечивает доступ внешних (удаленных) пользователей к ИС по защищенным каналам связи.

5.4. Внешние пользователи проходят двухфакторную аутентификацию при установлении сеанса связи с ИС.

5.5. Технические средства проходят идентификацию и аутентификацию в ИС. Идентификация и аутентификация устройств производится посредством информационного обмена по специализированным сетевым протоколам (ARP, SNMP, NetBIOS и др.). В качестве идентификаторов устройств могут выступать: логические

имена, идентификационные номера, IP-адреса, MAC-адреса или комбинация этих параметров. Администратор определяет правила идентификации и аутентификации устройств в ИС, конфигурирует протоколы и настраивает в средствах защиты информации соответствующие правила. Администратор принимает меры для предупреждения таких атак на ИС как MAC-flooding, MAC-spoofing, ARP-spoofing, ARP-poisoning и других.

5.6. Учетные записи Active Directory формируются в КГКУЗ МИАЦ, там же таким учетным записям назначаются роли и полномочия в системе. Администратор имеет возможность создавать только внутренние учетные записи системы qMS. В процессе управления учетными записями системы qMS Администратор производит следующие действия:

- определяет тип учетной записи;
- присвоение учетным записям ролей и полномочий;
- проводит верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
- производит заведение, активацию, блокирование и уничтожение учетных записей пользователей;
- проводит пересмотр и, при необходимости, корректировку учетных записей пользователей либо в процессе периодического мероприятия, либо в связи с изменением должностных обязанностей того или иного пользователя;
- своевременно уничтожает (блокирует) учетные записи уволенных сотрудников.

5.7. Средствами СЗИ от НСД Dallas Lock 8.0-K в ИС Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана запрещаются любые действия пользователя в ИС до прохождения процедур идентификации и аутентификации, в том числе ограничивается доступ к настройкам BIOS/UEFI. Администратору информационной безопасности до идентификации и аутентификации разрешаются следующие действия с целью диагностики проблем на элементах ИС и восстановления работоспособности элементов ИС:

- загрузка операционной системы в безопасном режиме;
- восстановление операционной системы с последней работоспособной конфигурацией;
- перепрошивка терминальной станции;
- изменение параметров BIOS/UEFI;
- загрузка с внешнего носителя с целью восстановления или переустановки операционной системы, восстановления работоспособности средств защиты информации, сканирования жесткого диска на вирусы, сканирования оперативной памяти или жесткого диска с целью выявления проблем и других действий восстановительного или диагностического характера.

5.8. Администратор является ответственным за хранение, выдачу, инициализацию средств аутентификации (учетных записей и первичных паролей). Администратор определяет парольную политику и требования к сложности паролей в системе qMS. Администратор выдает пользователю пароль для первоначального входа в ИС. QMS требует от пользователя сменить пароль при первом же входе в программное обеспечение. Плановая смена пароля производится пользователем самостоятельно. Смена пароля Администратором допускается в случаях компрометации пароля пользователя или при подозрении на его компрометацию, в этом случае система также должна запросить смену пароля пользователем при первом входе в ИС после смены пароля Администратором. Администратор не должен и не обязан знать пароли пользователей ИС. В ИС устанавливаются следующие требования к паролям:

- минимальная длина пароля составляет 8 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего реИСтров, как минимум одну цифру и один спецсимвол;
- при смене пароля, новый пароль должен отличаться минимум на два символа от предыдущего;
- максимальное время действия пароля – 90 дней;
- запрещается использование пользователями пяти последних использованных паролей при создании новых паролей;
- при восьми неудачных попытках входа учетная запись блокируется не менее чем на 10 минут.

5.9. Администратор устанавливает временной промежуток в 15 минут в качестве допустимого времени бездействия пользователя. После истечения указанного времени происходит блокировка сеанса пользователя.

5.10. Администратор контролирует наличие и работоспособность средств доверенной загрузки.

5.11. Администратор ограничительными программными методами запрещает пользователям самостоятельную установку любого программного обеспечения. В Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана утверждается перечень разрешенного к установке в ИС программного обеспечения. Перечень разрешенного к установке программного обеспечения определяется исходя из целей и задач, решаемых с помощью ИС. Перечень разрешенного к установке в ИС программного обеспечения подлежит периодическому пересмотру. Установка разрешенного программного обеспечения производится либо Администратором лично, либо в присутствии Администратора и под контролем Администратора.

6. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ И СРЕДСТВ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ, ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

6.1. При первичной настройке сетевого оборудования, Администратор изменяет все пароли по умолчанию, установленные производителем сетевого оборудования.

