УТВЕРЖДЕНА
Директором
МБОУ «СОШ №1»
_____ В.Г.Насырова

от «01» 09 2022 г. приказ № 124/1

Политика информационной безопасности в МБОУ «СОШ №1»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее - Политика) утверждается директором МБОУ «СОШ №1» и определяет мероприятия, процедуры и правила по защите информации в информационных системах МБОУ «СОШ №1».

1.2. Положения настоящей Политики распространяются на следующие информационные системы МБОУ «СОШ №1»:

- Программы Microsoft Office;
- Отдел Кадров Плюс 2018;
- Перечень льготных профессий;
- Программа Spu_orb;
- АИС Электронная школа;
- СУ ГосВеб;
- WEB-Торги-КС;
- ЕИС Закупок;
- База данных ЕГЭ;
- База данных ОГЭ;
- КТ-Аттестат;
- ИвАттестат.

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 №1» 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 или иных сообщений и так далее);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая 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 №1». 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 сотрудников МБОУ «СОШ №1»:

Все персональные данные работника Школы следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Директор Школы не имеет права получать и обрабатывать персональные данные работника Школы о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. Обработка указанных персональных данных работников возможна только с их согласия. Работник школы предоставляет секретарю школы достоверные сведения о себе. Секретарь Школы проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

2.3. Технологический процесс обработки персональных данных обучающихся на вакантные должности в МБОУ «СОШ №1»:

Все персональные данные учащегося Школы следует получать у его родителя (законного представителя).Директор Школы не имеет права получать и обрабатывать персональные данные Обработка персональных данных учеников возможна только с согласияего родителя (законного представителя).Родитель (законный представитель) предоставляет секретарю школы достоверные сведения о себе и учащемся. Секретарь Школы проверяет достоверность сведений, сверяя данные, предоставленные родителем (законным представителем), с имеющимися у родителя (законного представителя). документами.

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

3.1. В ИС в МБОУ «СОШ №1» 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.

3.2. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности. Пользователям запрещена установка любого ПО в ИС в МБОУ «СОШ №1».

3.3. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ИС 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.

3.4. Администратор ежемесячно проводит проверку соответствия состава программного обеспечения в ИС в МБОУ «СОШ №1» 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.

4. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, КОНТРОЛЬ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

4.1. Программист обеспечивает учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Учёту подлежат:
- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные 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)

4.2. Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации

4.3. Программист обеспечивает контроль перемещения используемых в информационной системе машинных носителей информации за пределы контролируемой зоны. При контроле перемещения машинных носителей информации должны осуществляться:

-определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны;

-предоставление права на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функций);

-учет перемещаемых машинных носителей информации;

-периодическая проверка наличия машинных носителей информации.

4.4. Программист обеспечивает уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

4.5. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

4.6. Программистом обеспечиваются регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации.

4.7. Программистом периодически проводится проверка процедур и тестирование средств стирания информации и контроля удаления информации.

4.8. Программист применяет следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:
- удаление файлов штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы;

- перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием;

- очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

- полная многократная перезапись машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

- размагничивание машинного носителя информации;

- физическое уничтожение машинного носителя информации (в том числе сжигание, измельчение, плавление, расщепление, распыление и другое).

5. РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА И ЗАЩИТА БЕСПРОВОДНЫХ СОЕДИНЕНИЙ

5.1. Для контроля использования и защиты имеющейся системы Wi-Fi установлен пароль входа в систему. Доступ открывает праграммист Школы по заявлению и разовому паролю. В остальное время зона доступа закрыта.

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

6.1. Взаимодействие Школы с информационными системами сторонних организаций осуществляется на основании договора с собственником, провайдером либо дистрибьютором.

7. ПРАВИЛА И ПРОЦЕДУРЫ ОБНАРУЖЕНИЯ (ПРЕДОТВРАЩЕНИЯ) ВТОРЖЕНИЙ

7.1. Для обнаружения и предотвращения вторжений в ИС МБОУ «СОШ №1» применяются следующие системы:
- установка антивирусной программы защиты ИС на ПК;
- установка провайдером сети Интернет системы блокировки;
- подключение функции автоматического выхода из системы при простое ПК;
- экстренный (ручной) выход из системы ПК.

8. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

8.1. В МБОУ «СОШ №1» в качестве средства выявления уязвимостей используется сертифицированная антивирусная программа.

8.2. Программист 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 ИС в МБОУ «СОШ №1» производится внеплановое обновление базы данных антивирусной программы и полное сканирование информационной системы.

8.3. Программист 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).

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, Программист 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, Программист уведомляет об этом директора МБОУ «СОШ №1».

9. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.1. Обновление программного обеспечения Школы осуществляется в автоматическом режиме. В случае невозможности автоматического обновления программного обеспечение, данная процедура выполняется вручную.

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) ИС в МБОУ «СОШ №1» фиксируется в Журнале разрешенного программного обеспечения.

10.2. В случае добавления новых ТС, ПО и СрЗИ в состав ИС в МБОУ «СОШ №1» или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Журнал разрешенного программного обеспечения.

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

10.4. Выявление несоответствия состава ТС, ПО и СрЗИ Журналу разрешенного программного обеспечения ИС в МБОУ «СОШ №1» является инцидентом безопасности. В случае выявления фактов несоответствия Программист устанавливает причины самостоятельно.

10.5. В случае выявления несоответствия состава ТС, ПО и СрЗИ, программист 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. Программист 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, Программист запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Программист сообщает об этом директору МБОУ «СОШ №1», 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 КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

11.1. контроль целостности средств защиты информации осуществляться по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

11.2. обеспечиваться контроль целостности средств защиты информации с использованием криптографических методов в соответствии с законодательством Российской Федерации, всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

11.3. сотрудниками обрабатывающими персональные данные исключаются возможности использования средств разработки и отладки программ во время обработки и (или) хранения персональных данных в целях обеспечения целостности программной среды.

