



Приложение № 3

УТВЕРЖДАЮ

Заведующая

Е.С. Черных

Пр. 01-32/17 28.08 2019г.

ИНСТРУКЦИЯ АДМИНИСТРАТОРА
информационной безопасности информационных систем
Муниципального бюджетного дошкольного образовательного
учреждение «Детский сад общеразвивающего вида с приоритетным
осуществлением деятельности по социально-личностному развитию
детей №1 «Звездочка» городского округа «город Якутск»

1. Общие положения

1.1. Инструкция Администратора информационной безопасности информационных систем МБДОУ № 1 (далее – ИС МБДОУ № 1) (далее – Инструкция) определяет функции, права и обязанности Администратора информационной безопасности (далее – Администратор ИБ) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов в ИС МБДОУ № 1. Администратор ИБ назначается из числа сотрудников МБДОУ № 1 приказом заведующего и обеспечивает правильность использования и нормальное функционирование установленной системы защиты ИС МБДОУ № 1.

1.2. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

1.3. Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах пользователей. Он несет ответственность за реализацию принятой политики безопасности.

2. Должностные обязанности

2.1. Администратор ИБ обязан:

2.1.1. Осуществлять учет и периодический контроль за составом и полномочиями пользователей ИС МБДОУ № 1

2.1.2. Осуществлять оперативный контроль за работой пользователей ИС в МБДОУ № 1 анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных архивов.

2.1.3. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в ИС МБДОУ № 1 СЗИ.

2.1.4. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных СВТ, обеспечивать и контролировать установку и настройку СЗИ.

2.1.5. Не реже одного раза в месяц проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.6. Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил в соответствии с «Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах МБДОУ № 1

2.1.7. Управлять идентификаторами (осуществлять создание, присвоение и уничтожение идентификаторов пользователей и устройств) и средствами аутентификации (аутентификационной информацией) внутренних пользователей в ИС МБДОУ № 1 обеспечивать соблюдение правил идентификации и аутентификации пользователей и устройств в соответствии с «Правилами идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах МБДОУ № 1

2.1.8. Осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации в соответствии с «Правилами идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах МБДОУ № 1

2.1.9. Осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в ИС МБДОУ № 1 программного обеспечения в соответствии с «Правилами по ограничению программной среды в информационных системах МБДОУ № 1.

2.1.10. Настраивать параметры журналов регистрации событий безопасности в соответствии с «Правилами регистрации событий безопасности в ИС МБДОУ № 1

2.1.11. Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже одного раза в неделю.

2.1.12. Управлять средствами антивирусной защиты в соответствии с «Инструкцией по антивирусной защите в информационных системах МБДОУ № 1

2.1.13. Осуществлять контроль уровня защищенности информации, обрабатываемой в ИС МБДОУ № 1 в соответствии с «Инструкцией по контролю защищенности информации в информационных системах МБДОУ № 1

2.1.14. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.

2.1.15. Обеспечивать сохранность СЗИ, эксплуатационной и технической документации к СЗИ, а также порядок обращения с СЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации в соответствии с «Инструкцией по порядку обращения со средствами защиты информации в информационных системах МБДОУ № 1

2.1.16. Проводить не реже одного раза **в 6 месяцев** контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в соответствии с «Инструкцией по организации парольной защиты МБДОУ № 1»

2.1.17. Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ ИС МБДОУ

2.1.18. Осуществлять поэкземплярный учет в соответствующем журнале:

- СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ);
- эксплуатационной и технической документации к СЗИ.

2.1.19. Осуществлять хранение:

- носителей дистрибутивов СЗИ;
- лицензий и сертификатов на СЗИ.

2.1.20. Не реже одного раза в месяц осуществлять проверки:

- состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);
- состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

2.1.21. Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ИС МБДОУ № 1 по вопросам работы с СЗИ.

2.1.22. Отвечать на вопросы обслуживающего и эксплуатирующего персонала ИС МБДОУ № 1, связанные с работой СЗИ.

2.1.23. Составлять инструкции по работе с СЗИ.

2.1.24. Докладывать руководству МБДОУ № 1 об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.

2.1.25. Участвовать в выявлении инцидентов информационной безопасности и реагировании на них.

В ходе выявления инцидентов и реагирования на них осуществляются:

- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС МБДОУ № 1 в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.1.26. Управлять системой защиты информации ИС МБДОУ № 1.

В ходе управления системой защиты информации ИС МБДОУ № 1 осуществляются:

- поддержание системы защиты информации (структуры системы защиты информации ИС МБДОУ № 1, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты;

– управление изменениями системы защиты информации, в том числе определение типов возможных изменений системы защиты информации, санкционирование внесения изменений в системы защиты информации, документирование действий по внесению изменений в системы защиты информации, сохранение данных об изменениях системы защиты информации, контроль действий по внесению изменений в системы защиты информации;

– анализ потенциального воздействия планируемых изменений в системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС МБДОУ № 1 определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС МБДОУ № 1 и их системы защиты информации;

2.1.27. внесение информации (данных) об изменениях в базовой конфигурации ИС МБДОУ № 1 и их системы защиты информации в эксплуатационную документацию на систему защиты информации ИС МБДОУ № 1

2.1.28. В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий. Оперативно докладывать вышестоящему руководству о случаях возникновения нештатных ситуаций и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС МБДОУ № 1. Предпринимаемые меры по возможности согласовывать с вышестоящим руководством.

3. Права

3.1. Администратор ИБ имеет право:

3.1.1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС МБДОУ № 1

3.1.2. Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ИС МБДОУ № 1 при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.1.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех недостатках в работе ИС МБДОУ № 1 и их системы защиты.

3.1.4. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.5. Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.

3.1.6. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в т.ч. вести мониторинг действий пользователей и обслуживающего персонала ИС МБДОУ № 1).

3.1.7. Вносить свои предложения по совершенствованию мер защиты информации в ИС МБДОУ № 1

4. Ответственность

4.1. Администратор ИБ ИС МБДОУ № 1 несет ответственность:

4.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.1.2. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

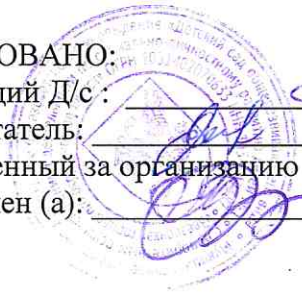
СОГЛАСОВАНО:

Заведующий Д/с:

Ст.воспитатель:

Ответственный за организацию обработки персональных данных

Ознакомлен (а):



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]