СОГЛАСОВАНО

Председатель профкома

_____ О.М. Баландина

« ___ » _____ 2018 г.

УТВЕРЖДАЮ

Директор МОУ-СОШ №1

_____ Л.П. Карманова

« ___ » _____ 2018 г.

ИНСТРУКЦИЯ АДМИНСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Подписан: Карманова Лидия Прокопьевна
DN: C=RU, O=МОУ-СОШ №1 г. Петровск-Забайкальский, CN=Карманова Лидия Прокопьевна, E=school-1-pzb@mail.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: г. Петровск-Забайкальский
Дата: 2022.04.20 14:01:57+09'00'

2018 г.

1. Общие положения

1.1. Настоящая инструкция администратора безопасности, информации информационной системы МОУ-СОШ №1 (далее - Инструкция) разработана в соответствии с требованиями следующих документов:

– Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждены приказом ФСТЭК России от 11 февраля 2013 г. №17.

– Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства РФ от 15.09.2008 № 687;

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержден приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21.

1.2. Настоящая Инструкция определяет задачи, функции, обязанности, права и ответственность администратора безопасности информации информационной системы МОУ-СОШ №1 (далее – ИС, ИСПДн). Кроме того, в настоящей Инструкции определена технология выполнения функций и обязанностей, а также решения задач администратором безопасности информации.

1.3. Администратор безопасности информации информационной системы МОУ-СОШ №1 назначается приказом из числа сотрудников отдела сопровождения МОУ-СОШ №1 и обеспечивает правильность использования и нормальное функционирование системы защиты в ИС. Методическое руководство его работой осуществляется руководителем МОУ-СОШ №1

1.4. Настоящая Инструкция является дополнением к действующим нормативным и организационно-распорядительным документам по вопросам обеспечения безопасности информации в информационной системе МОУ-СОШ №1 и не исключает обязательного выполнения их требований.

1.5. Администратор безопасности информации в пределах своих функциональных обязанностей обеспечивает безопасность конфиденциальных данных, обрабатываемых, передаваемых и хранимых в ИС.

2. Основные функции администратора безопасности информации

2.1. Контроль выполнения требований действующих нормативных документов Российской Федерации, нормативной и регламентной документации по вопросам обеспечения

безопасности информации, не составляющей государственную тайну (далее – конфиденциальные данные, информация ограниченного доступа, персональные данные), при ее обработке в ИС и работе пользователей с носителями этой информации.

2.2. Контроль за реализацией политики разграничения доступа к конфиденциальным данным в процессе их обработки в ИС.

2.3. Контроль и взаимодействие с системным администратором, администратором виртуальной инфраструктуры, администратором баз данных в ходе повседневной деятельности.

2.4. Участие в разработке проектов инструкций пользователям ИС по обеспечению безопасности информации.

2.5. Контроль доступа в серверные помещения, где установлены основные элементы ИС (серверное и коммутационное оборудование), в соответствии с утвержденным списком работников.

2.6. Организация работ по контролю своевременности смены пользователями паролей для доступа к ресурсам (согласно установленной периодичности).

2.7. Осуществление текущего контроля за соблюдением технологического порядка обработки конфиденциальных данных в ИС;

2.8. Сопровождение подсистемы регистрации и учета действий пользователей:

– проведение анализа системных электронных журналов АРМ пользователей и серверов безопасности с целью выявления попыток несанкционированного доступа к защищаемым ресурсам, а также контроль электронных журналов средств межсетевого экранирования;

– своевременное реагирование и участие в проведении расследования попыток НСД и других инцидентов безопасности информации;

– разработка предложений для принятия дополнительных мер по предотвращению попыток НСД.

2.9. Организация работ по сопровождению средств обеспечения целостности информации системы защиты конфиденциальных данных:

– периодическое тестирование функций средств защиты от НСД, в том числе при изменении программной среды и полномочий исполнителей;

– восстановление программной среды, программных средств и настроек СЗИ при сбоях;

– поддержание установленного порядка и правил антивирусной защиты информации;

– своевременное периодическое обновление вирусных баз средств антивирусной защиты информации, контроль соблюдения пользователями порядка и правил проведения антивирусного тестирования элементов ИС.

2.10. Сопровождение подсистемы управления доступом реализованной в ИС, при этом:

– реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтерам и т.д.);

– вводить описания пользователей ИС в информационную базу СЗИ от НСД;

– своевременно удалять описания пользователей из базы данных СЗИ при изменении Списков должностных лиц, имеющих доступ к информационным системам персональных данных, для выполнения служебных (трудовых) обязанностей;

– осуществлять управление средствами защиты информации, реализующими функционал подсистемы межсетевого экранирования, в соответствии с эксплуатационной документацией (далее – ЭД) на данные средства.

3. Обязанности администратора безопасности информации

3.1. Администратор безопасности информации обязан:

3.1.1. Знать состав основных и вспомогательных технических систем и средств (далее – ОТСС и ВТСС) установленных и смонтированных в ИС, перечень используемого программного обеспечения.

3.1.2. Знать требования основных нормативных и руководящих документов РФ, действующих в области защиты от НСД к информации.

