«УТВЕРЖДАЮ»
Директор МБОУ «СОШ № 18» НГО
_____И.В. Фомина
приказ от «29» июня 2018г. № 36-АХД

Политика информационной безопасности в МБОУ «СОШ № 18» НГО

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее - Политика) утверждается директором МБОУ «СОШ № 18» НГО и определяет мероприятия, процедуры и правила по защите информации в информационных системах МБОУ «СОШ № 18» НГО.

1.2. Положения настоящей Политики распространяются на следующие информационные системы МБОУ «СОШ № 18» НГО:

- ГИС «ФРДО»;

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей указанных в п. 1.2 информационных систем (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

1.4. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в МБОУ «СОШ № 18» НГО относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

1.5. Целями настоящей Политики являются:

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;
- предотвращение утечек защищаемой информации;
- мониторинг событий безопасности и реагирование на инциденты безопасности;
- нейтрализация актуальных угроз безопасности информации;
- выполнение требований действующего законодательства по защите информации.

1.6. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации,

информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

1.7. Настоящая Политика 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;
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2.1. В данном разделе настоящей Политики описаны технологические процессы обработки различных видов защищаемой информации в информационных системах МБОУ «СОШ № 18» НГО. Администраторы и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с соответствующими описаниями технологических процессов обработки информации, приведенных в данном разделе.

2.2. Технологический процесс обработки персональных данных учащихся в МБОУ «СОШ № 18» НГО:

В рамках получения государственных услуг заявители предоставляют свои персональные данные в документальном виде сотрудникам образовательной организации. При выдаче документа об образовании и (или) о квалификации, документа об обучении, данные о выпускнике и документе об образовании и (или) о квалификации, документе об обучении вносятся в ГИС «ФРДО».

ГИС «ФРДО» состоит из 1 автоматизированного рабочего места или локальной сети, имеющей одноточечный выход в сети общего пользования и международного телекоммуникационного обмена.
Задачей информационной системы является отправка данных на веб портал в ЦОД ФИС «ФРДО».
Основным программным обеспечением, которое используется в работе для обработки данных является Microsoft Office и браузер. Персональные данные вносятся путем ручного ввода оператором с бумажного носителя в электронную форму. Файлы с данными формируются при помощи прикладного программного обеспечения Microsoft Office и подписываются электронно-цифровой подписью. Отправка данных организована в виде веб-формы, просматриваемой в браузере. Для передачи защищаемой информации на веб портал ФИС «ФРДО», находящийся по адресу http://10.3.47.15, используется СКЗИ ViPNet Client. Физически все введённые данные хранятся в ЦОД ФИС «ФРДО».

3. ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ГИС, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ГИС

3.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику МБОУ «СОШ № 18» НГО, допущенному к работе с ресурсами ГИС «ФРДО» присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ГИС.

3.2. Под учетной записью Пользователя понимается учетная запись для доступа к автоматизированному рабочему месту. В ГИС применяется дополнительное разграничение доступа при доступе к порталу ФИС «ФРДО».

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

3.4. Процедура регистрации (создания учетной записи и выдачи при необходимости электронного ключа) пользователя ГИС для сотрудника МБОУ «СОШ № 18» НГО, и предоставления ему (или изменения его) прав доступа к ресурсам ГИС инициируется заявкой директора подразделения, в котором работает этот сотрудник. Форма заявки приведена в Приложении № 1 к настоящей Политике. В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ГИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ГИС ранее зарегистрированного пользователя);
- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ГИС);

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

3.5. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации, описанным в разделе 2 настоящей Политики. Допуск Пользователей к обработке информации в ГИС производится на основании завизированной Администратором заявки, составленной по форме, приведенной в Приложении № 1 к настоящей Политике. При визировании очередной заявки Администратор осуществляет актуализацию следующих документов:

- положение о разграничении прав доступа в ГИС (при необходимости, Приложение № 2 к настоящей Политике);
- Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ГИС «ФРДО» (Приложение № 3 к настоящей Политике).

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

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

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

3.9. В качестве модели разграничения доступа к ресурсам ГИС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ГИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ГИС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации, описанных в разделе 2 настоящей Политики. Описание всех возможных ролей в ГИС приведено в Приложении № 2 к настоящей Политике. Помимо учетных записей Пользователей доступ к системе получают различные системные службы и процессы.

