Муніципальна бюджетна загальноосвітня установа «Ялтинська середня школа № 4» муніципального утворення міський округ ЯлтаРеспубліки Крим

Муниципальное бюджетное общеобразовательное учреждение «Ялтинская средняя школа № 4» муниципального образования городской округ Ялта Республики Крым

Къырым Джумхуриетининъ Ялты шеэр округы тешкилятынынъ Муниципаль бюджет умумтасиль муэссисеси «Ялта орта мектеби № 4»

Пер.. Клубный, д. 7, г. Ялта, Республика Крым, 298637,
тел. (3654) 23-18-08, e-mail: school_4-yalta@crimeaedu.ru
ОГРН 1149102176563 ИНН 9103017147 КПП 910301001
ОКПО 00810213

П Р И К А З

от 11.01.2023 г. г. Ялта № 12

О назначении ответственного за организацию обработки персональных данных и администратора безопасности.

В целях исполнения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», 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 МБОУ «ЯСШ №4» назначить заместителя директора по УВР Атаманчук В.Б.
2. Ответственному за организацию обработки персональных данных обеспечить автоматизированную обработку персональных данных на объектах информатизации, удовлетворяющих действующему законодательству.
3. Утвердить прилагаемую инструкцию ответственного за организацию обработки персональных данных.
4. Ответственному за организацию обработки персональных данных руководствоваться инструкцией ответственному за организацию обработки персональных данных.
5. Ответственному за организацию обработки персональных данных обеспечить неавтоматизированную обработку персональных данных в соответствии с действующим законодательством.
6. Администратором безопасности информации в МБОУ «ЯСШ №4»назначить учителя информатики Макарову Д.А.
7. Утвердить прилагаемую инструкцию администратора безопасности.
8. Администратору безопасности в своей работе руководствоваться инструкцией администратора безопасности.
9. Администратору безопасности организовать проведение работ по защите информации в соответствии с законодательством Российской Федерации.
10. Допуск к обработке персональных данных осуществлять в соответствии с внутренними документами, регламентирующими разграничение прав доступа к персональным данным.
11. Лицам, допущенным к обработке персональных данных при неавтоматизированной их обработке и хранении руководствоваться документом «Правила обработки персональных данных без использования средств автоматизации».

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

- политика информационной безопасности;
- инструкция пользователя сегмента РЕГИСЗ ПК.

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

14. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Т.А.Шабанова
Ознакомлены В.Б.Атаманчук
Д.А.Макарова

УТВЕРЖДЕНА
приказом {Наименование МО}
от «___» _____20__г. № ___

Инструкция администратора безопасности

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности {Наименование МО}(далее – Администратор) назначается приказом главного врача{Наименование МО}и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее –ПДн)и другой конфиденциальной информации(далее – КИ) в процессе ее обработки в{Наименование МО}.

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{Наименование МО}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 ВСЕГМЕНТЕ РЕГИСЗПК

2.1. Изучение особенностей технологических процессов обработки информации в, либо поиск специализированных организаций, производящих на договорной основе такой анализ.В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации о{Наименование МО}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 модели угроз, 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 в{Наименование МО};
−существенное изменение условий функционирования системы защиты {Наименование МО}, внедрение новых технологий;
−изменение нормативной документации, касающейся моделирования угроз безопасности информации;
−в результате инцидента безопасности.

2.4. Участие в подготовке технических заданий для конкурсов и аукционов, связанных с закупкой технических средств, программного обеспечения или средств защиты информации для {Наименование МО}.

2.5. Участие в реализации проекта по защите информации в{Наименование МО}.

2.6. Выработка предложений главному врачу{Наименование МО} по совершенствованию системы защиты информации в {Наименование МО}.

2.7. Ведение учета применяемых в{Наименование МО}средств защиты информации (в том числе криптосредств), эксплуатационной и технической документации к ним.

2.8. Знание состава, структуры, назначения и выполняемых задач в {Наименование МО}, а также состава информационных технологий и технических средств, позволяющих осуществлять обработку ПДн и иной конфиденциальной информации.

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

2.10. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в{Наименование МО}и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятийпо мере необходимости.

2.11. Осуществление контроля неизменности состояния системы защиты{Наименование МО}, на который выдано заключение о соответствии требованиям по защите информации(расположение и состав технических средств, состав программного обеспечения, физическое и логическое строение сети) или составлен акт обоценки эффективности реализованных мер защиты информации. В случае планирования изменения условий функционирования сегментаРЕГИСЗ ПК, Администратор должен связаться с ГАУЗ «ПК МИАЦ» и получить указания к дальнейшим действиям.