6.2. С помощью средств межсетевого экранирования, штатных функций операционных систем и сетевых устройств и средства централизованного мониторинга и настройки Администратор осуществляет управление информационными потоками при передаче информации между устройствами и сегментами сети. Под управлением информационными потоками понимается: фильтрация информационных потоков, разрешение передачи информации в ИС только по определенному Администратором маршруту и обеспечение контролируемого изменения (перенаправления) маршрута передачи информации.

6.3. Администратор осуществляет настройку сетевого оборудования или контролирует этот процесс, в случае такой настройки представителями сторонних организаций.

6.4. Администратор анализирует технологические процессы обработки информации, а также особенности функциональных обязанностей сотрудников Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана для оптимизации настроек средств межсетевого экранирования. Средство межсетевого экранирования настраивается по принципу разрешения только тех ресурсов, сетевых портов и протоколов, необходимых для нормального функционирования ИС и Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана в целом.

6.5. Администратор обеспечивает защиту информации, передаваемой по не доверенным каналам связи за пределы контролируемой зоны, с помощью криптографических средств.

6.6. Администратор осуществляет настройку и контроль функционирования специальных средств, осуществляющих фильтрацию и контроль входящих нежелательных электронных писем (спама). При этом, учитывая возможность ложного срабатывания такой системы, пользователь должен иметь возможность просмотра отфильтрованных сообщений. Администратор инструктирует пользователей о возможных типах мошенничества с использованием электронной почты (социальная инженерия, фишинг и прочее).

7. ОБСЛУЖИВАНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

7.1. Общие правила работы с криптосредствами описаны в утвержденной Инструкции по обеспечению безопасности эксплуатации СКЗИ. В данном разделе описана часть, касающаяся функций и обязанностей Администратора.

7.2. Администратор обеспечивает соответствие работы с СКЗИ технической и эксплуатационной документации к ним.

7.3. Администратор осуществляет поэкземплярный учет СКЗИ, технической и эксплуатационной документации к ним в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в ИС.

7.4. Администратор контролирует передачу СКЗИ, ключевой информации, технической и эксплуатационной документации пользователям ИС. Факт передачи отражается в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в ИС.

7.5. Администратор обеспечивает хранение дистрибутивов СКЗИ, эксплуатационную и техническую документацию к ним, ключевую информацию в шкафах (сейфах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.6. Администратор обеспечивает раздельное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

7.7. Администратор производит инструктаж Пользователей ИС перед работой с СКЗИ. Отметка о проведении инструктажа проставляется в Журнале учета инструктажей по информационной безопасности в ИС.

7.8. Администратор составляет и поддерживает в актуальном состоянии список лиц, допущенных к работе с СКЗИ.

7.9. Администратор осуществляет проверку готовности СКЗИ к использованию в ходе проведения проверок согласно Плану мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в ИС (далее – План мероприятий). Факт проверки отражается в Журнале учета мероприятий по контролю обеспечения защиты информации в ИС. Результат проверки отражается в Журнале периодического тестирования средств защиты информации в ИС. Проверка каждого СКЗИ проводится не реже одного раза в месяц.

7.10. Администратор инструктирует пользователей о порядке хранения ключевой информации и осуществляет контроль соблюдения пользователями правил хранения такой информации.

7.11. Администратор принимает участие в составе группы реагирования на инциденты информационной безопасности в расследовании случаев попыток посторонних лиц получить сведения об используемых СКЗИ, случаев компрометации или при подозрении на компрометацию ключевой информации, случаев утраты дистрибутивов СКЗИ, ключевой информации, ключевых носителей, технической и эксплуатационной документации к СКЗИ, ключей от помещений и хранилищ СКЗИ. В случае компрометации ключевой информации, Администратор немедленно выводит ее из эксплуатации.

7.12. Администратор в составе комиссии по уничтожению принимает участие в уничтожении ключевой информации и ключевых документов. Уничтожение ключевой информации производится путем физического уничтожения ключевого носителя или путем гарантированного затирания ключевой информации.

8. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ

8.1. КГКУЗ МИАЦ осуществляет настройку и контроль функционирования системы антивирусной защиты в ИС. Управление системой осуществляется централизованно, и только Администратор может осуществлять такую функцию. Антивирусная защита осуществляется на серверах ИС Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана

8.2. КГКУЗ МИАЦ централизованно настраивает время, периодичность и другие параметры проведения полной антивирусной проверки узлов ИС на наличие вредоносных компьютерных программ (вирусов) согласно Плану мероприятий. Факт проверки отражается в Журнале учета мероприятий по контролю обеспечения защиты информации в ИС.

