УТВЕРЖДЕНА
приказом МБОУ «СОШ №15»
с. Кронштадтка
от «31» июля 2018г. № 38

Инструкция администратора безопасности в ГИС «ФРДО» МБОУ СОШ №15

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности в ГИС «ФРДО» (далее – Администратор) назначается приказом директора МБОУ «СОШ №15» с. Кронштадтка и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе ее обработки в ГИС «ФРДО».

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.

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 директору и имеет право требовать от пользователей ГИС 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 ГИС «ФРДО»

2.1. Изучение особенностей технологических процессов обработки информации в МБОУ «СОШ №15» с. Кронштадтка с целью принятия решения о необходимости защиты информации в ГИС и классификации ГИС, либо поиск специализированных организаций, производящих на договорной основе такой анализ. В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации о ГИС 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 ГИС», 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 ГИС;
- существенное изменение условий функционирования ГИС, 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 ГИС (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 ГИС.

2.6. Участие в реализации проекта по защите информации в ГИС (тестирование системы защиты информации, внедрение системы защиты информации, аттестация ГИС по требованиям к защите информации, ввод в действие аттестованной ГИС).

2.7. Выработка предложений директору МБОУ «СОШ №15» с. Кронштадтка по совершенствованию системы защиты информации в ГИС.

2.8. Ведение учета применяемых в ГИС средств защиты информации (в том числе криптосредств), эксплуатационной и технической документации к ним.

2.9. Знание состава, структуры, назначения и выполняемых задач ГИС, 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 ГИС и по защите периметра информационной системы. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в ГИС и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости.

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

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

2.14. Организация учета съемных носителей информации. Настройка соответствующих программных механизмов средств защиты информации для запрета неучтенных съемных носителей. Ведение журнала учета съемных носителей.

2.15. Организация учета иных машинных носителей информации.

2.16. Проведение инструктажей сотрудников, работающих с защищаемой информацией в ГИС (далее – Пользователи ГИС), по темам: правила работы в ГИС, защита информации в ГИС, положения законодательства в сфере защиты информации и персональных данных, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников МБОУ «СОШ №15» с. Кронштадтка в вопросах информационной безопасности.

2.17. Организация первоначального доступа пользователям ГИС к ресурсам информационный системы в соответствии с утвержденным положением о

разграничении прав доступа в ГИС. Блокировка учетных записей, изменение полномочий пользователей и добавление новых пользователей ГИС в соответствии с Инструкцией о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ГИС, утвержденной в МБОУ «СОШ №15» с. Кронштадтка

2.18. Осуществление резервного копирования защищаемой в соответствии разделом 11 настоящей Инструкции.

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

2.20. Участие в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности, внесение по результатам таких расследований предложений по совершенствованию системы безопасности. 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.

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

2.22. В случае получения от Пользователей ГИС 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.

2.23. Обеспечение отсутствия на АРМ Пользователей ГИС 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.

2.24. Выявление уязвимостей ГИС посредством периодического сканирования системы сертифицированным сканером безопасности. Принятие решений на основании итогов каждого сканирования.

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

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

2.27. Обеспечение функционирования и поддержания работоспособности в ГИС:

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

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

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

3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ГИС

Администратор имеет право:

3.1. Знакомиться с нормативными актами МБОУ «СОШ №15» с. Кронштадтка, регламентирующими процессы обработки и защиты ПДн и иной конфиденциальной информации.

3.2. Вносить предложения директору МБОУ «СОШ №15» с. Кронштадтка по совершенствованию существующей системы защиты информации.

3.3. Требовать от Пользователей ГИС соблюдения требований Инструкции пользователя ГИС 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 ГИС, как в целом, так и отдельных Пользователей ГИС, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ГИС.

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

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

4.1. Одним из ключевых элементов системы защиты информации в ГИС «ФРДО» 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. На АРМ Администратора устанавливаются средства централизованного управления: антивирусной защитой ГИС, средством защиты информации от несанкционированного доступа в ГИС. Также на АРМ Администратора устанавливается сканер уязвимостей.