2.12. Осуществление контроля физической сохранности и целостности технических средств{Наименование МО}. Контроль неизменности состава технических средств в{Наименование МО}.

2.13. Организация учета съемных носителей информации. Настройка соответствующих программных механизмов средств защиты информации для запрета неучтенных съемных носителей. Ведение журнала учета съемных носителей. {удалить раздел если не используются съемные носители информации}

2.14. Организация учета иных машинных носителей информации.

2.15. Проведение инструктажей сотрудников, работающих с защищаемой информацией в{Наименование МО}, по темам: правила работы в{Наименование МО}, защита информации в{Наименование МО}, положения законодательства в сфере защиты информации и персональных данных, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников в вопросах информационной безопасности.

2.16. Организация первоначального доступа пользователям{Наименование МО}к ресурсам информационных систем в соответствии с утвержденнымидокументами о разграничении прав доступа в{Наименование МО}.

2.17. Осуществление резервного копирования защищаемой в соответствии разделом 10 настоящей Инструкции.

2.18. Периодическое тестирование функций системы защиты от НСД.Тестирование функций системы защиты от НСД при изменении программной среды или полномочий Пользователей{Наименование МО}.

2.19. 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. По мере возможности, Администратор должен восстанавливать ущерб, нанесенный информационной системе во время инцидента безопасности, а такжевосстанавливать ПДн и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента.

2.20. Контроль выполнения Пользователями{Наименование МО}требований Инструкции пользователя{Наименование МО}, а также других установленных

требований для обеспечения безопасностиПДн и иной конфиденциальной информации.

2.21. В случае получения от Пользователей{Наименование МО}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.

2.22. Обеспечение отсутствия на АРМ Пользователей{Наименование МО}средств разработки и отладки программного обеспечения. Контроль за отключением на АРМ Пользователей и невозможностью самостоятельного включения пользователем технологий мобильного кода (JavaScript, AdobeFlash, макросы MSOfficeи т. д.), кроме случаев, когда использование таких технологий необходимо для выполнения служебных (должностных) обязанностей.

2.23. Выявление уязвимостейинформационным системам {Наименование МО}посредством периодического сканирования системы сертифицированным сканером безопасности.В случае выявления уязвимостей Администратор {Наименование МО}принимаетмеры по устранению выявленных уязвимостей.

2.24. Контроль обновлений системного, прикладного программного обеспечения и средств защиты информации (в том числе обновлений антивирусных баз, сигнатур сценариев вторжений, информации об уязвимостях).

2.25. Контроль сотрудников сторонних организаций, производящих ремонт/обслуживание технических средств{Наименование МО}или настройку/установку программного обеспечения{Наименование МО}.

2.26. Обеспечение функционирования и поддержания работоспособностив{Наименование МО}:

- системы защиты информации от несанкционированного доступа;
- системы межсетевого экранирования;
- системы криптографической защиты информации;
- системы антивирусной защиты.

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

2.28. Своевременное информирование Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа кинформационным системам {Наименование МО}.

3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

3.1. Знакомиться с локальными нормативными актами {Наименование МО}, регламентирующими процессы обработки и защиты ПДн и иной конфиденциальной информации.

3.2. Вносить предложения главному врачу{Наименование МО} по совершенствованию существующей системы защиты информации.

3.3. Требовать от Пользователей{Наименование МО}соблюдения требований Инструкции пользователя{Наименование МО}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 винформационных системах {Наименование МО} Пользователей{Наименование МО}, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционированияинформационных систем и/или системы защиты информации {Наименование МО}.

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

4. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИАНИРОВАННОГО ДОСТУПА

4.1. Администратор участвует в развертывании средства защиты информации от несанкционированного доступа (далее – СЗИ от НСД) в{Наименование МО}и осуществляет управление и мониторинг этих средств.

4.2. Администратор производит настройку подсистемы регистрации, идентификации и аутентификации в СЗИ от НСД согласно утвержденнымдокументам о разграничении доступа. Идентификации и аутентификации подлежат как пользователи, так и учетные записи служб, приложений, программных процессов.

4.3. Технические средства (мобильные и стационарные) также проходят идентификацию и аутентификацию в {Наименование МО}. 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 {Наименование МО}, конфигурирует протоколы и настраивает в средствах защиты информации соответствующие правила. Администратор принимает меры для предупреждения таких атак на {Наименование МО} как MAC-flooding, MAC-spoofing, ARP-spoofing, ARP-poisoning и других.

