УТВЕРЖДЕНО
Приказом МДОУ ДС «Морошка»
№ 23-ОД от 18.11 2022 г.

# ИНСТРУКЦИЯ
# по эксплуатации аттестованных информационных систем Муниципального дошкольного образовательного учреждения детский сад «Морошка»

Приложение к приказу **№ 23-ОД** от 18.11.2022

**ИНСТРУКЦИЯ**
**по эксплуатации аттестованных информационных систем**
**Муниципального дошкольного образовательного**
**учреждения**
**детский сад «Морошка»**

## 1. Общие положения

**1.1.** Настоящая Инструкция по эксплуатации аттестованных информационных систем Муниципального дошкольного образовательного учреждения детский сад «Буратино» разработана для реализации меры, установленной в соответствии с требованиями приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными документами по безопасности информации, и определяет порядок эксплуатации аттестованных информационных систем в Муниципальном дошкольном образовательном учреждении детский сад «Морошка» (далее - МДОУ), устанавливает ответственность администратора безопасности информации и работников в том числе сотрудников, за обеспечение безопасности информации при эксплуатации аттестованных информационных систем МДОУ.

**1.2.** Оператор - муниципальный орган, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

## 2. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

2.1. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и комплектом организационно- распорядительными документами по защите персональных данных и в том числе включает:

– управление (администрирование) системой защиты информации информационной системы;

– выявление инцидентов и реагирование на них;

– управление конфигурацией аттестованной информационной системы и ее системы защиты информации;

– контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:

– заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;

– управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

–

– установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации;

– централизованное управление системой защиты информации информационной системы (при необходимости);

– регистрация и анализ событий в информационной системе, связанных с защитой информации (далее - события безопасности);

– информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение;

– сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

**2.2.** В ходе выявления инцидентов и реагирования на них осуществляются:

– определение лиц, ответственных за выявление инцидентов и реагирование на них;

– 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;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

– 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 информационной системы и ее сегментов 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.

**2.3.** В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации осуществляются:

– поддержание конфигурации информационной системы и ее системы защиты информации (структуры системы защиты информации информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее системы защиты информации);

– определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

– управление изменениями базовой конфигурации информационной системы и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации информационной системы и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации информационной системы и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных актуальных угроз безопасности информации и работоспособность информационной системы;

– 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 информационной системы и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации информационной системы;

– принятие решения о повторной аттестации информационной системы (в случае изменения по результатам управления конфигурацией класса защищенности информационной системы, состава актуальных угроз безопасности информации или проектных решений по системе защиты информации информационной системы).

**2.4.** В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

– контроль за событиями безопасности и действиями пользователей в информационной системе;

– контроль (анализ) защищенности информации, содержащейся в информационной системе;

– анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;

– периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации информационной системы и повторной аттестации информационной системы (в случае изменения класса защищенности информационной системы, состава актуальных угроз безопасности информации или проектных решений по системе защиты информации информационной системы).

## 3. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы

**3.1.** Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно- информации и (или) уничтожение машинных носителей информации.

**3.2.** Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора.

**3.3.** Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

**3.4.** При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

## 4. Ответственность

**4.1.** Ответственность за проведение мероприятий в соответствии с требованиями настоящей Инструкции возлагается на ответственного за организацию обработки персональных данных в МДОУ, администратора безопасности информации МДОУ, ответственных за обеспечение безопасности, ответственного по защите информации МДОУ и сотрудников МДОУ.