Государственное казенное общеобразовательное учреждение
«Михайловская школа – интернат»

УТВЕРЖДАЮ:
Директор

ГКОУ «Михайловская школа-интернат»
_____ И.Ю. Акимова
«__» _____ 2022г.

Инструкция
эксплуатационному персоналу пользовательских сегментов государственной информационной системы «Единая государственная система в сфере образования Волгоградской области» ГКОУ «Михайловская школа-интернат»

1. Общие требования.

1. Настоящая инструкция определяет состав, функции, права и обязанности эксплуатационного персонала пользовательских сегментов ГИС ГКОУ «Михайловская школа-интернат».
2. Для обеспечения защиты информации, обрабатываемой на пользовательских сегментах ГИС, Абонентом назначается эксплуатационный персонал, включающий:
   - ответственный за эксплуатацию пользовательского сегмента ГИС;
   - администратор ИБ пользовательского сегмента ГИС;
   - пользователи, допущенные к работе в пользовательских сегментах ГИС;
   - системный администратор пользовательского сегмента ГИС.

2. Системный администратор.

2.1. Функции системного администратора.

1. Системный администратор производит настройку ОСПО, осуществляет мониторинг состояния ТС, входящих в состав АРМ ГИС, выполняет анализ производительности сети, резервное копирование информации и ее восстановление после сбоев.
2. Деятельность системного администратора включает в себя:
3. Администрирование файловых систем, в т.ч планирование, создание, мониторинг функционирования.
4. Резервирование и восстановление информации на АРМ ГИС.
5. Настройку антивирусных средств, обновление их сигнатурных баз, а также контроль их работоспособности.
6. Контроль использования дискового пространства.
7. Диагностику и поиск ошибок, в т.ч.:
   - начальной загрузки и завершения функционирования операционных систем ТС АРМ ГИС;
   - проверку целостности файловых систем ТС АРМ ГИС;
   - анализ аварийных дампов;
   - диагностирование проблем с ТС АРМ ГИС и замену вышедших из строя компонент ТС АРМ ГИС.
8. Организацию работ по внесению изменений в аппаратно-программную конфигурацию

АРМ ГИС, в т.ч. при замене и ремонте вышедшего из строя оборудования.
9. Установку нового ОСПО и пакетов его обновлений.
10. Анализ и планирование развития кабельной структуры и сетевого оборудования АРМ ГИС.
11. Настройку сетевого оборудования АРМ ГИС.
12. Мониторинг функционирования сетевого оборудования АРМ ГИС.
13. Участие совместно с администратором ИБ в управлении (выявлении, идентификации, реагировании, ликвидации последствий) инцидентов информационной безопасности в АРМ ГИС.
14. Контроль физической сохранности ТС АРМ ГИС.

2.2. Обязанности системного администратора.

Системный администратор обязан:

1. Не допускать установку, использование, хранение и размножение на АРМ ГИС программных средств, не связанных с выполнением функциональных задач АРМ ГИС.
2. В случае отказа работоспособности ТС и ОСПО АРМ ГИС, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности. В случае выхода из строя СрЗИ оповестить администратора ИБ и ответственного за эксплуатацию АРМ ГИС.
3. Обеспечивать контроль за соблюдением технологического процесса обработки защищаемой информации в АРМ ГИС.
4. Информировать администратора ИБ и ответственного за эксплуатацию о фактах нарушения установленного порядка работ и попытках НСД к информационным ресурсам АРМ ГИС.
5. Обеспечивать выполнение требований по защите информации при обслуживании ТС АРМ ГИС и отправке их в ремонт. При проведении ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.
6. Контролировать выполнение работ по техническому обслуживанию элементов АРМ ГИС сотрудниками сторонних организаций.
7. Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, в соответствии инструкциями по действиям в нештатных ситуациях.
8. Знать и выполнять требования действующих нормативных и руководящих документов, а также инструкций, приказов (распоряжений), регламентирующих порядок защиты информации на АРМ ГИС.
9. Знать состав АРМ ГИС и вести формуляры АРМ ГИС.
10. Согласовывать свои действия, связанные с изменением технологического процесса обработки защищаемой информации с администратором ИБ и ответственным за эксплуатацию АРМ ГИС.

2.3. Права системного администратора.

Системный администратор имеет право:

1. Требовать от пользователей АРМ ГИС соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению ИБ.
2. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ ГИС или СРЗИ.