3.10. Перечень лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами ГИС и сопоставляемые им роли приведены в Приложении № 3 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.11. Перечень помещений, в которых разрешена работа с ресурсами ГИС, расположены технические средства ГИС, а также перечень лиц, допущенных в эти помещения приведен в Приложении № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.12. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети МБОУ «СОШ № 18» НГО на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.

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

4. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

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

4.2. С целью управления информационными потоками внутри периметра защищаемой сети МБОУ «СОШ № 18» НГО на всех сетевых устройствах (включая сетевые адаптеры АРМ Пользователей и серверов) прописываются статические маршруты. Перечень статических маршрутов приведен в Приложении № 5 к настоящей политике.

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

4.4. Контроль и фильтрация информационных потоков между ГИС «ФРДО» и внешними телекоммуникационными сетями осуществляется с помощью межсетевого экрана ViPNet Client.

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

ресурсов с вредоносным содержимым при выборе политики «Разрешено все, кроме явно запрещенного».

4.6. С целью реализации политики контроля и фильтрации информационных потоков между ГИС «ФРДО» и внешними телекоммуникационными сетями «Блокировать все, кроме явно разрешенного» утверждается список разрешающих правил взаимодействия с внешними телекоммуникационными сетями, приведенный в Приложении № 6 к настоящей Политике. Данный список может быть дополнен на основании служебной записки Администратору с указанием обоснования добавления того или иного ресурса/сайта/протокола/порта в список разрешенных.

4.7. Администратор обеспечивает соответствие настроек межсетевого экрана ViPNet Client, приведенному в Приложении № 6 к настоящей Политике списку разрешительных правил.

5. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

5.1. В ГИС «ФРДО» разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

5.2. Перечень разрешенного программного обеспечения в ГИС «ФРДО» определен в Приложении № 7 к настоящей Политике.

5.3. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением № 7. Пользователям запрещена установка любого ПО в ГИС «ФРДО».

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

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

6. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

6.1. Одной из основных целей злоумышленников являются машинные носители информации, используемые в ГИС «ФРДО» для хранения и обработки защищаемой информации. Исходя их этого, защита машинных носителей информации (как в стационарных АРМ и серверах, так и мобильных/съемных) является ключевым звеном политики информационной безопасности МБОУ «СОШ № 18» НГО.

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

6.3. В МБОУ «СОШ № 18» НГО учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные подобные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

6.4. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

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

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

6.7. Использование неучтенных съемных носителей и/или портативных устройств (в том числе личных) в ГИС «ФРДО» запрещено.

6.8. Невозможность использования неучтенных съемных носителей информации обеспечивается путем программных настроек СЗИ от НСД Dallas Lock 8.0-K. Настройками Dallas Lock 8.0-K неучтенные носители информации блокируются на всех стационарных устройствах ГИС. Попытки использования неучтенных съемных носителей информации фиксируются средствами Dallas Lock 8.0-K. Такие попытки являются инцидентами безопасности и расследуются в установленном порядке.

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

6.10. Невозможность использования неучтенных машинных носителей в стационарных устройствах обеспечивается путем физического контроля

доступа в соответствии с инструкциями Пользователя и Администратора, а также путем проведения периодических мероприятий по инвентаризации ресурсов ГИС и комплектности технических средств.

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

- возвращения учтенного съемного носителя информации Администратору;
- при вводе в эксплуатацию нового машинного носителя или технического средства со встроенными носителями информации;
- при передаче носителя информации в сторонние организации (в том числе и для проведения ремонта технического средства);
- при утилизации технических средств.

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

6.13. При возвращении учтенного съемного носителя информации Пользователем, а также при вводе в эксплуатацию нового машинного носителя, информация уничтожается путем использования механизма СЗИ от НСД Dallas Lock 8.0-K затирания файлов случайной битовой последовательностью.

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

6.15. В случаях уничтожения информации способами, описанными в пунктах 6.19 и 6.20 настоящей Политики, Администратор фиксирует факт уничтожения информации, а также факт контроля уничтожения информации в Журнале учета мероприятий по защите информации в ГИС «ФРДО».

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

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

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

7.1. В МБОУ «СОШ № 18» НГО осуществляется взаимодействие со следующими внешними информационными системами:

- ФИС «ФРДО»;

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

7.3. Порядок обработки, хранения и передачи информации с использованием внешних информационных систем определяются технологическими процессами обработки информации, описанными в разделе 2 настоящей Политики.

