Утверждаю:

Директор МАУК ДО «Киевская

 детская школа искусств»

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.С.Толстых

 «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024г.

**Правила выявления инцидентов информационной безопасности**

**информационных систем персональных данных**

1. Общие положения

1.1. Правила выявления инцидентов информационной безопасности информационных систем персональных данных (далее Правила) устанавливают порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления, разбирательства и предотвращения иных инцидентов информационной безопасности в МАУК ДО «Киевская детская школа искусств» (далее – Оператор).

1.2. Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», а также иными нормативными правовыми актами действующими на территории Российской Федерации.

1.3. Настоящие Правила обязательны для работников Оператора, участвующих в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

1.4. Инцидент информационной безопасности (далее - ИБ) — это определенное событие, которое может указывать на то, что информация или данные организации были украдены или могли быть украдены, а системы защиты не сработали.

2. Выявление инцидента информационной безопасности

2.1. Основными источниками информации об инцидентах ИБ являются:

* факты, выявленные ответственным за организацию обработки персональных данных, администратором информационной безопасности и иными уполномоченными работниками должника.
* факты, установленные в результате проверок и внутреннего аудита;
* обращения субъектов персональных данных;
* запросы и предписания органов надзора за соблюдением прав субъектов персональных данных;
* иные источники информации.

2.2. Работник Оператора может выявить признаки инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям, действующего законодательства и локальных нормативных актов Оператора. Подобные сведения должны быть незамедлительно переданы выявившим их работником ответственному за организацию обработки персональных данных.

3. Принятие решения о проведении разбирательства

3.1. Ответственный за организацию обработки персональных данных (далее - Ответственный) после получения информации о предполагаемом инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа проводится проверка наличия в выявленном факте нарушений.

3.2. По усмотрению Ответственного, при отсутствии негативным последствий может быть принято решение об отсутствии необходимости в проведении проверки.

3.3. В случае наличия признаков инцидента ИБ в полученной информации, Ответственный принимает решение проведения разбирательства и информирует Директора.

4. Разбирательство инцидента ИБ

4.1. Целями разбирательства инцидентов ИБ являются:

* выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
* обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных;
* предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

4.2. Разбирательство инцидента ИБ, осуществляется Директором, ответственным за организацию обработки персональных данных и администратором информационной безопасности, если иной состав лиц не определен приказом Директора.

4.3. В ходе разбирательства ИБ, осуществляются следующие действия:

* проверка факта возникновения инцидента ИБ;
* установление размера вреда причиненного инцидентом ИБ;
* уточнение дополнительных обстоятельств;
* сбор доказательств и установления причин инцидента ИБ;
* минимизация негативных последствий инцидента ИБ;
* информирование и консультирование работников Оператора по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
* разработка мероприятий по обнаружению и предупреждению инцидентов ИБ.

4.4. В процессе проведения разбирательства инцидента ИБ обязательными для установления являются:

* дата и время совершения;
* ФИО, должность сотрудника допустившего нарушение ИБ;
* уровень угрозы инцидента ИБ;
* обстоятельства и мотивы совершения инцидента ИБ;
* информационные базы, затронутые инцидентом ИБ;
* характер и размер реального и потенциального ущерба;
* обстоятельства, способствовавшие возникновению инцидента ИБ.

4.5. На время проведения расследования лицу допустившему нарушение запрещается доступ к персональным данным субъектов и информационным базам, которые их содержат.

4.6. В ходе проведения разбирательства проводится оценка негативных последствий от инцидента ИБ. В ходе оценки учитываются:

* прямой финансовый ущерб;
* репутационный ущерб;
* потенциальный ущерб;
* косвенные потери, связанные с недоступностью сервисов, потерей информации;
* другие виды ущерба или аспекты негативных последствий для Оператора и субъектов персональных данных.

5. Завершение разбирательства

5.1. По завершению разбирательства инцидента ИБ, принимается решение по вопросу о целесообразности привлечения виновного работника к дисциплинарной ответственности.

5.2. В случае выявления в инциденте ИБ признаков административного правонарушения или уголовного преступления Оператором подается заявление в правоохранительные, либо иные органы компетентные принимать решения по указанному факту.

5.3. На основании полученных результатов разбирательства ответственный за организацию обработки персональных данных в срок не более организовывает проведение мероприятий, направленных на снижение рисков информационной безопасности в будущем.