МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 12 С. ТЕРЕХОВКА НАДЕЖДИНСКОГО РАЙОНА» (МБОУ ООШ № 12)

ПРИКАЗ

27.08.2024 **№158-а**

с. Тереховка

О назначении ответственного за организацию обработки персональных данных и администратора безопасности в информационных системах МБОУ ООШ № 12, а также в Государственной информационной системе Приморского края «Региональное образование» В 2024-2025 учебном году

В соответствии с Федеральным законом от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», **ПРИКАЗЫВАЮ:**

1. Утвердить прилагаемую инструкцию администратора безопасности. (Приложение 1)
2. Утвердить Должностные инструкции Администратора АИС «Сетевой Город. Образование» (Приложение 2)
3. Утвердить Должностную инструкцию координатора, ответственного за методическое сопровождение педагогических работников по работе с АИС «Сетевой Город. Образование» (Приложение 3)
4. Утвердить и довести до сведения учителей, классных руководителей Комментарии к должностным обязанностям работников образовательных учреждений, связанные с использованием АИС «Сетевой Город. Образование» (Приложение 4).
5. Утвердить Правила пользования автоматизированной информационно-управляющей системой «Сетевой город. Образование» (приложение 5).
6. Ответственным за организацию обработки персональных данных Государственная информационная система Приморского края «Региональное образование» (далее ГИС РО) МБОУ ООШ № 12 назначить следующего сотрудника:

директора К.А. Фриз.

7. Ответственному за организацию обработки персональных данных обеспечить автоматизированную обработку персональных данных на объектах информатизации, удовлетворяющих действующему законодательству.
8. Назначить администратором ГИС РО – учителя Александрюк И.И.
9. Ответственным за организацию обработки персональных данных и администратору ГИС РО руководствоваться инструкцией ответственного за организацию обработки персональных данных.
10. Ответственному за организацию обработки персональных данных обеспечить неавтоматизированную обработку персональных данных в соответствии с действующим законодательством.
11. Администратором безопасности информации в информационных системах МБОУ ООШ № 12 назначить следующего сотрудника: учителя Александрюк И.И.

12. Назначить Координатором АИС «СГО» Абрамович Татьяну Владимировну, учителя, лицом ответственным за методическое сопровождение педагогических работников по работе с АИС «Сетевой Город. Образование».

13. Заместителю директора по УВР :

- организовать контроль над своевременностью и правильностью работы учителей-предметников и классных руководителей по информационному наполнению автоматизированной системы управления «Сетевой Город. Образование» согласно функциональным обязанностям.

13. Администратору АИС «Сетевой Город. Образование», Александрюк И.И.:

- обеспечить информационное наполнение и функционирование системы.

14. Учителям-предметникам и классным руководителям осуществлять систематическую работу с АИС «Сетевой Город. Образование» в соответствии с утвержденным Положением об автоматизированной системе «Сетевой город. Образование» (приложение 4), а также Правилами пользования автоматизированной информационно-управляющей системой «Сетевой город. Образование» (приложение 5).

15. Администратору безопасности в своей работе руководствоваться инструкцией администратора безопасности информационных систем МБОУ ООШ № 12.

16. Лицам, допущенным к обработке персональных данных при неавтоматизированной их обработке и хранении, руководствоваться документом «Правила обработки персональных данных без использования средств автоматизации».

17. Лицам, допущенным к обработке персональных данных в ГИС РО, при автоматизированной их обработке и хранении, руководствоваться следующими документами:

– политика информационной безопасности в МБОУ ООШ № 12;

– инструкция пользователя информационных систем МБОУ ООШ № 12.

18. Контроль за исполнением настоящего приказа оставляю за собой.

Директор **К.А. Фриз**

Приложение №1
УТВЕРЖДЕНО
Приказом №158-а от 27.08.2024

Инструкция администратора безопасности в информационных системах
МБОУ ООШ № 12

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности (далее – Администратор) в информационных системах МБОУ ООШ № 12 (далее - ИС) назначается приказом Директора МБОУ ООШ № 12 и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ДПД) и другой конфиденциальной информации в процессе ее обработки в ИС.