7.4. Разрешение обработки, хранения и передачи информации с использованием внешних информационных систем в МБОУ «СОШ № 18» НГО возможно только при выполнении следующих условий:

- при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;
- при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

8. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

8.1. В МБОУ «СОШ № 18» НГО в качестве средства выявления уязвимостей используется сертифицированный сканер уязвимостей.

8.2. Администратор не реже одного раза в месяц проводит полное сканирование системы на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ГИС «ФРДО» производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.

8.3. Администратор изучает отчеты по результатам сканирования и принимает решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться ГРИИБ.

8.4. Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

8.5. При выявлении уязвимостей, Администратор анализирует системные журналы и журналы средств защиты информации, на предмет выявления

эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.

8.6. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом директора МБОУ «СОШ № 18» НГО.

9. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.1. С целью противодействия эксплуатации известных уязвимостей, в МБОУ «СОШ № 18» НГО устанавливаются правила и процедуры контроля установки обновлений системного и прикладного программного обеспечения.

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

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

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

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

9.6. Администратор в соответствии с эксплуатационной документацией на программное обеспечение осуществляет проверку установки обновлений, а также корректность установки обновлений. В МБОУ «СОШ № 18» НГО должно применяться только такое программное обеспечение, которое поддерживает проверку целостности файлов обновлений.

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

9.8. Обновление микропрошивок и программного обеспечения BIOS/UEFI производится только при поступлении информации о критичных уязвимостях в таком программном обеспечении, применяемом в МБОУ «СОШ № 18» НГО.

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

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

10.2. В случае добавления новых ТС, ПО и СрЗИ в состав ГИС «ФРДО» или удаления существующих компонентов, на основании акта ввода в

эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

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

10.4. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ГИС «ФРДО» является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

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

10.6. Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом директору МБОУ «СОШ № 18» НГО, который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

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

11.1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ГИС «ФРДО» осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 10 к настоящей Политике.

11.2. Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ГИС «ФРДО».

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

11.4. Нештатными ситуациями являются:

- разглашение информации ограниченного доступа сотрудниками МБОУ «СОШ № 18» НГО, имеющими к ней право доступа, в том числе:
  - разглашение информации лицам, не имеющим права доступа к защищаемой информации;
  - передача информации по незащищенным каналам связи;
  - обработка информации на незащищенных технических средствах обработки информации;

    - опубликование информации в открытой печати и других средствах массовой информации;
    - передача носителя информации лицу, не имеющему права доступа к ней;
    - утрата носителя с информацией.
- неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
    - несанкционированное изменение информации;
    - несанкционированное копирование информации;
- несанкционированный доступ к защищаемой информации:
    - несанкционированное подключение технических средств к средствам и системам ГИС «ФРДО»;
    - использование закладочных устройств;
    - использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ГИС «ФРДО»;
    - использование злоумышленником уязвимостей программного обеспечения ГИС;
    - использование злоумышленником программных закладок;
    - заражение ГИС злоумышленником программными вирусами;
    - хищение носителей информации;
    - нарушение функционирования технических средств обработки информации;
    - блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
- дефекты, сбои, отказы, аварии технических средств и систем ГИС;
- дефекты, сбои, отказы программного обеспечения ГИС;
- сбои, отказы и аварии систем обеспечения ГИС;
- природные явления, стихийные бедствия:
    - термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
    - механические факторы (повреждения зданий, землетрясения и т. д.);
    - электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

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

11.6. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 11 настоящей Политики.

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

11.8. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации

по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

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

- корректное отключение технических средств ГИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ГИС а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

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

- Пользователи корректно отключают и обесточивают свои рабочие места;
- системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;
- Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ГИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
- **в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.**

Приложение № 1 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

ЗАЯВКА
на внесение изменений в списки пользователей
и наделение пользователей полномочиями доступа к ресурсам ГИС

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

_____
(должность с указанием подразделения)

_____
(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)
(нужное подчеркнуть)

для решения задач:

_____
(список задач согласно формуляров задач)

_____

_____

_____

_____

_____

Начальник

_____
(наименование заказывающего подразделения)

«___» _____ 20__ г. _____ _____
(подпись) (фамилия)

Согласовано Администратор безопасности

«___» _____ 20__ г. _____ _____
(подпись) (фамилия)

ЗАДАНИЕ
на внесение изменений в списки пользователей ГИС

Администратору безопасности информации

_____
(фамилия и инициалы исполнителя)

Произвести изменения в списках пользователей

Директор МБОУ «СОШ № 18» НГО

_____ Фомина Ирина Владимировна

«___» _____ 20__ г.