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

12.1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ИС в МБОУ «СОШ №1» осуществляется в соответствии с инструкцией администратора безопасности информации.

12.2. Программист осуществляет проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ИС в МБОУ «СОШ №1».

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

12.4. Нештатными ситуациями являются:

- разглашение информации ограниченного доступа сотрудниками МБОУ «СОШ №1», 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 ИС в МБОУ «СОШ №1»;
  - использование закладочных устройств;
  - использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ИС в МБОУ «СОШ №1»;
  - использование злоумышленником уязвимостей программного обеспечения ИС;
  - использование злоумышленником программных закладок;
  - заражение ИС 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 ИС;
- дефекты, сбои, отказы программного обеспечения ИС;
- сбои, отказы и аварии систем обеспечения ИС;
- 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.).

12.5. 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.

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

12.7. 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.

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

- корректное отключение технических средств ИС 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 ИС 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.

12.9. 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;
- Программист предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ИС 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, Программист 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 №1»

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

Прошу зарегистрировать пользователя (исключить из списка пользователей, изменить полномочия пользователя) ИС

(нужное подчеркнуть)

_____

(должность)

_____

(фамилия имя и отчество сотрудника)

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

(нужное подчеркнуть)

для решения задач:

_____

(список задач согласно формуляров задач)

_____

_____

_____

_____

_____

«___» _____ 20__ г. _____ _____

(подпись) (фамилия)

Согласовано Администратор безопасности

«___» _____ 20__ г. _____ _____

(подпись) (фамилия)

Разрешено\Запрещено Директор МБОУ «СОШ №1»

«___» _____ 20__ г. _____ В.Г.Насырова

(подпись) (фамилия)

Приложение № 2 к Политике информационной
безопасности в МБОУ «СОШ №1»

Положение о разграничении прав доступа в ИС в МБОУ «СОШ №1»

Исходя из характера и режима обработки защищаемой информации в ИС в МБОУ «СОШ №1»определяется следующий перечень групп Пользователей, служб и процессов, участвующих в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам ИС приведен в таблице.

Роль	**Описание параметров доступа к ресурсам ИС для данной роли**
Администратор	Полный доступ
Заместитель администратор по АИС	Полный доступ
Заместитель администратора по ДИС	Полный доступ
Оператор АИС	Ограниченный доступ, достаточный для выполнения работ
Оператор ДИС	Ограниченный доступ, достаточный для выполнения работ

Приложение № 3 к Политике информационной
безопасности в МБОУ «СОШ №1»

Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ИС МБОУ «СОШ №1»

Настоящий Перечень устанавливает перечень лиц, должностей и процессов, допущенных к работе с ресурсами ИС МБОУ «СОШ №1». 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 ИС). 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	Роль
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			

Приложение № 4 к Политике информационной
безопасности в МБОУ «СОШ №1»

Перечень помещений, в которых разрешена работа с ресурсами ИС в МБОУ «СОШ №1», в которых размещены технические средства ИС, а также перечень лиц, допущенных в эти помещения

№п/п	Название/номер помещения	Техническое средство ИС			Сотрудники, допущенные в помещение	
		Тип	Модель	Учетный № (серийный, инвентарный)	ФИО	Должность
1.	Серверная	Сервер	HP xxxxxx	S/N: xxxxxxx	Иванов Иван Иванович	Специалист по защите информации
		Коммутатор	Cisco ASA xxxx	Инв.: xxxxxx	Петров Петр Петрович	Системный администратор
		СХД	HP xxxxxx	S/N: xxxxxxx		
2.	Бухгалтерия	Компьютер	HP xxxxxx	Инв.: xxxxxx	Сидорова Ольга Ивановна	Бухгалтер
		Ноутбук	Acer xxxxxxxx	S/N: xxxxxxx		
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						

Приложение № 5 к Политике информационной
безопасности в МБОУ «СОШ №1»
утвержденной приказом
от «___» _____20__г. № ___

Список разрешенного программного обеспечения в ИС МБОУ «СОШ №1»

№ п/п	Наименование ПО	Тип ПО	Цель применения ПО в ИС	Место установки компонентов ПО
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

Приложение № 6 к Политике информационной
безопасности в МБОУ «СОШ №1»

План обеспечения непрерывности функционирования ИС в МБОУ «СОШ №1»

№ 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 ИС 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 времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инциден-	10 минут в рабочее время (1 час в нерабочее)	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
				та		
8.	Маскировка под зареИСтрированного 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 зареИСтрированного 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

№ 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
		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
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,		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	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
	повлекшие утерю или повреждение защищаемой информации					
21.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	20 минут	2 дня
		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 ИС	Сбой ТС и систем ИС	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	1 час	2 дня
		Отказ ТС и систем ИС, 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 ИС, затронувший работу одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	1 час	2 дня
		Авария ТС и систем ИС	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
23.	Сбои, отказы и аварии систем обеспечения ИС	Сбой систем обеспечения ИС	Ответственному за материально- техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день по-	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
				сле инцидента		
		Отказ систем обеспечения ИС, 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
		Отказ систем обеспечения ИС, 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 ИС	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		Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	10 минут	30 минут
25.	Природные явления, стихийные бед-		Руководителю, за-	Руководителю,	10 минут	1 час

№ 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
	ствия, не несущие угрозу жизни человека		местителям Руководителя, Администратору	заместителям Руководителя, Администратору		