4.4. Администратор осуществляет учет машинных носителей информации, как стационарных (жесткие диски АРМ и серверов, SSD-накопители и т. д.), так и съемных (флеш-накопители, съемные жесткие диски, карты памяти, память мобильных устройств и т. д.). Каждому носителю присваивается идентификационный номер. Для стационарных машинных носителей информации фиксируется местонахождение носителя (АРМ, кабинет), в случае замены или утилизации стационарногоили съемного машинного носителя принимаются меры по гарантированному уничтожению информации на

носителе или самого носителя с соответствующей пометкой в Журнале учета машинных носителей информации.Съемные машинные носители информации выдаются пользователем под роспись в Журнале учета машинных носителей информации. Дата сдачи машинного носителя также фиксируется в Журнале. Администратор средствами СЗИ от НСД реализует запрет использования неучтенных машинных носителей в{Наименование МО}.{Удалить часть раздела, касающуюся съемных носителей, если таковые не применяются}

4.5. В процессе управления учетными записямисистемы Администратор производит следующие действия:

- определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная учетная запись, учетная запись приложения, гостевая учетная запись, временная учетная запись и т. д.);
- объединяет учетные записи в группы (при необходимости);
- проводит анализ необходимости тех или иных полномочий в системе для учетных записей служб и приложений;
- присваивает учетным записям роли и полномочия;
- 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 в связи с изменением должностных обязанностей того или иного пользователя;
- уничтожает временные учетные записи пользователей, предоставленные для однократного (или ограниченного по времени) выполнения задач иучетные записи уволенных сотрудников;
- осуществляет настройку прав доступа пользователей к ресурсам {Наименование МО} средствами СЗИ от НСД в соответствии с утвержденными документами о разграничении доступа.

4.6. Средствами СЗИ от НСД в{Наименование МО}запрещаются любые действия пользователя {Наименование МО}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 элементахинформационных систем {Наименование МО}и восстановления работоспособности элементовинформационных систем{Наименование МО}:

- 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.

4.7. Администратор является ответственным за хранение, выдачу, инициализацию средств аутентификации (учетных записей и первичных паролей).

Администратор определяет парольную политику и требования к сложности паролей. Администратор выдает пользователю пароль для первоначального входа на АРМ {Наименование МО}. Операционная система требует от пользователя сменить пароль при первом же входе. 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 на АРМ {Наименование МО}после смены пароля Администратором. Администратор не должен и не обязан знать пароли пользователей{Наименование МО}. В{Наименование МО}устанавливаются следующие требования к паролям:

- минимальная длина пароля составляет 8 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего регистров, 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.

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

4.9. Администратор ограничительными программными методамизапрещает пользователям самостоятельную установку любого программного обеспечения. В {Наименование МО}утверждается перечень разрешенного к установке в{Наименование МО}программного обеспечения.Перечень разрешенного к установке программного обеспечения определяется исходя из целей и задач, решаемых в {Наименование МО}. Перечень разрешенного к установке в{Наименование МО}программного обеспечения подлежит периодическому пересмотру.Установка разрешенного программного обеспечения производится либо Администратором лично, либо в присутствии Администратора и под контролем Администратора.

4.10. Механизмами СЗИ от НСД Администратор устанавливает правила использования интерфейсов ввода/вывода технических средств{Наименование МО}. СЗИ от НСД настраивается таким образом, чтобы пользователь{Наименование МО}получал доступ к использованию только тех интерфейсов ввода/вывода, которые необходимы ему для выполнения служебных обязанностей.

5. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ, ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

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

5.2. 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 локальной сети. Под управлением информационными потоками

понимается: фильтрация информационных потоков, разрешение передачи информации в{Наименование МО}только по определенному Администратором маршруту и обеспечение контролируемого изменения (перенаправления) маршрута передачи информации.

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

5.4. Администратор анализирует технологические процессы обработки информации, а также особенности функциональных обязанностей сотрудников {Наименование МО} для оптимизации настроек средств межсетевого экранирования. Средство межсетевого экранирования настраивается по принципу разрешения только тех ресурсов, сетевых портов и протоколов, необходимых для нормального функционирования{Наименование МО}.

5.5. Администратор организует взаимодействие с информационными системами сторонних организаций.

5.6. Администратор обеспечивает защиту информации, передаваемой по недоверенным каналам связи за пределы контролируемой зоны, с помощью криптографических средств.

5.7. 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)

6. ОБСЛУЖИВАНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

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

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

6.3. Администратор осуществляетпоэкземплярный 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{Наименование МО}.

6.4. Администратор контролирует передачу СКЗИ, ключевой информации, технической и эксплуатационной документации пользователям{Наименование МО}. Факт передачи отражается в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в{Наименование МО}.

6.5. 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.

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

6.7. Администратор производит инструктаж Пользователей сегмента РЕГИСЗПКперед работой с СКЗИ. Отметка о проведении инструктажа проставляется в Журнале учета инструктажей по информационной безопасности в{Наименование МО}.