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

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

1.4. Администратор безопасности подчиняется напрямую Руководителю и имеет право требовать от пользователей ИС выполнения указаний и инструкций, связанных с защитой информации.

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

– Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;

– «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;

– методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

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

2. ФУНКЦИИ И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Изучение особенностей технологических процессов обработки информации в МБОУ ООШ № 12 с целью принятия решения о необходимости защиты информации в ИС и классификации ИС, либо поиск специализированных организаций, производящих на договорной основе такой анализ. В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации о ИС сотрудниками сторонней организации. По окончании

аналитических работ Администратор обязан ознакомиться с их результатами и подписать отчетные документы, либо составить мотивированный отказ в подписании таких документов и отправить их на доработку сторонней организации.

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

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

– ежегодный плановый пересмотр актуальных угроз безопасности информации;

– появление в общедоступных источниках информации о новых угрозах и уязвимостях, имеющих предпосылки в ИС;

– существенное изменение условий функционирования ИС, внедрение новых технологий;

– изменение нормативной документации, касающейся моделирования угроз безопасности информации;

– в результате инцидента безопасности.

2.4. Разработка проектной документации на систему защиты информации в ИС (Техническое задание, Технический проект), либо привлечение на договорной основе сторонних организаций для таких работ.

2.5. Участие в подготовке технических заданий для конкурсов и аукционов, связанных с закупкой технических средств, программного обеспечения или средств защиты информации для ИС.

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

2.7. Выработка предложений руководству МБОУ ООШ № 12 по совершенствованию системы защиты информации в ИС.

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

2.9. Знание состава, структуры, назначения и выполняемых задач ИС, а также состава информационных технологий и технических средств, позволяющих осуществлять обработку ДПД и иной конфиденциальной информации.

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

2.11. Разработка плана мероприятий по обеспечению безопасности защищаемой информации в ИС и по защите периметра ИС. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в ИС и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости.

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

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

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

2.15. Организация учета иных машинных носителей информации.

2.16. Проведение инструктажей сотрудников, работающих с защищаемой информацией в ИС (далее – Пользователи ИС), по темам: правила работы в ИС, защита информации в ИС, положения законодательства в сфере защиты информации и персональных данных, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников МБОУ ООШ № 12 в вопросах информационной безопасности.

2.17. Организация первоначального доступа пользователям ИС к ресурсам ИС в соответствии с утвержденным положением о разграничении прав доступа в ИС. Блокировка учетных

записей, изменение полномочий пользователей и добавление новых пользователей ИС в соответствии с Инструкцией о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИС.

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

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

2.20. Участие в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности, внесение по результатам таких расследований предложений по совершенствованию системы безопасности. По мере возможности, Администратор должен восстанавливать ущерб, нанесенный ИС во время инцидента безопасности, а также восстанавливать ДПД и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента.

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

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

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

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

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

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

2.27. Обеспечение функционирования и поддержания работоспособности в ИС:

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

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

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

3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИС

Администратор имеет право:

3.1. Знакомиться с нормативными актами МБОУ ООШ № 12, регламентирующими процессы обработки и защиты ДПД и иной конфиденциальной информации.

3.2. Вносить предложения руководству МБОУ ООШ № 12 по совершенствованию существующей системы защиты информации.

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

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

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

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

4. УЧЕТНАЯ ЗАПИСЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИС И УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Одним из ключевых элементов системы защиты информации в ИС является учетная запись Администратора.

4.2. Под учетной записью Администратора устанавливаются средства управления: антивирусной защитой, средством защиты информации от несанкционированного доступа.

4.3. Администратор осуществляет управление политиками безопасности в ИС, обновлениями средств защиты информации, обновлениями антивирусных баз и сигнатур, конфигурацией информационной системы.

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

4.5. Учетная запись администратора является объектом защиты и защищается согласно требованиям к тому же классу, по которому классифицированы ИС в целом.

5. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИАНИРОВАННОГО ДОСТУПА

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

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

5.3. Технические средства (мобильные и стационарные) также проходят идентификацию и аутентификацию в ИС. Идентификация и аутентификация устройств производится посредством информационного обмена по специализированным сетевым протоколам (ARP, SNMP, NetBIOS и др.). В качестве идентификаторов устройств могут выступать: логические имена, идентификационные номера, IP-адреса, MAC-адреса или комбинация этих параметров. Администратор определяет правила идентификации и аутентификации устройств в ИС, конфигурирует протоколы и настраивает в средствах защиты информации соответствующие правила. Администратор принимает меры для предупреждения таких атак на ИС как: MAC-flooding, MAC-spoofing, ARP-spoofing, ARP-poisoning и других.

5.4. Администратор осуществляет учет машинных носителей информации, как стационарных (жесткие диски АРМ и серверов, SSD-накопители и т. д.), так и съемных (флеш-накопители, съемные жесткие диски, карты памяти, память мобильных устройств и т. д.). Каждому носителю присваивается идентификационный номер. Для стационарных машинных носителей информации фиксируется местонахождение носителя (АРМ, кабинет), в случае замены или утилизации стационарного или съемного машинного носителя принимаются меры по гарантированному уничтожению информации на носителе или самого носителя с соответствующей пометкой в Журнале учета машинных носителей информации. Съемные машинные носители информации выдаются пользователям под роспись в Журнале учета приема/выдачи съемных машинных носителей информации. Дата сдачи машинного носителя также фиксируется в Журнале. Администратор средствами СЗИ от НСД реализует запрет использования неучтенных машинных носителей в ИС.

5.5. Администратор осуществляет управление учетными записями с помощью встроенных механизмов ОС и с помощью механизмов СЗИ от НСД. В процессе управления учетными записями Администратор производит следующие действия:

– определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная учетная запись, учетная запись приложения, гостевая учетная запись, временная учетная запись и т. д.);

– объединение учетных записей в группы (при необходимости);

– проводит верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

– проводит анализ необходимости тех или иных полномочий в системе для учетных записей служб и приложений;

– производит заведение, активацию, блокирование и уничтожение учетных записей пользователей;

– проводит пересмотр и, при необходимости, корректировку учетных записей пользователей либо в процессе периодического мероприятия, либо в связи с изменением должностных обязанностей того или иного пользователя;

– уничтожает временные учетные записи пользователей, предоставленные для однократного (или ограниченного по времени) выполнения задач в ИС, и учетные записи уволенных сотрудников;

– осуществляет настройку прав доступа пользователей к ресурсам ИС средствами СЗИ от НСД в соответствии с утвержденным Положением о разграничении доступа;

– средствами СЗИ от НСД настраивает автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования более 90 дней.

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

– загрузка операционной системы в безопасном режиме;

– восстановление операционной системы с последней работоспособной конфигурацией;

– изменение параметров BIOS/UEFI;

– загрузка с внешнего носителя с целью восстановления или переустановки операционной системы, восстановления работоспособности средств защиты информации, сканирования жесткого диска на вирусы, сканирования оперативной памяти или жесткого диска с целью выявления проблем и других действий восстановительного или диагностического характера.

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

– минимальная длина пароля составляет 8 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего регистров, как минимум одну цифру и один спецсимвол;

– при смене пароля, новый пароль должен отличаться минимум на два символа от предыдущего;

– максимальное время действия пароля – 90 дней;

– минимальное время действия пароля – 10 дней;

– запрещается использование пользователями пяти последних использованных паролей при создании новых паролей;

–при восьми неудачных попытках входа учетная запись блокируется не менее, чем на 10 минут.

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

5.9. Администратор средствами СЗИ от НСД запрещает пользователям самостоятельную установку любого программного обеспечения. В МБОУ ООШ № 12 утверждается перечень разрешенного к установке в ИС программного обеспечения. Перечень разрешенного к установке программного обеспечения определяется исходя из целей и задач, решаемых с помощью ИС. Перечень разрешенного к установке в ИС программного обеспечения подлежит периодическому пересмотру. Установка разрешенного программного обеспечения производится либо Администратором лично, либо в присутствии Администратора и под контролем Администратора.

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

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

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

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

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

6.4. Администратор анализирует технологические процессы обработки информации, а также особенности функциональных обязанностей сотрудников МБОУ ООШ № 12 для оптимизации настроек средств межсетевого экранирования. Средство межсетевого экранирования настраивается по принципу разрешения только тех ресурсов, сетевых портов и протоколов, необходимых для нормального функционирования ИС и МБОУ ООШ № 12 в целом.

