МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
№ 48 «ЭНЕРГЕТИК» Г. НЕРЮНГРИ НЕРЮНГРИНСКОГО РАЙОНА

УТВЕРЖДЕНО
приказом № 84 от 25.05.2022г.

Заведующая МДОУ № 48 «Энергетик»
Папина Е. В.

Алгоритм реагирования на инциденты информационной безопасности в МДОУ № 48 «Энергетик» города Нерюнгри Нерюнгринского района

I. Реагирование на инцидент ИБ

Реагирование на инцидент информационной безопасности (далее – ИБ) включает в себя технические мероприятия, обеспечивающие целостность криминалистически значимых данных и возможность судебного исследования этих данных в будущем, а также организационные мероприятия, которые позволяют снизить ущерб от инцидента и составить необходимые для правоохранительных органов документы.

Сущностью технических мероприятий является немедленное обеспечение целостности данных, потенциально имеющих отношение к инциденту, путем отключения, упаковки и опечатывания, а затем и должного хранения соответствующих носителей информации. Отключение носителей информации позволяет свести к нулю риск уничтожения криминалистически значимых данных в результате работы вредоносных программ и действий злоумышленника, а их упаковка, опечатывание и должное хранение обеспечивают достаточный уровень оцениваемой достоверности результатов криминалистического исследования в суде.

Организационные мероприятия заключаются в уведомлении руководства ДОУ информационной безопасности организации и иных заинтересованных организаций о факте инцидента. Документы, составленные при проведении организационных мероприятий, могут использоваться как основания для рассмотрения вопросов о возбуждении уголовных дел или для уточнения

вопросов, выносимых на разрешение при назначении судебных экспертиз носителей информации организации.

После реагирования на инцидент ИБ начинается расследование инцидента и восстановление информационной системы организации. Восстановление информационной системы организации заключается в замене изъятых, упакованных и опечатанных носителей информации на новые, установке требуемого ПО и конфигурации информационной системы с учетом повышенных требований ИБ.

II. Общий алгоритм действий при наступлении инцидента

Основная задача службы ИБ – это предотвращение реализации возможных рисков, связанных с утечкой или потерей информации для ДОУ, которая основана на понимании, формулировании и удовлетворении осознанных пожеланий образовательного процесса.

Деятельность ДОУ в области ИБ описывается в документе «Политика информационной безопасности», где прописаны все общие принципы и правила, а также формализованы задачи на текущий горизонт планирования в развитии ДОУ.

Общий алгоритм действий сотрудников СБ в случае наступления инцидента информационной безопасности. Типовой сценарий при нарушениях ИБ может быть основан на приведенных ниже базовых действиях. В случае возникновения инцидента ИБ необходимо:

1. Идентифицировать инцидент и убедиться, что он действительно имеет место быть.
2. Локализовать область ИТ-инфраструктуры, задействованной в инциденте.
3. Ограничить доступ к объектам, задействованным в инциденте.
4. Оформить служебную записку на имя заведующего ДОУ о факте возникновения инцидента.
5. Привлечь компетентных специалистов для консультации.
6. Создать группу по расследованию инцидента и составить план работ по сбору доказательств и восстановлению систем. Протоколировать все действия, которые осуществляются в ходе реагирования на инцидент.
7. Обеспечить сохранность и должное оформление доказательств.

7.1. Снять энергозависимую информацию с работающей системы.

7.2. Собрать информацию о протекающем в реальном времени инциденте.

7.3. Отключить от сети питание.

8. В присутствии третьей независимой стороны произвести изъятие и опечатывание носителей информации с доказательной базой, а также снятие образов и другой информации для последующего анализа и сохранения.

8.1. Оформить протоколом все операции с носителями информации.

8.2. Провести детальную опись объектов с информацией, извлекаемых данных, а также мест их сохранения.

8.3. Задокументировать процесс на фотовидеокамеру. Инциденты информационной безопасности.

8.4. Сохранить опечатанные объекты вместе с протоколом в надежном месте до передачи носителей на исследование или в правоохранительные органы.

9. После сохранения и оформления вещественных доказательств восстановить работоспособность информационных систем.

10. При проведении исследования источников информации обеспечить неизменность доказательств. Работать только с копией.

11. При проведении расследования обеспечить корректное взаимодействие с заинтересованными подразделениями (Управление «К», Центр информационной безопасности ФСБ РФ) и внешними организациями (компании, предоставляющие услуги в области расследования инцидентов ИБ и обеспечения ИБ).

12. По завершении расследования оформить соответствующий отчет и составить рекомендации по снижению рисков возникновения подобных инцидентов в будущем.

13. При обращении в правоохранительные органы представить им подробное описание инцидента, описание собранных доказательств и результаты их анализа.