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

6.9. Администратор осуществляет проверку готовности СКЗИ к использованию. Факт проверки отражается в Журнале учета мероприятий по контролю обеспечения защиты информации в{Наименование МО}. Результат проверки отражается в Журнале периодического тестирования средств защиты информации в{Наименование МО}. Проверка каждого СКЗИ проводится не реже одного раза в месяц.

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

6.11. 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.

6.12. 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.

7. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ

7.1. Администратор осуществляет настройку и контроль функционирования системы антивирусной защиты в{Наименование МО}. Управление системой осуществляется централизованно, и только Администратор может осуществлять такую функцию. Антивирусная защита осуществляется на АРМ и серверах,мобильных технических средствах и иных точках доступав информационные системы {Наименование МО}.

7.2. Администратор централизованнонастраивает время, периодичность и другие параметры проведения полной антивирусной проверки узлов{Наименование МО}на наличие вредоносных компьютерных программ (вирусов). Факт проверки отражается в Журнале учета мероприятий по контролю обеспечения защиты информации в{Наименование МО}.

7.3. 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.

7.4. Администратор настраивает периодичность обновления баз и сигнатур антивирусного средства. Администратор также настраивает механизм распространения обновленных антивирусных баз на все узлы{Наименование МО}. Обновление антивирусных баз и сигнатур проводится ежедневно.

8. РЕГИСТРАЦИЯ И УЧЕТ СОБЫТИЙ БЕЗОПАСНОСТИ

8.1. Под системой регистрации и учета событий безопасности в{Наименование МО}понимается совокупность средств регистрации и учета событий безопасности всех СЗИ, операционных систем и прикладного программного обеспечения в{Наименование МО}.

8.2. Система регистрации и учета событий безопасности, а также информация, хранящаяся в электронных журналах регистрации событий сами по себе являются объектами защиты. Администратор 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 Администратору.

8.3. 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.

9. ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

9.1. Выявление уязвимостей в информационной системе осуществляется Администратором {Наименование МО}.

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

9.3. В случае проведения сканирований, для которых необходимо предоставить сканеру безопасности учетные данные в системе, создается отдельная учетная запись с минимально необходимыми правами. Вводить данные уже существующей учетной записи в сканер безопасности категорически запрещено.

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

9.5. С целью оперативного устранения известных уязвимостей на серверах и АРМ информационной системы настраивается обновление в автоматическом режиме компонентов операционных систем, прикладного программного обеспечения и средств защиты информации.

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

10.1. В {Наименование МО}с целью обеспечения целостности и доступности защищаемой информации применяется резервное копирование.

10.2. Резервное копирование баз данных производится*(пример: вручную Администратором наавтономный съемный носитель информации)*. Резервное копирование в места, где не представляется возможность обеспечить или проконтролировать наличие должной системы защиты информации (например, в облачные хранилища), запрещено.

10.3. Перечень ресурсов, подлежащих резервному копированию, а также периодичность резервного копирования той или иной информации утверждаются внутренними документами {Наименование МО} и должны актуализироваться Администратором по мере необходимости.

10.4. Процедуры резервного копирования проводятся в нерабочее время, либо во время наименьшей нагрузки на информационные системы.

10.5. 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.

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

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

10.8. Восстановление информации из резервной копии производится Администратором 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 информационным системам в результате инцидента информационной безопасности.

10.9. 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.

10.10. 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{Наименование МО}предусмотрены источники бесперебойного питания на АРМ Пользователей.

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

11.1. Администратор присутствует в процессе установки, обновления, настройки программного обеспечения в{Наименование МО}(в том числе и средств защиты информации) сотрудниками сторонних организаций.

11.2. Администратор присутствует в процессе ремонта технических средств{Наименование МО}сотрудниками сторонних организаций на территории {Наименование МО}. 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.

11.3. 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 {Наименование МО}
от «___» _____20__г. № ___

Инструкция ответственного за организацию обработки персональных данных в {Наименование МО}

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных в {Наименование МО} (далее – Ответственный) назначается приказом главного врача{Наименование МО} (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 сегментаЕГИСЗ, 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;
- контроль изменений в процессах обработки ПДн и, в случае необходимости, отправка информации об этих изменениях в уполномоченный территориальный орган по защите прав субъектов персональных данных (Роскомнадзор) с целью актуализации уведомления {Наименование МО} в реестре операторов ПДн;
- рассмотрение предложений по совершенствованию действующей системы защиты ПДн, предоставленных Администратором, назначаемым приказом руководителя {Наименование МО};
- 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 ПДнв соответствии с утвержденным приказом главного врача{Наименование МО} 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 вУчреждении.

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{Наименование МО} 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.