3.1.3. Знать ЭД (в том числе инструкции по администрированию и настройке) на СЗИ, реализующие функционал подсистем защиты персональных данных.

3.1.4. Осуществлять постоянный контроль за полномочиями пользователей ИС, обрабатывающих конфиденциальные данные.

3.1.5. Осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных.

3.1.6. Знать, соблюдать и обеспечивать соблюдение пользователями порядка и правил уничтожения носителей конфиденциальных данных.

3.1.7. Проводить анализ системных электронных журналов системы защиты конфиденциальных данных для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 30 дней.

3.1.8. Периодически тестировать функции СЗИ от НСД, в частности при изменении программной среды и полномочий исполнителей.

3.1.9. Контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, технических средствах АРМ и других устройствах информационной сети.

3.1.10. Обеспечивать функционирование и поддерживать работоспособность средств защиты информации в пределах возложенных функций.

3.1.11. Проводить инструктаж пользователей по правилам работы со средствами защиты от НСД к информации.

3.1.12. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники.

3.1.13. В случае отказа средств защиты информации принимать меры по их восстановлению.

3.1.14. Докладывать ответственному за обеспечение безопасности персональных данных и начальнику отдела информационных технологий о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации.

3.1.15. Вести документацию ИС в соответствии с требованиями нормативных документов, контролировать соответствие реальных конфигураций программно-аппаратных средств изложенных в документации.

3.1.16. Контролировать соответствие документально утвержденного состава аппаратной и программной части ИС реальным конфигурациям ИС.

3.1.17. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИС и отправке его в ремонт (контролировать затирание конфиденциальных данных на МНИ с составлением соответствующего акта).

3.1.18. Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИС.

4. Права администратора безопасности информации

4.1. Администратор безопасности информации ИС имеет право:

4.1.1. Требовать от пользователей ИС и обслуживающего персонала соблюдения установленных правил обработки конфиденциальных данных и выполнения требований руководящих и нормативно-методических документов по защите информации, не составляющей государственную тайну.

4.1.2. Требовать от пользователей ИС правильной эксплуатации технических средств ИС, средств защиты информации и программного обеспечения.

4.1.3. Требовать объяснительных документов и назначения служебного расследования в отношении пользователя ИС и обслуживающего персонала по фактам нарушения безопасности информации и НСД к конфиденциальным данным.

4.1.4. Участвовать в анализе инцидентов, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4.1.5. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4.1.6. Получать информацию, необходимую для выполнения должностных обязанностей, определенных Настоящей инструкцией.

4.1.7. Привлекать в установленном порядке работников к решению задач по обеспечению безопасности конфиденциальных данных по согласованию с руководителем.

5. Технология решения основных задач и выполнения своих функций администратором безопасности информации

5.1. В процессе эксплуатации ИС администратор безопасности информации обеспечивает выполнение всех требований руководящих документов ФСТЭК (Гостехкомиссии) России применительно к установленному классу ИС и уровню защищенности ИСПДн в объеме следующих настроек и установок системы защиты информации (СЗИ):

5.1.1. На автоматизированных рабочих местах пользователей должен быть реализован режим доверительной загрузки, путем установки пароля на средства BIOS и запрета несанкционированной загрузки операционных систем с внешних МНИ.

5.1.2. Для АРМ, использующих СЗИ от НСД, должны быть установлены следующие настройки:

- установлено однократное количество циклов затирания данных при их удалении;
- установлено минимальное количество символов в пароле 6 (шесть);
- установлены режимы полномочного управления доступом, контроль буфера обмена.

5.1.3. На каждом АРМ, использующем СЗИ от НСД:

- должна осуществляться сигнализация при нарушении целостности контролируемых ресурсов;
- установлен режим запроса пароля при входе в систему;

– запрещен прямой доступ к НЖМД АРМ путем опечатывания корпуса системного блок;

– запрещено кэширование паролей на жестком диске;

– отключены привилегии на администрирование системы защиты;

– включен режим затирания данных в файлах на локальных и сетевых дисках при их удалении;

– установлен режим замкнутой программной среды и сформирован список разрешенных для запуска программ, включен режим контроля целостности программ из этого списка;

– установлен «жесткий» режим контроля внешних устройств;

– установлена регистрация событий не ниже «обычной».

5.2. Администратор безопасности информации контролирует порядок ведения, смены и хранения паролей доступа в ИС.

5.2.1. При проверке правильности ведения паролей администратор безопасности информации устанавливает соответствие всех используемых паролей доступа в ИС требованиям п.7 «Положения о защите персональных данных, обрабатываемых в информационной системе МОУ-СОШ №1.

5.2.2. Администратор безопасности информации контролирует работу пользователей ИС. Контроль осуществляется путем анализа электронных журналов регистрации событий в системе защиты на предмет наличия в них фактов НСД к защищаемой информации. Журналы регистрации событий всех используемых СЗИ должны храниться в системе не менее 1 (одного) месяца.

5.2.3. В процессе эксплуатации ИС администратор безопасности информации обеспечивает безотказность функционирования подсистемы межсетевого экранирования и соблюдение установленных правил фильтрации сетевого трафика и маршрутизации в сегментах ИС, реализованных с использованием сертифицированных межсетевых экранов, руководствуясь при этом эксплуатационной документацией, входящей в комплект поставки.

