Приложение 13
к Приказу
от 23.01.2023 г. №ОД-27

ПОРЯДОК
выявления инцидентов информационной безопасности информационных систем персональных данных
Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №125 с углубленным изучением отдельных предметов»

1. Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.
ИБ – информационная безопасности.
ИС – информационная система.
ИСПДн – информационная система персональных данных.

2. Общие положения

2.1. Настоящий Порядок устанавливает правила выявления фактов несоблюдения условий обработки защищаемой информации, использования средств защиты информации, которые могут привести к нарушению конфиденциальности, целостности и доступности защищаемой информации данных или другим нарушениям, приводящим к снижению класса защищенности государственной информационной системы, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления и предотвращения иных инцидентов информационной безопасности ИСПДн Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №125 с углубленным изучением отдельных предметов» (далее – МБОУ «СОШ №125»).

2.2. Порядок разработан в соответствии с:

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– приказом от 18.02.2013 ФСТЭК № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– иными нормативными правовыми актами, а также в соответствии с локальными нормативными актами организации.

2.3. Настоящий Порядок обязателен к соблюдению всеми пользователями ИСПДн МБОУ «СОШ №125».

2.4. Разбирательство по всем инцидентам ИБ проводится администратором

информационной безопасности МБОУ «СОШ №125».

3. Выявление инцидента информационной безопасности

3.1. Основными источниками информации об Инцидентах ИБ являются:

– факты, выявленные пользователями ИСПДн, администратором информационной системы, администратором информационной безопасности;

– результаты работы средств мониторинга ИБ результаты проверок и аудита (внутреннего или внешнего);

– запросы и предписания органов надзора;

– другие источники информации.

3.2. Пользователь ИСПДн может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям, утвержденных в локальных актах МБОУ «СОШ №125». Любые сведения о Происшествие или Инциденте ИБ должны быть незамедлительно переданы выявившим их пользователем АИБу.

4. Анализ исходной информации и принятие решения о проведении разбирательства

4.1. АИБ после получения информации о предполагаемом Инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа сотрудник проводит проверку наличия в выявленном факте нарушений.

4.2. По решению АИБа единичный Инцидент ИБ, не приведший к негативным последствиям и совершенный пользователем ИСПДн впервые, фиксируется в карточке данных «Инциденты ИБ» с присвоением статуса «Разбирательство не требуется».

4.3. В случае наличия признаков Инцидента ИБ, АИБ по общим вопросам определяет предварительную степень важности Инцидента ИБ и принимает решение о необходимости проведения разбирательства, информирует руководителя структурного подразделения (начальника отдела) об Инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

4.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте ИБ, АИБ определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

5. Разбирательство инцидента информационной безопасности

5.1. Цели и этапы разбирательства Инцидента ИБ:

Целями разбирательства инцидентов ИБ являются:

– выработка организационных и технических решений, направленных на

снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;

– защита прав пользователей ИСПДн МБОУ «СОШ №125», установленных законодательством Российской Федерации;

– обеспечение безопасности защищаемой информации данных;

– предотвращение несанкционированного доступа к защищаемой информации.

Разбирательство Инцидента ИБ, состоит из следующих этапов:

– подтверждение/опровержение факта возникновения Инцидента ИБ;

– подтверждение/корректировка уровня значимости Инцидента ИБ;

– уточнение дополнительных обстоятельств (деталей) Инцидента ИБ;

– получение (сбор) доказательств возникновения Инцидента ИБ, обеспечение их сохранности и целостности;

– минимизация последствий Инцидента ИБ;

– информирование и консультирование пользователей ИСПДн по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;

– разработка мероприятий по обнаружению и/или предупреждению инцидентов ИБ.

5.2. Создание Рабочей группы для проведения расследования Инцидента ИБ:

5.3. При необходимости АИБ незамедлительно уведомляет МБОУ «СОШ №125» о факте Инцидента ИБ и инициирует создание Рабочей группы для разбирательства указанного Инцидента ИБ. Взаимодействие между членами Рабочей группы осуществляется в рабочем порядке с соблюдением при этом требований конфиденциальности. При необходимости проводятся заседания Рабочей группы, время, место и темы которых определяются ее Руководителем. В иных случаях, АИБ может проводить расследование Инцидента ИБ самостоятельно с подготовкой всех необходимых документов.

5.4. Порядок проведения разбирательства Инцидента ИБ:

В процессе проведения разбирательства Инцидента ИБ обязательными для установления являются:

– дата и время совершения Инцидента ИБ;

– ФИО, должность и подразделение Нарушителя ИБ[1];

– уровень критичности Инцидента ИБ;

– обстоятельства и мотивы совершения Инцидента ИБ;

– информационные ресурсы, затронутые Инцидентом ИБ;

– характер и размер реального и потенциального ущерба;

– обстоятельства, способствовавшие совершению Инцидента ИБ.

После получения необходимой информации по Инциденту ИБ осуществляющий разбирательство сотрудник проводит анализ полученных данных.

Осуществляющий разбирательство сотрудник проводит оценку негативных последствий от реализации Инцидента ИБ. В ходе данной оценки учитываются:

– прямой финансовый ущерб;

---

[1] В случае внутреннего нарушителя ИБ

- репутационный ущерб;
- потенциальный ущерб;
- косвенные потери, связанные с недоступностью сервисов, потерей информации;
- другие виды ущерба или аспекты негативных последствий для МБОУ «СОШ №125» или ее пользователей.