4.4. Администратор осуществляет централизованное управление политиками безопасности в ГИС, обновлениями средств защиты информации, обновлениями антивирусных баз и сигнатур, конфигурацией информационной системы. Также Администратор централизованно осуществляет периодическое сканирование уязвимостей ГИС.

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

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

5. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИАНИРОВАННОГО ДОСТУПА DALLAS LOCK 8.0-K

5.1. Администратор участвует в развертывании средства защиты информации от несанкционированного доступа (далее – СЗИ от НСД) в ГИС 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-K согласно утвержденному Положению о разграничении доступа. Идентификации и аутентификации подлежат как пользователи, так и учетные записи служб, приложений, программных процессов.

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

5.4. 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 стационарного или 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 пользователям под роспись в Журнале учета приема/выдачи съемных машинных носителей информации. Дата сдачи машинного носителя также фиксируется в Журнале. Администратор средствами СЗИ от НСД Dallas Lock 8.0-K реализует запрет использования неучтенных машинных носителей в ГИС.

5.5. Администратор осуществляет управление учетными записями с помощью встроенных механизмов ОС и с помощью механизмов СЗИ от НСД Dallas Lock

8.0-K. В процессе управления учетными записями 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.);
- объединение учетных записей в группы (при необходимости);
- проводит верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
- проводит анализ необходимости тех или иных полномочий в системе для учетных записей служб и приложений;
- 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;
- уничтожает временные учетные записи пользователей, предоставленные для однократного (или ограниченного по времени) выполнения задач в ГИС, и учетные записи уволенных сотрудников;
- осуществляет настройку прав доступа пользователей к ресурсам ГИС средствами СЗИ от НСД Dallas Lock 8.0-K в соответствии с утвержденным Положением о разграничении доступа;
- средствами СЗИ от НСД Dallas Lock 8.0-K настраивает автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования более 90 дней.

5.6. Администратор запрещает средствами СЗИ от НСД Dallas Lock 8.0-K любые действия пользователя в ГИС до прохождения процедур идентификации и аутентификации, в том числе ограничивает доступ к настройкам BIOS/UEFI. Администратору информационной безопасности до идентификации и аутентификации разрешаются следующие действия с целью диагностики проблем на элементах ГИС и восстановления работоспособности элементов ГИС:

- загрузка операционной системы в безопасном режиме;
- восстановление операционной системы с последней работоспособной конфигурацией;
- 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.

5.7. Администратор является ответственным за хранение, выдачу, инициализацию средств аутентификации (аппаратных ключей, учетных записей, первичных паролей). Администратор с помощью механизмов СЗИ от НСД Dallas Lock 8.0-K определяет парольную политику и требования к сложности паролей.

Администратор выдает пользователю пароль для первоначального входа в ГИС. СЗИ от НСД требует от пользователя сменить пароль при первом же входе в систему. 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 ГИС после смены пароля Администратором. Администратор не должен и не обязан знать пароли пользователей ГИС. В ГИС средствами СЗИ от НСД Dallas Lock 8.0-K 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;
- минимальное время действия пароля – 10 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.

5.8. Администратор с помощью механизмов СЗИ от НСД Dallas Lock 8.0-K устанавливает временной промежуток в 15 минут в качестве допустимого времени бездействия пользователя. После истечения указанного времени происходит блокировка сеанса пользователя.

5.9. Администратор средствами СЗИ от НСД Dallas Lock 8.0-K запрещает пользователям самостоятельную установку любого программного обеспечения. В МБОУ «СОШ №15» с. Кронштадтка утверждается перечень разрешенного к установке в ГИС программного обеспечения. Перечень разрешенного к установке программного обеспечения определяется исходя из целей и задач, решаемых с помощью ГИС. Перечень разрешенного к установке в ГИС программного обеспечения подлежит периодическому пересмотру. Установка разрешенного программного обеспечения производится либо Администратором лично, либо в присутствии Администратора и под контролем Администратора.

5.10. Механизмами СЗИ от НСД Dallas Lock 8.0-K Администратор устанавливает правила использования интерфейсов ввода/вывода технических средств ГИС. СЗИ от НСД настраивается таким образом, чтобы пользователь ГИС получал доступ к использованию только тех интерфейсов ввода/вывода, которые необходимы ему для выполнения служебных обязанностей.

6. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ И 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 ГИС только по определенному Администратором маршруту и изменение (перенаправление) маршрута передачи информации.

6.3. Администратор осуществляет настройку сетевого оборудования или контролирует этот процесс.

6.4. Администратор анализирует технологические процессы обработки информации, а также особенности функциональных обязанностей сотрудников МБОУ «СОШ №15» с. Кронштадтка для оптимизации настроек средств межсетевого экранирования. Средство межсетевого экранирования настраивается по принципу разрешения только тех ресурсов, сетевых портов и протоколов, необходимых для нормального функционирования ГИС и МБОУ «СОШ №15» с. Кронштадтка в целом.

6.5. Администратор организует взаимодействие с информационными системами сторонних организаций.

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

6.7. 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).

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. Исходя из требований к защите информации и актуальных угроз безопасности информации в ГИС, Администратор определяет необходимость использования средств криптографической защиты информации (далее – СКЗИ) в системе защиты информации ГИС.

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

7.4. 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 ГИС.

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

7.6. 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.

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

7.8. Администратор производит инструктаж пользователей перед работой с СКЗИ. Отметка о проведении инструктажа проставляется в Журнале учета инструктажей по информационной безопасности в ГИС.

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

7.10. 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 ГИС. Факт проверки отражается в Журнале учета мероприятий по контролю обеспечения защиты информации в ГИС. Результат проверки отражается в Журнале периодического тестирования средств защиты информации в ГИС. Проверка каждого СКЗИ проводится не реже одного раза в месяц.

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

7.12. 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.

7.13. 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. Администратор осуществляет настройку и контроль функционирования системы антивирусной защиты в ГИС. Управление системой осуществляется централизованно, и только Администратор может осуществлять такую функцию. Антивирусная защита осуществляется на АРМ, серверах, мобильных технических средствах и иных точках доступа в ГИС.

8.2. Администратор централизованно настраивает время, периодичность и другие параметры проведения полной антивирусной проверки узлов ГИС на наличие вредоносных компьютерных программ (вирусов) согласно «Плану мероприятий по обеспечению защиты информации в ГИС». Факт проверки отражается в «Журнале по учету мероприятий по контролю обеспечения защиты информации в ГИС».

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

9. РЕГИСТРАЦИЯ И УЧЕТ СОБЫТИЙ БЕЗОПАСНОСТИ

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

9.2. 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.

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. Для выявления уязвимостей в информационной системе используется сертифицированный сетевой сканер уязвимостей.

10.2. Сканирование ГИС 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.

10.3. 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.

10.4. В случае получения информации о новых уязвимостях, связанных с информационной системой, из открытых источников необходимо провести обновление базы данных об уязвимостях и провести внеплановое сканирование.

10.5. Администратор принимает меры по устранению или нейтрализации выявленных уязвимостей. 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.

10.6. 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.

10.7. Администратор не реже чем один раз в месяц осуществляет контроль состава технических средств, программного обеспечения и средств защиты

информации, а также корректности функционирования и настроек программного обеспечения и средств защиты информации.

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

11.1. В МБОУ «СОШ №15» с. Кронштадтка с целью обеспечения целостности и доступности защищаемой информации применяется резервное копирование.

11.2. Резервное копирование защищаемой информации, баз данных, образов операционных систем, конфигураций программного обеспечения производится Администратором с помощью стандартных средств Windows (создание образа системы, архивация и восстановление, в ручную) на учтенный съемный носитель. 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 Администратором по мере необходимости.

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

11.5. Для возможности оперативного восстановления информации 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. 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.

11.8. 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 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 в ручную или из предварительно сохраненных в резервную копию конфигураций.

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 ГИС (в том числе и средств защиты информации) сотрудниками сторонних организаций.

12.2. Администратор присутствует в процессе ремонта технических средств ГИС сотрудниками сторонних организаций на территории МБОУ «СОШ №15» с. Кронштадтка. 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.