3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения ИБ, НСД, утраты, порчи обрабатываемой информации и ТС АРМ ГИС.
4. Обращаться к ответственному за эксплуатацию АРМ ГИС с требованием прекращения работы пользователя на АРМ ГИС при несоблюдении установленной технологии обработки информации и невыполнении требований по обеспечению ИБ.

3. Администратор ИБ.

3.1. Функции администратора ИБ.

1. Администратор ИБ обеспечивает разработку и выполнение мероприятий по защите информации в АРМ ГИС. Деятельность администратора ИБ включает в себя:
2. Настройку и администрирование СРЗИ, не имеющих средств централизованного управления.
3. Управление учетными записями пользователей АРМ ГИС в СРЗИ (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа к защищаемым ресурсам АРМ ГИС согласно разрешительной системе допуска к защищаемой информации.
4. Учет сведений о составе групп пользователей АРМ ГИС, а также их полномочий доступа к защищаемым информационным ресурсам.
5. Контроль за работоспособностью СРЗИ.
6. Координацию деятельности других администраторов с целью достижения необходимого уровня защиты информации на АРМ ГИС;
7. Анализ состояния ИБ на АРМ ГИС, включая периодическое сканирование и анализ уязвимостей АРМ ГИС. Сканирование и анализ уязвимостей осуществляется один раз в квартал, либо при изменении конфигурации программного обеспечения. По результатам сканирования оформляется протокол.
8. Анализ функционирования применяемых СРЗИ.
9. Планирование развития подсистемы ИБ АРМ ГИС.
10. Сопровождение и поддержку в актуальном состоянии технических паспортов АРМ ГИС (включающую структурную схему АРМ ГИС, планы размещения ТС, перечень установленного ОСПО и СПО и др.).
11. Контроль физической сохранности ТС АРМ ГИС.
12. Контроль исполнения пользователями АРМ ГИС установленного режима защиты информации, а также правильность работы с элементами АРМ ГИС и СрЗИ.
13. Анализ журналов учета событий, регистрируемых СРЗИ, с целью выявления возможных нарушений.
14. Регистрацию, выдачу (при необходимости) и учет выдачи пользователям электронных ключей (персональных идентификаторов) от СРЗИ.
15. Периодический контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусах ТС АРМ ГИС.
16. Периодические контрольные проверки автоматизированных рабочих мест АРМ ГИС и тестирование правильности функционирования СРЗИ.
17. Консультирование пользователей АРМ ГИС в части применения СРЗИ и по вопросам установленного режима ИБ.
18. Реагирование на инциденты, связанные с нарушением требований о защите информации.
19. Участие в восстановлении после сбоев и отказов СрЗИ в соответствии с предусмотренными документацией процедурами восстановления.
20. Планирование работ по защите информации на АРМ ГИС, организацию их выполнения, а также контроль за их эффективностью.

21. Контроль работ по внесению изменений в технологический процесс обработки защищаемой информации АРМ ГИС.
22. Участие в подготовке АРМ ГИС к аттестации на соответствие требованиям по защите информации.
23. Организацию разработки нормативно-методических и организационно-распорядительных документов по вопросам организации защиты информации АРМ ГИС.
24. Согласование мероприятий по защите информации на АРМ ГИС.
25. Разработку предложений по совершенствованию системы защиты информации АРМ ГИС.
26. Участие в разработке требований по защите информации при проведении исследований, при разработке (модернизации), испытаниях и эксплуатации АРМ ГИС.
27. Участие в согласовании технических заданий (частных технических заданий) на проведение работ, оказание услуг по созданию (модернизации) АРМ ГИС.
28. Участие в создании (совершенствовании) системы защиты информации АРМ ГИС.
29. Организация проведения периодического контроля эффективности мер защиты информации АРМ ГИС. Учет и анализ результатов контроля.
30. Участие в расследовании инцидентов ИБ на АРМ ГИС и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений.
31. Подготовку отчетов о состоянии работ по защите информации на АРМ ГИС.

3.2. Обязанности администратора ИБ.