Обратная сторона заявки

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

Наименование задач

Администратор безопасности Векслер Оксана Анатольевна

Имя учетной записи и начальное значение пароля получил, о порядке смены пароля при первом входе в систему проинструктирован, с инструкцией Пользователя ГИС ознакомлен

Пользователь

_____
(подпись, фамилия)

«___» _____ 20__ года

Приложение № 2 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

Положение о разграничении прав доступа в ГИС «ФРДО»

Исходя из характера и режима обработки защищаемой информации в ГИС «ФРДО» определяется следующий перечень групп Пользователей, служб и процессов, участвующих в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам ГИС приведен в таблице.

Роль	**Описание параметров доступа к ресурсам ГИС для данной роли**
Администратор безопасности	Полный доступ к ресурсам ГИС, настройкам ОС и СЗИ. Полный доступ к системным журналам, журналам средств защиты информации и другим электронным журналам сообщений.
Системный администратор	Полный доступ к ресурсам ГИС за исключением доступа к настройкам СЗИ и к журналам средств защиты информации.
Оператор	Доступ на запись и чтение персональных данных при работе. Учетным записям с этой ролью разрешен доступ со следующих устройств: АРМ 1;

Приложение № 3 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ГИС «ФРДО»

Настоящий Перечень устанавливает перечень лиц, должностей и процессов, допущенных к работе с ресурсами ГИС «ФРДО». Для каждого элемента списка в таблице обязательно указываются ФИО (Имя службы или процесса для неодушевленных субъектов доступа), должность (только для одушевленных субъектов доступа), имя присвоенной учетной записи и роль (в соответствии с Положением о разграничении прав доступа в ГИС). Тип и серийный номер выданного идентификатора указываются только при выдаче пользователю электронного ключа. Роспись о получении электронного ключа ставится только при выдаче пользователю такого ключа.

В настоящем Перечне не отражены вопросы, связанные с использованием средств криптографической защиты информации (СКЗИ). Перечни пользователей СКЗИ, а также иные учетный данные, связанные с СКЗИ приведены в других журналах и перечнях.

№ п/п	ФИО сотрудника / Имя службы или процесса	Должность	Имя присвоенной учетной записи	Роль	Выдан эл. ключ	Роспись о получении эл. ключа
1.	Фомина Ирина Владимировна	Директор	школа	Оператор	-	-
2.	Голоцван Светлана Ивановна	Заместитель директора по УВР	user	Оператор	-	-
3.	Векслер Оксана Анатольевна	Диспетчер образовательного учреждения	AdminSec	Администратор безопасности	-	-
			user2	Оператор	-	-

Приложение № 4 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

Перечень помещений, в которых разрешена работа с ресурсами ГИС «ФРДО», в которых размещены технические средства ГИС, а также перечень лиц, допущенных в эти помещения

№ п/п	Название/номер помещения	Техническое средство ГИС						Сотрудники, допущенные в помещение	
		Тип	Модель	Учетный № (серийный, инвентарный)	Сетевое имя	IP-адрес	MAC-адрес	ФИО	Должность
1.	«Приемная»	Компьютер	Velton	б/н	ШКОЛА-ПК	DHCP	00-1E-90-B4-F2-7B	Фомина Ирина Владимировна	Директор
								Голоцван Светлана Ивановна	Заместитель директора по УВР
								Векслер Оксана Анатольевна	Диспетчер образовательного учреждения

Приложение № 5 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

Перечень статических сетевых маршрутов в ГИС «ФРДО»

№ п/п	Сеть	Маска подсети	Шлюз по умолчанию	Метрика	Где применяется
1.	0.0.0.0	0.0.0.0	192.168.0.1	20	АРМ Пользователей
2.	127.0.0.0	255.0.0.0	192.168.0.1	306	
3.	127.0.0.1	255.255.255.255	192.168.0.1	306	
4.	127.255.255.255	255.255.255.255	192.168.0.1	306	
5.	192.168.0.0	255.255.255.0	192.168.0.1	276	
6.	192.168.0.101	255.255.255.255	192.168.0.1	276	
7.	192.168.0.255	255.255.255.255	192.168.0.1	276	
8.	224.0.0.0	224.0.0.0	192.168.0.1	306	
9.	224.0.0.0	224.0.0.0	192.168.0.1	276	
10.	255.255.255.255	255.255.255.255	192.168.0.1	306	
11.	255.255.255.255	255.255.255.255	192.168.0.1	276	
12.	10.0.0.0	255.255.255.0	10.10.0.1	306	с ViPNet Client