8.3. Администратор самостоятельно или в составе группы реагирования на инциденты информационной безопасности (в случае значительного инцидента безопасности) реагирует на сообщения системы антивирусной защиты или пользователей об обнаружении вредоносных компьютерных программ (вирусов), или на подозрение наличия таковых, и принимает меры по нейтрализации обнаруженных угроз.

8.4. КГКУЗ МИАЦ настраивает периодичность обновления баз и сигнатур антивирусного средства. Администратор также настраивает механизм распространения обновленных антивирусных баз на все узлы ИС. Обновление антивирусных баз и сигнатур проводится ежедневно.

9. РЕИСТРАЦИЯ И УЧЕТ СОБЫТИЙ БЕЗОПАСНОСТИ

9.1. Под системой регистрации и учета событий безопасности в ИС понимается совокупность средств централизованного управления всех СЗИ в ИС.

9.2. Система регистрации и учета событий безопасности, а также информация, хранящаяся в электронных журналах регистрации событий сами по себе являются объектами защиты. КГКУЗ МИАЦ принимает меры по защите этой информации в соответствии с техническим заданием на систему защиты информации и эскизным проектом системы защиты информации. Доступ к записям системы регистрации и учета событий безопасности разрешен только КГКУЗ МИАЦ.

9.3. Администратор периодически изучает записи системы регистрации и учета событий безопасности и в случае обнаружения инцидентов безопасности информации созывает

группу реагирования на инциденты информационной безопасности, которая в свою очередь действует согласно соответствующим инструкциям.

10. ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

10.1. Выявление уязвимостей в информационной системе осуществляется централизованно КГКУЗ МИАЦ с помощью сетевого сканера Max Patrol (модуль – PenTest).

10.2. В случае обнаружения уязвимостей в ИС Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана, специалисты КГКУЗ МИАЦ направляют отчет о сканировании Администратору. В случае неполучения такого отчета, констатируется, что уязвимостей в ИС Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана не обнаружено.

10.3. В случае получения отчета с выявленными уязвимостями, Администратор принимает меры по их устранению или нейтрализации. В первую очередь обрабатываются уязвимости с наивысшим баллом по шкале CVSS. В случае необходимости, до устранения уязвимости могут быть локализованы (отключены от общей сети) сегменты или отдельные АРМы информационной системы.

11. ПРАВИЛА РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ, ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

11.1. В Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана с целью обеспечения целостности и доступности защищаемой информации применяется резервное копирование.

11.2. Резервное копирование базы данных qMS производится автоматически на систему хранения данных механизмами СУБД Cache (производится вручную КГКУЗ МИАЦ на автономный съемный носитель информации – оставить подходящий вариант или сформулировать свой). Резервное копирование в места, где не представляется возможность обеспечить или проконтролировать наличие должной системы защиты информации (например, в облачные хранилища), запрещено.

11.3. Перечень ресурсов, подлежащих резервному копированию, а также периодичность резервного копирования той или иной информации приведены в политике информационной безопасности и должны актуализироваться КГКУЗ МИАЦ по мере необходимости.

11.4. Процедуры резервного копирования проводятся в нерабочее время, либо во время наименьшей нагрузки на информационную систему.

11.5. На носителе с резервной копией хранится не более трех последних резервных копий каждого вида информации. Наиболее старые резервные копии удаляются с целью освобождения дискового пространства для более свежих резервных копий.

11.6. На резервные копии и на носители с резервными копиями распространяются все политики и требования по обеспечению информационной безопасности.

11.7. КГКУЗ МИАЦ осуществляет проверку удачного завершения каждой процедуры резервного копирования. В случае ошибки при резервном копировании, КГКУЗ МИАЦ выясняет причину ошибки, устраняет ее и запускает процесс резервного копирования повторно.

11.8. Восстановление информации из резервной копии производится КГКУЗ МИАЦ по мере необходимости или в случае инцидента информационной безопасности. Восстановление информации из резервной копии может проводиться в экстренном

порядке или в штатном режиме, в зависимости от ущерба, который был нанесен информационной системе в результате инцидента информационной безопасности.

11.9. Программное обеспечение и средства защиты информации в случае нарушения целостности или работоспособности восстанавливаются с эталонных дистрибутивов, поставляемых в комплекте с документацией. Эталонные дистрибутивы хранятся в сейфе у Администратора. Настройки программного обеспечения и средств защиты информации восстанавливаются вручную или из предварительно сохраненных конфигураций.

11.10. В случае выхода из строя технических средств, Администратор принимает меры по ремонту и/или их замене. С целью предотвращения потери данных при отключении электричества в ИС предусмотрены источники бесперебойного питания на серверах и АРМ Пользователей.