Администратор ИБ обязан:

1. Знать и выполнять требования действующих нормативных и руководящих документов, а также инструкций, приказов (распоряжений), регламентирующих порядок защиты информации на АРМ ГИС.
2. Знать состав АРМ ГИС и вести их технические паспорта.
3. Осуществлять регулярный анализ записей журналов безопасности технических, программных СРЗИ и работы пользователей на АРМ ГИС.
4. Осуществлять контроль за полномочиями пользователей АРМ ГИС, на соответствие их значений ранее установленным.
5. Осуществлять контроль за неизменностью программной среды АРМ ГИС.
6. В случае отказа работоспособности СРЗИ АРМ ГИС, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
7. Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, в соответствии с инструкцией по действиям в нештатных ситуациях.
8. Следить за своевременным проведением необходимых регламентных работ по обеспечению безопасности конфиденциальной информации при ее обработке на АРМ ГИС с целью поддержания системы защиты информации в актуальном состоянии.
9. Следить за поддержанием применяемой системы защиты информации в актуальном состоянии (своевременная разработка, корректировка и переиздание документов, изучение и мониторинг нормативной базы по защите конфиденциальной информации, обрабатываемой на АРМ ГИС) и подготавливать предложения по ее совершенствованию.
10. Принимать участие в осуществлении внутреннего контроля соответствия требованиям к защите конфиденциальной информации.

3.3. Права администратора ИБ.

Администратор ИБ имеет право:

1. Требовать от пользователей АРМ ГИС соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению ИБ.
2. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ ГИС или СрЗИ.
3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и ТС АРМ ГИС.
4. Обращаться к ответственному за эксплуатацию АРМ ГИС с требованием прекращения работы пользователя на АРМ ГИС при несоблюдении установленной технологии обработки защищаемой информации и невыполнении требований по обеспечению ИБ.
5. Направлять ответственному за эксплуатацию АРМ ГИС предложения по совершенствованию технологических мер защиты информации.

4. Ответственный за эксплуатацию АРМ ГИС.

4.1. Функции ответственного за эксплуатацию АРМ ГИС.

Деятельность ответственного за эксплуатацию АРМ ГИС включает в себя:

1. Организацию работ по эксплуатации АРМ ГИС и ее развитие, а также обеспечение контроля за выполнением требований действующих нормативных и руководящих документов в отношении АРМ ГИС.
2. Организацию работ по внесению изменений в технологический процесс обработки защищаемой информации АРМ ГИС.
3. Планирование работ по организации эксплуатации АРМ ГИС, организацию их выполнения, а также контроль за их эффективностью.
4. Участие в подготовке АРМ ГИС к аттестации на соответствие требованиям по защите информации.
5. Согласование мероприятий по защите информации в АРМ ГИС.
6. Участие в согласовании технических заданий (частных технических заданий) на проведение работ, оказание услуг по созданию (модернизации) АРМ ГИС.
7. Участие в создании (совершенствовании) системы защиты информации АРМ ГИС.
8. Участие в проведении периодического контроля эффективности мер защиты информации АРМ ГИС.
9. Участие в расследовании инцидентов ИБ на АРМ ГИС и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений.
10. Подготовку отчетов по вопросам эксплуатации АРМ ГИС.

4.2. Обязанности ответственного за эксплуатацию АРМ ГИС.

Ответственный за эксплуатацию АРМ ГИС обязан:

1. Принимать решение о прекращении обработки конфиденциальной информации на АРМ ГИС при несанкционированном доступе (попытках) к ним или возникновении ситуаций, послуживших причиной возможной утраты конфиденциальной информации;
2. Контролировать, а в случае необходимости, корректировать работы по выбору, закупке и приемке нового ОСПО, СРЗИ, и ТС АРМ ГИС.
3. Следить за неизменностью условий функционирования

и эксплуатации АРМ ГИС с последующим информированием Оператора ЦОД в случае изменений.

4.3. Права ответственного за эксплуатацию АРМ ГИС.

Ответственный за эксплуатацию АРМ ГИС имеет право:

1. Требовать от администраторов выполнения организационно-распорядительной документации по обеспечению безопасности конфиденциальной информации, обрабатываемой на АРМ ГИС.
2. Принимать решения о прекращении работы пользователей на АРМ ГИС при несоблюдении установленной технологии обработки конфиденциальной информации и невыполнении требований по обеспечению безопасности информации.
3. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ ГИС или СРЗИ.
4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения ИБ, НСД, утраты, порчи обрабатываемой информации и ТС АРМ ГИС.

5. Примечание.

В настоящем документе применены следующие сокращения:

ИБ	информационная безопасность
ИС	информационная система
МЭ	межсетевой экран
НСД	несанкционированный доступ
ОСПО	общесистемное и специальное программное обеспечение
СрЗИ	средство защиты информации
СПО	специальное программное обеспечение
ТС	техническое средство
ЦОД	Единый центр обработки данных органов исполнительной власти Волгоградской области