Приложение № 6 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

Список разрешающих правил взаимодействия с внешними телекоммуникационными сетями в ГИС «ФРДО»

№ п/п	IP/URL ресурса, подсеть или протокол	Обоснование разрешения	Правило	Время действия правила	Учетные записи, устройства, процессы, для которых действует правило
Фильтры защищенной сети					
1.	Протокол: DHCP	Правило необходимо для автоматического получения IP-адреса	Разрешить входящие и исходящие соединения по протоколу: DHCP	Круглосуточно	Пользователи ViPNet Client
2.	Протоколы: NetBIOS-DGM, NetBIOS-NC	Правило необходимо для работы в локальных сетях	Разрешить входящие и исходящие соединения по протоколам: NetBIOS-DGM, NetBIOS-NC	Круглосуточно	Пользователи ViPNet Client
3.	Протоколы: ViPNet базовый, ViPNet StateWatch, ViPNet MFTP	Правило необходимо для корректной работы средства криптографической защиты ViPNet Client	Разрешить входящие и исходящие соединения по протоколам: ViPNet базовый, ViPNet StateWatch, ViPNet MFTP	Круглосуточно	Пользователи ViPNet Client
4.	Протокол: ICMP	Правило необходимо для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных	Разрешить входящие и исходящие соединения по протоколу: ICMP	Круглосуточно	Пользователи ViPNet Client
5.	Протокол: RDP	Правило необходимо для обеспечения удалённой работы пользователя с сервером, на котором запущен сервис терминальных подключений	Разрешить входящие и исходящие соединения по протоколу: RDP	Круглосуточно	Пользователи ViPNet Client
6.	Протокол: IGMP	Правило необходимо для управления групповой передачей данных в сетях	Разрешить входящие и исходящие соединения по протоколу: IGMP	Круглосуточно	Пользователи ViPNet Client
7.	Протоколы: SIP, SCCP, H323	Правило необходимо для управления передачей мультимедийного трафика в сетях,	Разрешить входящие и исходящие соединения по протоколам: SIP, SCCP, H323	Круглосуточно	Пользователи ViPNet Client

№ п/п	IP/URL ресурса, подсеть или протокол	Обоснование разрешения	Правило	Время действия правила	Учетные записи, устройства, процессы, для которых действует правило
8.	Весь трафик	Правило необходимо для передачи данных через средство криптографической защиты ViPNet Client	Разрешить входящие и исходящие соединения 55777/UDP	Круглосуточно	Пользователи ViPNet Client
Фильтры открытой сети					
9.	Протокол: DHCP	Правило необходимо для автоматического получения IP-адреса	Разрешить входящие и исходящие соединения по протоколу: DHCP	Круглосуточно	Все пользователи
10.	Протоколы: NetBIOS-DGM, NetBIOS-NC	Правило необходимо для работы в локальных сетях	Разрешить входящие и исходящие соединения по протоколам: NetBIOS-DGM, NetBIOS-NC	Круглосуточно	Все пользователи
11.	Протокол: IGMP	Правило необходимо для управления групповой передачей данных в сетях	Разрешить входящие и исходящие соединения по протоколу: IGMP	Круглосуточно	Все пользователи
12.	Протокол: ICMP	Правило необходимо для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных	Разрешить входящие и исходящие соединения по протоколу: ICMP	Круглосуточно	Все пользователи
13.	Исходящий трафик	Правило необходимо для доступ пользователя в Интернет	Разрешить исходящие соединения	Круглосуточно	Все пользователи

Приложение № 7 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

Список разрешенного программного обеспечения в ГИС «ФРДО»