5.2.4. Управление подсистемой межсетевого экранирования осуществляется с персонального рабочего места администратора безопасности информации, с использованием специализированного программного обеспечения, либо с помощью консоли управления по протоколу SSH.

5.2.5. Администратору безопасности информации запрещается изменять настройки СЗИ и средств межсетевого экранирования без согласования с организацией, проводившей аттестационные испытания ИС.

6. Порядок проверки электронных журналов СЗИ

6.1. Проверка электронных журналов СЗИ проводится с целью выявления несанкционированного доступа к конфиденциальным данным в ИС.

6.2. Право проверки электронного журнала обращений имеют:

– администратор безопасности информации;
– ответственный за обеспечение безопасности персональных данных;
– руководитель.

6.3. Проверке подлежат электронные журналы СЗИ НСД и межсетевого экрана.

6.4. Проверка должна проводиться не реже чем один раз в месяц.

7. Режим безопасности в помещениях ИС

7.1. Режим безопасности в помещениях ИС обеспечивается следующими методами и способами защиты информации от несанкционированного доступа:

- Реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе персональных данных и связанной с ее использованием работам, документам;
- Ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку конфиденциальной информации (персональных данных), а также хранятся носители информации;
- Размещение технических средств, позволяющих осуществлять обработку конфиденциальной информации (персональных данных), в пределах охраняемой территории.
- Организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку конфиденциальной информации (персональных данных).

8. Общие требования по физической защите объекта информатизации

8.1. Эксплуатация ИС и системы защиты информации в ее составе должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией.

8.2. С целью предотвращения либо существенного затруднения проникновения в здания, помещения посторонних лиц, хищения технических средств, документов и носителей

информации должна быть организована физическая защита помещений и собственно технических средств обработки информации с использованием технических средств охраны.

8.3. Должно быть организовано ограничение доступа персонала в помещения, где размещено коммутационное и серверное оборудование.

8.4. На период обработки защищаемой информации в помещениях, где размещаются средства обработки информации, могут находиться только лица, допущенные к обрабатываемой информации в установленном порядке.

8.5. Допуск в эти помещения других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться только с санкции руководителя учреждения или руководителя подразделения, эксплуатирующего ИС, по согласованию с администратором информационной безопасности ИС. При этом должны быть соблюдены меры, исключающие ознакомление этих лиц с конфиденциальной информацией. Рекомендуется обеспечивать защиту таких помещений соответствующими средствами контроля доступа.

8.6. С целью исключения предоставления избыточных прав доступа к информации в процессе эксплуатации ИС должен осуществляться периодический пересмотр прав доступа пользователей к информации.

8.7. В случае размещения в одном помещении различных технических средств одной или нескольких ИС должен быть исключен несанкционированный просмотр конфиденциальной информации.

8.8. Обращение с ключевыми документами средств криптографической защиты информации (СКЗИ), в случае их использования, должно осуществляться в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

8.9. При увольнении или изменении должностных обязанностей пользователей и администраторов ИС, в установленном в организации порядке должны быть приняты меры по оперативному изменению соответствующих паролей и прав доступа.

8.10. Контроль состояния и эффективности защиты информации осуществляется администратором информационной безопасности ИС и заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер, в проверке выполнения норм эффективности защиты информации ограниченного доступа в соответствии требованиями нормативных документов по защите информации.

9. Порядок охраны и допуска посторонних лиц в защищаемые помещения

9.1. Вскрытие и закрытие помещений осуществляется работниками, работающими в данных помещениях. Список работников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.

9.2. При отсутствии работников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа, о чем составляется акт.

9.3. При закрытии помещений и сдачей их под охрану работники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержится конфиденциальная информация убираются для хранения в опечатываемый сейф (металлический шкаф).

9.4. При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и (или) администратору информационной безопасности. Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

9.5. Руководитель, ответственный за защиту информации и администратор информационной безопасности организуют проверку ИС на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

9.6. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или руководителю, или администратору информационной безопасности. Помещения вскрывать запрещается.

9.7. Помещения вскрываются ответственным за помещение, или руководителем, в присутствии сотрудника охраны с составлением акта.

9.8. В соответствии с требованиями данного Положения при обработке защищаемой информации в ИС необходимо исключить не контролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИС, определенных соответствующим приказом.

10. **Ответственность администратора безопасности информации**

10.1. Администратор безопасности информации несет ответственность за:

– ненадлежащее выполнение своих обязанностей;

– не принятие мер по противодействию и локализации попыток НСД к конфиденциальным данным;

– разглашение состава и содержания комплекса организационно-технических мероприятий по защите конфиденциальных данных субъектам, не принимающим участие в обработке информации, не составляющей государственную тайну;

– разглашение сведений конфиденциального данных, ставших известными ему в ходе выполнения функциональных (должностных) обязанностей.

Лист ознакомления с инструкцией

№ п/п	Ф.И.О.	Дата ознакомления с инструкцией	Подпись	Примечание
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				