Приложение № 13
к Приказу от 06.02.2018 г. № 19

Порядок выявления инцидентов и реагирование на них в типовом сегменте «Информационной системы, содержащей сведения о возможностях дополнительного образования на территории Московской области»

1. Настоящий порядок выявления инцидентов и реагирования на них в иповом сегменте «Информационной системы, содержащей сведения о озможностях дополнительного образования на территории Московской бласти» (далее по тексту – информационная система) определяет меры по ыявлению инцидентов информационной безопасности и реагированию на них, оторые должны обеспечивать обнаружение, идентификацию, анализ нцидентов в информационной системе, а также принятие мер по устранению и редупреждению инцидентов.

2. Инцидент - одно событие или группа событий, которые могут привести сбоям или нарушению функционирования информационной системы и (или) к зникновению угроз безопасности информации.

3. В МАУДО ОЦЭВ за выявление инцидентов и реагирование на них ечает администратор информационной безопасности.

4. Обнаружение, идентификация и регистрация инцидентов ществляется согласно «Инструкции по регистрации событий безопасности в вом сегменте «Информационной системе, содержащей сведения о можностях дополнительного образования на территории Московской асти».

5. Работники МАУДО ОЦЭВ, должны сообщать ответственным за ление инцидентов, любые инциденты, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в системы обработки информации, в помещения обработки информации и к хранилищам информации;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы средств защиты информации;
- факты разглашения информации, содержащей персональные данные;
- факты разглашения информации о методах и способах защиты и обработки информации.

6. Все нештатные ситуации, факты вскрытия и опечатывания технических в, выполнения профилактических работ, установки и модификации тных и программных средств обработки информации в информационной е, должны быть занесены администратором информационной сности в «Журнал учета нештатных ситуаций, фактов вскрытия и вания технических средств, выполнения профилактических работ,

установки и модификации аппаратных и программных средств обработки информации» (Приложение 1).

7. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно «Порядку проведения разбирательств по фактам возникновения инцидентов в типовом сегменте Информационной системе, содержащей сведения о возможностях дополнительного образования на территории Московской области».

8. Меры по устранению последствий инцидентов, планированию и принятию мер по предотвращению повторного возникновения инцидентов, возлагаются на администратора информационной безопасности.

ремонт, установки и модификации аппаратных и программных средств обработки информации

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО администратора информационной безопасности, подпись	Примечание