6.5. Администратор организует взаимодействие ИС с информационными системами сторонних организаций.

6.6. Администратор запрещает пользователям внешних информационных систем доступ к ИС.

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

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

7. ОБСЛУЖИВАНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

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

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

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

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

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

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

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

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

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

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

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

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

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

8. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ

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

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

8.3. Администратор самостоятельно или в составе группы реагирования на инциденты информационной безопасности (в случае значительного инцидента безопасности) реагирует на

сообщения системы антивирусной защиты или пользователей об обнаружении вредоносных компьютерных программ (вирусов), или на подозрение наличия таковых, и принимает меры по нейтрализации обнаруженных угроз.

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

9. РЕГИСТРАЦИЯ И УЧЕТ СОБЫТИЙ БЕЗОПАСНОСТИ

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

9.2. Администратор периодически изучает записи системы регистрации и учета событий безопасности и, в случае обнаружения инцидентов безопасности информации, созывает группу реагирования на инциденты информационной безопасности, которая, в свою очередь, действует согласно соответствующим инструкциям.

10. ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

10.1. Для выявления уязвимостей в ИС привлекается Организация-лицензиат ФСТЭК России.

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

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

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

10.5. Администратор принимает меры по устранению или нейтрализации выявленных уязвимостей. В первую очередь обрабатываются уязвимости с наивысшим баллом по шкале CVSS. В случае необходимости, до устранения уязвимости могут быть локализованы (отключены от общей сети) сегменты или отдельные АРМ.

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

10.7. Администратор не реже чем один раз в месяц осуществляет контроль состава технических средств, программного обеспечения и средств защиты информации, а также корректности функционирования и настроек программного обеспечения и средств защиты информации.

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

11.1 В ИС с целью обеспечения целостности и доступности защищаемой информации применяется резервное копирование.

11.2 Резервное копирование защищаемой информации, образов операционных систем, конфигураций программного обеспечения производится Администратором на учтенный съемный носитель информации. Резервное копирование в места, где не представляется возможность обеспечить или проконтролировать наличие должной системы защиты информации (например, в облачные хранилища), запрещено.

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

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

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

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

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

11.8 Восстановление информации из резервной копии производится Администратором по мере необходимости или в случае инцидента информационной безопасности. Восстановление информации из резервной копии может проводиться в экстренном порядке или в штатном режиме, в зависимости от ущерба, который был нанесен ИС в результате инцидента информационной безопасности.

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

11.10 Резервирование основных технических средств и систем (далее - ОТСС) обеспечивается путем подключения к этим средствам ИБП и путем замены вышедшего из строя ОТСС на резервное устройство администратором.

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

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

12.2. Администратор присутствует в процессе ремонта технических средств ИС сотрудниками сторонних организаций на территории МБОУ ООШ № 12. Администратор обеспечивает гарантированное затирание данных с носителей информации, либо демонтаж носителей информации (в том числе и оперативной памяти) с технических средств в случае необходимости отправки технических средств для ремонта на территорию сторонних организаций.

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

Приложение №2
УТВЕРЖДЕНО
Приказом №158-а от 27.08.2024

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

Администратора
автоматизированной системы «Сетевой Город. Образование».

I. Общие положения

1. На должность администратора автоматизированной системы «Сетевой Город. Образование» назначается лицо, являющееся работником ОУ, имеющее высшее образование и обладающее опытом работы на персональном компьютере на уровне продвинутого пользователя.

2. Назначение на должность администратора АСУ «Сетевой Город. Образование». и освобождение от нее производится приказом директора образовательного учреждения.

II. Функциональные обязанности:

−осуществляет изучение структуры и содержания общешкольной базы данных, реализованной в АСУ «Сетевой Город. Образование».

