ПРИЛОЖЕНИЕ № 2
к приказу от 22.04. 2025г. № 75

Регламент выявления инцидентов информационной безопасности и реагирования на них в МОБУ СОШ с.Тазларово

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент устанавливает порядок действий по управлению инцидентами информационной безопасности в МОБУ СОШ с.Тазларово.

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 *МОБУ СОШ с.Тазларово*;

– 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 *МОБУ СОШ с.Тазларово* (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 *МОБУ СОШ с.Тазларово* (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.