В течение 5 (пяти) рабочих дней с момента назначения осуществляющего разбирательство сотрудника (формирования Рабочей группы), осуществляющий разбирательство сотрудник запрашивает у руководителя структурного подразделения (начальника отдела) объяснительную записку Нарушителя ИБ[2]. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение (двух) рабочих дней и представлена его непосредственным руководителем осуществляющему разбирательство сотруднику в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа Нарушителя ИБ предоставить объяснительную записку, осуществляющему разбирательство сотруднику предоставляется акт, составленный в соответствии с установленным порядком.

С целью минимизации последствий Инцидента ИБ возможно временное отключение прав доступа сотрудника к Информационным системам (ИС) на время проведения расследования предварительно сделав заявку. Подобное отключение инициируется осуществляющим разбирательство сотрудником с обязательным предварительным устным согласованием с руководителем Нарушителя.

В случае, если у Нарушителя ИБ были отключены права доступа к ИС на время проведения разбирательства, то по его результатам осуществляющий разбирательство сотрудник по согласованию с руководителем Нарушителя ИБ принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у Нарушителя ИБ прав доступа к ИС либо инициирует официальную процедуру отмены (изменения) прав доступа к ИС в соответствии с установленным порядком в МБОУ «СОШ №125». Если Нарушение ИБ было вызвано незнанием Нарушителем ИБ правил (технологии) работы с информационными ресурсами высокого уровня безопасности, то основанием для возврата прав доступа является успешное прохождение повторного инструктажа сотрудниками отделов, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами МБОУ «СОШ №125».

Восстановление временно отключенных у Нарушителя ИБ прав доступа к ИС (разблокировка пользователя) может производиться только по заявке руководителя Нарушителя ИБ или осуществляющего разбирательство сотрудника.

6. Оформление результатов проведенного разбирательства

6.1. Собранная в процессе разбирательства Инцидента ИБ информация фиксируется осуществляющим разбирательство сотрудником в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по Инциденту

[2] В случае внутреннего нарушителя ИБ

ИБ.

6.2. Осуществляющий разбирательство сотрудник формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию Инцидента ИБ.

6.3. Итоговое заключение по Инциденту ИБ осуществляющий разбирательство сотрудник направляет начальнику МБОУ «СОШ №125».

6.4. Осуществляющий разбирательство сотрудник фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

6.5. Осуществляющий разбирательство сотрудник, при необходимости определения правовой оценки Инцидента ИБ, может обратиться за консультациями в другие подразделения МБОУ «СОШ №125» и соответствующие организации. В этом случае информацию по инциденту ИБ осуществляющий разбирательство сотрудник передает с грифом «Конфиденциально».

6.6. В случае выявления в инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, осуществляющий разбирательство сотрудник передает все материалы по Инциденту ИБ начальнику МБОУ «СОШ №125» для принятия решения, в соответствии с установленным порядком, о подаче заявления в правоохранительные органы Российской Федерации.

6.7. Осуществляющий разбирательство сотрудник фиксирует полученную дополнительную информацию в карточке данных «Инциденты ИБ» и информирует начальника МБОУ «СОШ №125».

7. Завершение разбирательства, превентивные мероприятия

7.1. По завершению разбирательства Инцидента ИБ, осуществляющий разбирательство сотрудник передает имеющиеся материалы (в объеме, достаточном для принятия решения) вышестоящему руководителю Нарушителя ИБ[3] для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.

7.2. На основании полученных результатов разбирательства руководитель структурного подразделения в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

- повторное ознакомление Нарушителя ИБ с Правилами;
- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у Нарушителя ИБ;
- доведение до всех пользователей ИСПДн требований внутренних нормативных документов МБОУ «СОШ №125»;
- отмена неактуальных прав доступа к информационным ресурсам;
- проведение мероприятий, направленных на предотвращение

[3] Здесь и далее- В случае внутреннего нарушителя ИБ

несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

– и другие обоснованные мероприятия.

8. Права, обязанности и ответственность участников разбирательства

8.1. Осуществляющий разбирательство сотрудник имеет право:

– по согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам Инцидента ИБ у Нарушителя ИБ;

– запрашивать и получать от пользователей ИСПДн, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства Инцидента ИБ;

– инициировать на основании заявок отключение от информационных ресурсов пользователей ИСПДн, нарушивших правила или требования ИБ, на период проведений расследования Инцидента ИБ в случае, если имеется существенный риск того, что продолжение пользователя с ИС может повлечь значительное увеличение ущерба или новые инциденты ИБ;

– инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной/ материальной ответственности.

8.2. Осуществляющий разбирательство сотрудник обязан:

– объективно и основательно проводить разбирательство каждого инцидента ИБ;

– определять первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий;

– фиксировать в карточке данных «Инциденты ИБ» всю исходную информацию об инциденте ИБ и результаты его расследования;

– предоставлять отчеты и рекомендации по проведенным разбирательствам начальнику МБОУ «СОШ №125»;

– проводить анализ обстоятельств, способствовавших совершению каждого инцидента ИБ, и на его основе, разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных Инцидентов ИБ и минимизации возможности их повторения в будущем;

– составление заключений по фактам инцидентов ИБ, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

8.3. Пользователи ИСПДн обязаны:

– предоставлять по запросам проводящего разбирательство сотрудника устные и письменные разъяснения и иную информацию в рамках своей компетенции,

– необходимую для проведения разбирательства Инцидента ИБ;

– информировать АИБа о выявленных Инцидентах ИБ.