− наполняет контентом общешкольную базу данных в виде ключевых позиций в рамках определенных прав доступа для формирования базового функционала системы, включающего в себя: структуры учебного года (четверти, триметры и т.п.); списки изучаемых предметов; учебные планы, списки обучающихся; списки педагогов; списки классов; списков учебных групп, текущую и промежуточную успеваемость и т.д.;

− осуществляет обмен данными между общешкольной базой данных, реализованной в АСУ «Сетевой Город. Образование». и распространенными программами для редактирования электронных таблиц (MS Excel, Calc и др.) в виде импорта\экспорта списочных сведений;

−осуществляет необходимые мероприятия по поддержанию базы данных в актуальном состоянии (своевременно вносит изменения и коррективы в информацию, содержащуюся в базе данных);

−осуществляет подтверждение данных;

−осуществляет необходимую минимальную настройку и готовит отчетные печатные формы в рамках своих полномочий в общешкольной базе данных, реализованной в АСУ «Сетевой Город. Образование».

−осуществляет мероприятия по обеспечению преемственности и сохранности информации в общешкольной информационной базе, включая: регламентные работы, перевод базы данных на следующий учебный год;

−ведет журнал учета выданных работникам ОУ учетных данных (логинов и паролей) для авторизации на сайте АСУ ««Сетевой Город. Образование».

−разрабатывает предложения по организации эффективного использования общешкольной базы данных, реализованной в АСУ «Сетевой Город. Образование».

– осуществляет руководство, планирование, организацию, регулирование и контроль выполнения работ педагогическими работниками по внедрению и использованию АСУ «Сетевой Город. Образование».

– несет ответственность за сводную отчетность из общешкольной базы данных для представления в базе данных муниципального органа управления образования;

– разрабатывает нормативные документы, обеспечивающие внедрение и использование АСУ «Сетевой Город. Образование» в деятельности образовательного учреждения.

III. Требования, предъявляемые к администратору АИС «Сетевой Город. Образование».

– владеет ИКТ - компетентностью и новыми информационными технологиями;

– владеет умениями и навыками работы с АИС «Сетевой Город. Образование».

– владеет умениями и навыками работы с прикладными офисными пакетами (Microsoft Office, Open Office.org);

– знает Закон РФ “Об образовании”, нормативные документы по вопросам информатизации образования;

– знает систему организации образовательного процесса в школе;

– знает принципы систематизации методических и информационных материалов;

– знает основы трудового законодательства;

– знает правила ТБ и пожарной безопасности, санитарно-гигиенические нормы работы с компьютерной техникой.

Приложение №3
УТВЕРЖДЕНО
Приказом №158-а от 27.08.2024

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
КООРДИНАТОРА,
ответственного лица за методическое сопровождение педагогических работников по работе с автоматизированной системой управления образовательным учреждением ««Сетевой Город. Образование».

I. Общие положения

1. На должность ответственного лица за методическое сопровождение педагогических работников по работе с автоматизированной системой управления «Сетевой Город. Образование» назначается лицо, являющееся работником ОУ, имеющее высшее образование и обладающее опытом работы на персональном компьютере на уровне продвинутого пользователя.

2. Назначение на должность ответственного лица за методическое сопровождение педагогических работников по работе с АСУ «Сетевой Город. Образование» и освобождение от нее производится приказом директора образовательного учреждения.

II. Функциональные обязанности:

– осуществляет изучение структуры и содержания общешкольной базы данных, реализованной в АСУ «Сетевой Город. Образование».

– участвует в мероприятиях по поддержанию базы данных в актуальном состоянии;

– осуществляет подтверждение данных при производственной необходимости;

– разрабатывает предложения по организации эффективного использования общешкольной базы данных, реализованной в АСУ «Сетевой Город. Образование».

– организует обучение педагогических работников ОУ по работе с общешкольной базой данных, реализованной в АСУ «Сетевой Город. Образование».

– оказывает консультативную и практическую помощь педагогическим и иным работникам школы, использующим в своей деятельности автоматизированную систему управления, в организации ввода информации в общешкольную базу данных и подготовке к печати отчетов;

– осуществляет планирование занятости рабочих мест (компьютеров, компьютерных классов) при необходимости организации фронтального ввода информации в общешкольную базу данных, составляет графики работ;

– участвует в осуществлении контроля выполнения работ педагогическими работниками по внедрению и использованию АСУ «Сетевой Город. Образование».