12. ДЕЙСТВИЯ АДМИНИСТРАТОРА ПРИ РЕМОНТЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ОБСЛУЖИВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И УТИЛИЗАЦИИ НОСИТЕЛЕЙ ИНФОРМАЦИИ

12.1. Администратор присутствует в процессе установки, обновления, настройки программного обеспечения в ИС (в том числе и средств защиты информации) сотрудниками сторонних организаций.

12.2. Администратор присутствует в процессе ремонта технических средств ИС сотрудниками сторонних организаций на территории Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана. Администратор обеспечивает гарантированное затирание данных с носителей информации, либо демонтаж носителей информации (в том числе и оперативной памяти) с технических средств в случае необходимости отправки технических средств для ремонта на территорию сторонних организаций.

12.3. Администратор обеспечивает гарантированное затирание данных на машинных носителях информации при утилизации технических средств, либо принимает участие в физическом уничтожении машинных носителей информации в составе комиссии по уничтожению.

УТВЕРЖДЕНА
Приказом о назначении ответственного за организацию обработки персональных данных и администратора безопасности в информационной системе персональных данных «Филиале №1 "ГБУЗ ККПТД" - пгт. Палана»
от «30» 12 2020г. № 441

Инструкция ответственного за организацию обработки персональных данных в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана (далее – Ответственный) назначается приказом главного врача Камчатского краевого противотуберкулезного диспансера (далее – Учреждение) и отвечает за организацию, обеспечение своевременного и квалифицированного выполнения сотрудниками Учреждения законодательства Российской Федерации о персональных данных (далее – ПДн), в том числе требований к обработке и защите ПДн.

1.2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн. Ответственный поддерживает в актуальном состоянии свои знания в сфере действующего законодательства и законодательных инициатив, связанных с защитой персональных данных.

1.3. В своей деятельности Ответственный руководствуется Положением об обработке и защите персональных данных, настоящей Инструкцией и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.

2. ОСНОВНЫЕ ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по организации обработки ПДн при решении следующих основных вопросов:

- организация доступа к ПДн и учет сотрудников Учреждения, допущенных к обработке ПДн, как в программных комплексах, входящих в состав ИС, так и на бумажных носителях;
- контроль за поддержанием в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с ПДн;
- контроль за обеспечением соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
- организация работы по заключению договоров на работы по защите ПДн;
- рассмотрение предложений по совершенствованию действующей системы защиты ПДн, предоставленных Администратором, назначаемым приказом руководителя Камчатского краевого противотуберкулезного диспансера;
- осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

3. ОСНОВНЫЕ ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Знать цели обработки ПДн в Учреждении и перечень обрабатываемых ПДн.

3.2. Соблюдать требования нормативных актов Учреждения, устанавливающих порядок работы с ПДн.

3.3. Обеспечивать доведение до сведения сотрудников Учреждения законодательства Российской Федерации о ПДн, нормативных актов по вопросам обработки ПДн, требований к защите ПДн.

3.4. Осуществлять внутренний контроль за соблюдением сотрудниками Учреждения законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

3.5. Контролировать ведение документации, предусмотренной нормативными актами Учреждения в части обеспечения безопасности ПДн.

3.6. Обеспечивать доработку локальных нормативных документов по защите ПДн Учреждения в случае такой необходимости или при поступлении такого требования от регулирующего органа.

3.7. Участвовать в расследовании нарушений по вопросам защиты ПДн, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений.

3.8. Обеспечивать организацию проведения занятий со специалистами Учреждения по организационным вопросам обработки ПДн (проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в Учреждении).

3.9. Обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно п.3 ч.4 ст.22.1 Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных».

4. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Знакомиться с документами и материалами, необходимыми для выполнения возложенных на него задач.

4.2. Проводить проверки соблюдения режима обеспечения безопасности ПДн в соответствии с утвержденным приказом главного врача Камчатского краевого противотуберкулезного диспансера планом мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана.

4.3. Требовать от сотрудников Учреждения соблюдения требований нормативно-правовых и организационно-распорядительных документов по вопросам обработки ПДн.

4.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обработки ПДн.

4.5. Требовать от сотрудников Учреждения письменных объяснений при проведении служебных расследований по вопросам нарушений требований по обработке и защите ПДн.

4.6. Вносить предложения главному врачу Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите ПДн.

4.7. Давать сотрудникам Учреждения обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и локальными нормативными актами Учреждения.

4.8. Привлекать в установленном порядке специалистов Учреждения, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.