БАШҠОРТОСТАН РЕСПУБЛИКАҺЫ
ДҮРТӨЙЛӨ РАЙОНЫ
МУНИЦИПАЛЬ РАЙОНЫ
ДҮРТӨЙЛӨ ҠАЛАҺЫНЫҢ 1–СЕ ҺАНЛЫ
УРТА ДӨЙӨМ БЕЛЕМ БИРЕҮ МӘКТӘБЕ
МУНИЦИПАЛЬ БЮДЖЕТ ДӨЙӨМ БЕЛЕМ
БИРЕҮ УЧРЕЖДЕНИЕҺЫ
(МБОУ СОШ №1)
452320, Башҡортостан Республикаһы
Дүртөйлө ҡалаһы, Рәзил Мусин урамы, 80
Тел. /факс (34787) 2-23-52
E-mail: dcosh1@yandex.ru

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ
ШКОЛА №1 ГОРОДА ДЮРТЮЛИ
МУНИЦИПАЛЬНОГО РАЙОНА
ДЮРТЮЛИНСКИЙ РАЙОН
РЕСПУБЛИКИ БАШКОРТОСТАН
(МБОУ СОШ №1)
Разила Мусина, 80 Дюртюлинский район,
Республика Башкортостан, 452320
Тел. /факс (34787) 2-23-52
E-mail: dcosh1@yandex.ru

ОКПО 42984743, ОГРН 1020201758510, ИНН/КПП 0260005787/026001001

БОЙОРОҠ **ПРИКАЗ**

№ 70— од

07 апрель 2025 й. 07 апреля 2025 г.

О сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них в (МБОУ СОШ № 1 г. Дюртюли)

В целях выполнения требований приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», п р и к а з ы в а ю :

1. Утвердить перечень сотрудников, ответственных за выявление инцидентов информационной безопасности и реагирование на них в МБОУ СОШ № 1 г. Дюртюли (ПРИЛОЖЕНИЕ № 1).
2. Утвердить регламент выявления инцидентов информационной безопасности и реагирования на них в МБОУ СОШ № 1 г. Дюртюли (ПРИЛОЖЕНИЕ № 2).
3. Контроль исполнения настоящего приказа оставляю за собой.

Директор Л.В. Биктанова

ПРИЛОЖЕНИЕ № 2
к приказу от 07.04.2025, № 70 – од

Регламент выявления инцидентов информационной безопасности и реагирования на них в *(наименование организации)*

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент устанавливает порядок действий по управлению инцидентами информационной безопасности в *(наименование организации)*.

1.2. Под инцидентом информационной безопасности (далее – инцидент) понимается событие или совокупность событий, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.

2. ПОРЯДОК ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЯ НА НИХ

2.1. В качестве источников информации об инцидентах могут использоваться:

– журналы и оповещения системного и прикладного программного обеспечения информационных систем, обрабатывающих защищаемую информацию, не содержащую сведения, составляющие государственную тайну (далее – ИС);

– журналы и оповещения системы защиты информации (далее – СЗИ);

– оповещения средств обнаружения вторжений;

– информация, получаемая от сотрудников *(наименование организации)*;

– информация, полученная на основе анализа защищенности ИС и контроля эффективности СЗИ.

2.2. При обнаружении инцидента сотрудник, ответственный за выявление инцидентов информационной безопасности и реагирование на них в *(наименование организации)*(далее – Ответственный за управление инцидентами), должен оповестить ответственного за обеспечение безопасности персональных данных и за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах *(наименование организации)* (далее – Ответственный за обеспечение безопасности защищаемой информации).

2.3. Ответственный за управление инцидентами должен провести анализ инцидента информационной безопасности в целях выявления факта или предпосылки негативного воздействия на защищаемую информацию, не содержащую сведения, составляющие государственную тайну (далее – защищаемая информация). В ходе анализа инцидента по возможности следует выявить следующие показатели:

– факт или потенциальная возможность реализации угрозы безопасности защищаемой информации (далее – угрозы);

– опасность угрозы;

– области, перечни информационных ресурсов, затрагиваемые воздействием угрозы;

– потенциальные нарушители, цели и причины реализации угрозы;

– перечень мер по локализации и остановке распространения действия угрозы.

2.4. Ответственный за управление инцидентами оповещает Ответственного за обеспечение безопасности защищаемой информации о ходе и результатах реагирования на инциденты.

2.5. Ответственный за управление инцидентами составляет предложения Ответственному за обеспечение безопасности защищаемой информации о недопущении повторных инцидентов. При необходимости Ответственный за обеспечение безопасности защищаемой информации обеспечивает реализацию данных предложений.