– несет ответственность за сводную отчетность из общешкольной базы данных для представления в базе данных муниципального органа управления образования;

– участвует в разработке нормативных документов, обеспечивающих внедрение и использование АСУ «Сетевой Город. Образование».

– в деятельности образовательного учреждения;

– ведёт журнал учета выданных учащимся и родителям (законным представителям) ОУ учетных данных (логинов и паролей) для авторизации на сайте АСУ «Сетевой Город. Образование».

– ведёт мониторинг предоставляемой информации об успеваемости учащихся в электронном виде.

– III. Требования, предъявляемые к ответственному лицу за методическое сопровождение педагогических работников по работе с АСУ «Сетевой Город. Образование».

– владеет ИКТ-компетентностью и новыми информационными технологиями;

– владеет умениями и навыками работы с АСУ «Сетевой Город. Образование».

– владеет умениями и навыками работы с прикладными офисными пакетами (Microsoft Office, Open Office.org);

– знает Закон РФ “Об образовании”, нормативные документы по вопросам информатизации образования;

– знает систему организации образовательного процесса в школе;

– знает принципы систематизации методических и информационных материалов;

– знает основы трудового законодательства;

– знает правила ТБ и пожарной безопасности, санитарно-гигиенические нормы работы с компьютерной техникой.

Приложение №4
УТВЕРЖДЕНО
Приказом №158-а от 27.08.2024

Комментарии

к должностным обязанностям педагогических работников образовательных учреждений в пункте «Осуществляет контрольно-оценочную деятельность в образовательном процессе с использованием современных способов оценивания в условиях информационно-коммуникационных технологий (ведение электронных форм документации, в том числе электронного журнала и дневников обучающихся)» связанные с использованием АСУ «Сетевой Город. Образование».

Комментарии к должностным обязанностям учителей, связанные с использованием АСУ «Сетевой Город. Образование».

Учитель-предметник (пользователь АСУ «Сетевой Город. Образование»).

1. Осуществляет информационное наполнение электронных журналов АСУ «Сетевой Город. Образование»- осуществляет заполнение раздела Тематическое планирование;
- осуществляет заполнение раздела Учебные материалы;
- осуществляет систематическую работу (ежедневно) по заполнению электронного журнала (тема урока, домашние задания, оценки, пропуски занятий).
2. Осуществляет работу по использованию дополнительных возможностей АСУ «Сетевой Город. Образование» (внутренняя почта).

Комментарии к должностным обязанностям классных руководителей, связанные с использованием АСУ «Сетевой Город. Образование».

Классный руководитель - пользователь АСУ «Сетевой Город. Образование».

- осуществляет информационное наполнение АСУ «Сетевой Город. Образование»
- осуществляет заполнение шаблона список учащихся класса,
- осуществляет заполнение модуля создание подгрупп класса;
- осуществляет заполнение модуля индивидуальные учебные планы;
- осуществляет заполнение личной карты ученика;
- осуществляет заполнение личной карты родителей;
- осуществляет систематическую работу (ежедневно или 1 раз в неделю) по проверке заполнения электронного журнала;
- осуществляет снятие отчета классного руководителя;
- обеспечивает доступ к АСУ «Сетевой Город. Образование» учащимся и родителям/законным представителям (ввод и выдача учетных записей: логины и пароли)

2. Осуществляет работу по использованию дополнительных возможностей АСУ «Сетевой Город. Образование».

Приложение №5
УТВЕРЖДЕНО
Приказом №158-а от 27.08.2024

Правила пользования автоматизированной информационно-управляющей системой «Сетевой город. Образование» в МБОУ ООШ №12

1. Общие положения.

1.1. Правила пользования автоматизированной информационно-управляющей системы "Сетевой город. Образование" (далее - Правила) определяют единый для всех субъектов порядок использования документированной информации о кадрах, контингенте и об учебном процессе образовательного учреждения, содержащейся в автоматизированной информационно-управляющей системе "Сетевой город. Образование» (далее – АИС «СГО»).

1.2. Участниками пользования АИС «СГО» являются сотрудники, учащиеся, родители (или их законные представители) МБОУ ООШ №12

1.3. Правила утверждаются в соответствии с Федеральными Законами «Об информации, информационных технологиях и о защите информации», «О персональных данных» №152-ФЗ от 27.07.2006 года в целях установления единого порядка пополнения АИС «СГО» и получения пользователями документированной информации, соблюдения конституционных прав и свобод граждан, унификации и защиты от несанкционированного доступа документированной информации, содержащейся в АИС «СГО» (далее - документированная информация).

