МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ОТКРЫТАЯ (СМЕННАЯ) ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №11

СОГЛАСОВАНО
председатель ПК
_____ Г.А.Летина

УТВЕРЖДАЮ
Директор _____
Л.Н. Хопрова

ПОЛОЖЕНИЕ № 45

о порядке разбирательств и составления заключений по фактам нарушений информационной безопасности

Раздел 3. Локальные акты, регламентирующие отношения образовательного учреждения с работниками и организацию учебно-методической работы.

2015

Рассмотрено на Совете Учреждения

Протокол № 06 от 31.08.2015

Положение №45
о порядке разбирательств и составления заключений по фактам нарушений информационной безопасности

1.Термины и определения

1.1. Инцидент информационной безопасности – событие, в результате наступления которого организации нанесен ущерб в виде финансовых потерь, операционных и репутационных рисков (атака на информационные ресурсы организации, разглашение конфиденциальной информации, нарушение работоспособности информационных ресурсов организации, внесение несанкционированных изменений, утечка или разглашение персональных данных работников, клиентов и т.д.).

2. Общие положения

2.1. Целью настоящего Положения является определение порядка расследования инцидентов информационной безопасности.

3. Порядок регистрации

3.1. Источником информации об инциденте информационной безопасности может служить следующее:

- сообщения работников, контрагентов организации направленные в организацию виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.
- данные, полученные на основании анализа журналов регистрации информационных систем, систем защиты.

3.2. При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения "обратного" звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).

3.3. Работник, получивший информацию об инциденте, должен сообщить об этом ответственному работнику.

4. Порядок разбора

4.1. Для проведения служебного расследования приказом руководителя организации создается комиссия в составе не менее трех человек.

4.2. Комиссия обязана установить имела ли место утечка сведений конфиденциального характера и обстоятельства ей сопутствующие, установить лица, виновные в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению.

4.3. Комиссия собирает и анализирует все данные об обстоятельствах инцидента (электронные письма, логи информационных систем, показания работниковников и др.).

4.4 Результаты всех мероприятий, проводимых в процессе служебного расследования, документируются.

4.5 Служебное расследование должно проводиться в максимально короткие сроки (не более месяца со дня обнаружения факта утери/разглашения). В эти же сроки должно быть принято решение о привлечении виновных лиц к ответственности в установленном порядке.

4.6. По окончании разбора инцидента информационной безопасности комиссией оформляется отчет, в котором указываются основные "контрольные точки" инцидента.

4.7. Отчет предоставляется руководителю организации, начальнику отдела информационной безопасности. В конце отчета указывается причина возникновения инцидента и предложения по недопущению подобных инцидентов в будущем.

4.8. После окончания расследования комиссия принимает решение о наказании виновных лиц.

5. Контроль исполнения настоящего положения

5.1. Контроль надлежащего исполнения требований настоящего Положения осуществляется ответственным работником.