№ п/п	Наименование ПО	Тип ПО	Цель применения ПО в ГИС	Место установки компонентов ПО
1.	Windows 7 Максимальная	Операционная система	Обеспечение работы АРМ Пользователей	АРМ 1
2.	Microsoft Office 2007	Прикладное	Набор приложений, предназначенных для обработки электронной документации: тексты, электронные таблицы, базы данных	АРМ 1
3.	Coogle Chrome	Прикладное	Программа для просмотра веб-страниц; документов HTML, содержания веб-документов	АРМ 1
4.	Adobe Reader XI	Прикладное	Программа для редактирования и чтения файлов в формате PDF	АРМ 1
5.	«ФЛАК ОО-1»	Прикладное	Программное средство необходимое в образовательной деятельности организации	АРМ 1
6.	Сверка ИС и Перечней	Прикладное	Программное средство необходимое в образовательной деятельности организации	АРМ 1
7.	FastStone Image Viewer 4.9 Final Corporate	Прикладное	Программа для просмотра и изменения графических файлов	АРМ 1
8.	CCleaner	Прикладное	Программа для очистки и оптимизации графических файлов	АРМ 1
9.	«Флак 83-РИК»	Прикладное	Программное средство необходимое в образовательной деятельности организации	АРМ 1
10.	WinRAR	Прикладное	Программа для создания и управления архивами	АРМ 1
11.	Megafon Internet	Прикладное	Средство для подключения к сети Интернет	АРМ 1
12.	7-Zip	Прикладное	Программа для создания и управления архивами	АРМ 1
13.	PotPlayer	Прикладное	Мультимедийный проигрыватель	АРМ 1
14.	K-Lite Mega Codec Pack	Прикладное	Мультимедийный проигрыватель	АРМ 1
15.	Dr. Web Security Space	Средство защиты информации	Средство обеспечения антивирусной защиты	АРМ 1
16.	ViPNet Client 4.3	Средство защиты информации	Средство криптографической защиты информации и средство межсетевого экранирования	АРМ 1

№ п/п	Наименование ПО	Тип ПО	Цель применения ПО в ГИС	Место установки компонентов ПО
17.	Dallas Lock 8.0K	Средство защиты информации	Система защиты конфиденциальной информации от несанкционированного доступа в процессе её хранения и обработки	АРМ 1

Приложение № 8 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

Порядок резервирования информационных ресурсов в ГИС «ФРДО»

№ п/п	Наименование информационного ресурса	Место размещения ресурса в системе	Вид резервного копирования	Ответственный за резервное копирование	Место хранения резервной копии	Частота резервного копирования
1.	Образ пользовательской операционной системы	АРМ 1	Образ системы, периодическое	Администратор информационной безопасности	Учтённый съёмный носитель	По мере внесения существенных изменений в состав пользовательской операционной системы
2.	Средство криптографической защиты информации ViPNet Client	АРМ 1	Эталонный дистрибутив	Администратор информационной безопасности	Сейф администратора безопасности информации	Единовременно

Приложение № 9 к Политике информационной
безопасности в МБОУ «СОШ № 18» НГО,
утвержденной приказом
от «___» _____20__г. № ___

План обеспечения непрерывности функционирования ГИС «ФРДО»

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

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

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

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	работоспособности ТС и ПО	Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	20 минут	1 день
22.	Дефекты, сбои, отказы, аварии ТС, программных средств и систем ГИС	Сбой ТС и систем ГИС	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	1 час	2 дня
		Отказ ТС и систем ГИС, затронувший работу группы пользователей	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день
		Отказ ТС и систем ГИС, затронувший работу одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	1 час	2 дня
		Авария ТС и систем ГИС	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
23.	Сбои, отказы и аварии систем обеспечения ГИС	Сбой систем обеспечения ГИС	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента	1 час	1 день
		Отказ систем обеспечения ГИС, затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	1 час	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
		Отказ систем обеспечения ГИС, затронувший работу одного пользователя	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента	1 час	2 дня
		Авария систем обеспечения ГИС	Ответственному за материально-техническое обеспечение, Администратору сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение, Администратору не позднее 8 часов после инцидента	1 час	1 день
24.	Природные явления, стихийные бедствия, несущие угрозу жизни человека		Директору, заместителям директора, которые оповещают всех своих сотрудников сразу после получения информации	Директору, заместителям директора, которые оповещают всех своих сотрудников сразу после получения информации	10 минут	30 минут
25.	Природные явления, стихийные бедствия, не несущие угрозу жизни человека		Директору, заместителям Директора, Администратору	Директору, заместителям Директора, Администратору	10 минут	1 час