2. Права и обязанности сотрудников МБОУ ООШ №12

2.1. МБОУ ООШ №12 технологически обеспечивает круглосуточную работоспособность АИС «СГО» и ее базы данных.

2.2. МБОУ ООШ №12 обеспечивает содержательное сопровождение документированной информации в АИС «СГО» с учетом особенностей образовательного процесса.

2.3. МБОУ ООШ №12 регламентирует и координирует содержательное сопровождение документированной информации в АИС «СГО» посредством нормативно - правовых актов в пределах своей компетенции с учетом особенностей образовательного процесса.

2.4. МБОУ ООШ №12 использует документированную информацию для решения вопросов тактических и стратегически задач в процессе управления образовательным процессом.

2.5. МБОУ ООШ №12 предоставляет участникам образовательного процесса доступ к документированной информации на основе распределенных прав пользователей АИС «СГО» и в соответствии с нормативно-правовыми актами.

2.6. Пользователи АИС «СГО» обязаны вносить документированную информацию согласно прав доступа и Регламента работы.

2.7. На пользователей АИС «СГО», не осуществляющих внесение документированной информации, настоящие Правила распространяются в полном объеме.

2.8. Пользователи АИС «СГО» несут ответственность за нарушение режима защиты, обработки и порядка использования документированной информации в соответствии с действующим законодательством РФ.

3. Порядок обращения с документированной информацией

3.1. Документированная информация предоставляется в АИС «СГО» на основании Регламента работы.

3.2. Документированная информация является конфиденциальной информацией и относится к

категории персональных данных.

3.3. МБОУ ООШ №12 обязана принимать меры по обеспечению защиты документированной информации и соблюдению требований по защите информации в соответствии с действующим законодательством РФ и иными нормативно - правовыми актами в области защиты информации.

3.4. Документированная информация является конфиденциальной информацией, относится к категории персональных данных, имеет ограниченный доступ и разглашению не подлежит.

3.5. Документированная информация не может быть использована пользователями АИС СГО в целях причинения имущественного и (или) морального вреда гражданам, затруднения реализации их прав и свобод.

4. Права учащихся, родителей (или лиц их заменяющих).

4.1. Учащиеся МБОУ ООШ №12, родители (или лица их заменяющие) (далее - субъекты) в соответствии с «Положением об автоматизированной информационно-управляющей системы "Сетевой город. Образование" имеют право на ознакомление с документированной информацией об обучающемся.

4.2. Доступ учащихся МБОУ ООШ №12, родителей (или лиц их заменяющих) к документированной информации осуществляется в соответствии с правами доступа, на основе логина и пароля, определяемого МБОУ ООШ №12.

4.3. Документированная информация о субъекте может быть предоставлена только субъекту, непосредственно обратившемуся в образовательное учреждение с письменным заявлением и предъявившему документ, удостоверяющий его личность.

4.4. МБОУ ООШ №12 обязана обеспечить доступ учащихся, родителей (или лиц их заменяющих) к документированной информации не позднее 10 дней с момента обращения.

4.5. Предоставление субъекту документированной информации о третьих лицах не допускается.

4.6. В случае обнаружения в АИС «СГО» несоответствия документированной информации о субъекте, он вправе обратиться в образовательное учреждение с заявлением об устранении неточностей. МБОУ ООШ №12 обязана в трёхдневный срок внести соответствующие изменения в документированную информацию, содержащуюся в АИС «СГО», и уведомить об этом субъекта.

4.8. МБОУ ООШ №12 обязана вести учет обращений субъекта.

5. Ответственность пользователей.

5.1. В случае нарушения пользователем АИС «СГО» настоящих Правил МБОУ ООШ №12 вправе отказать данному лицу в доступе к документированной информации.

5.2. Пользователь, виновный в разглашении сведений, ставших ему известными в процессе использования АИС «СГО», несет ответственность в пределах действующего трудового, административного, уголовного и гражданского законодательства.