Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа № 24»

Принято
на общем собрании
трудового коллектива
протокол № 3
« 27 » августа 2021 г.

Утверждаю
Директор МБОУ «СОШ № 24»
Приказ № 69/17-ОД
« 31 » августа 2021 г.

Регламент
реагирования на инциденты информационной безопасности

1. Общие положения

1.1. Настоящий регламент реагирования на инциденты информационной безопасности (далее - Регламент) устанавливает порядок реагирования на инциденты информационной безопасности, 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, разработки и принятия мер по предотвращению возможных опасных последствий подобных нарушений, а также выявления, расследования и предотвращения иных инцидентов информационной безопасности в МБОУ «СОШ №24» (далее – Школа).

1.2. Регламент разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иными нормативными правовыми актами.

1.3. Настоящий Регламент обязателен к соблюдению всеми работниками Школы, участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности (далее – ИБ).

1.4. Разбирательство по всем инцидентам ИБ проводится постоянно действующей комиссией по информационной безопасности (далее – ПДК).

2. Выявление инцидента информационной безопасности

2.1. Основными источниками информации об инцидентах ИБ являются:

- факты, выявленные директором, заместителями директора школы, членами ПДК по ИБ, лицом ответственным по обеспечению информационной безопасности в школе, назначенным приказом по школе, а также другими сотрудниками организации.
- результаты работы средств мониторинга ИБ, проверок и аудита (внутреннего или внешнего);
- журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;
- обращения субъектов персональных данных с указанием инцидента ИБ;
- запросы и предписания органов надзора за соблюдением прав субъектов персональных данных;
- другие источники информации.

2.2. Основными видами инцидентов ИБ в школе являются:

- разглашение конфиденциальной или внутренней информации либо угроза такого разглашения;
- несанкционированный доступ лиц, не имеющих легального доступа к ресурсам или помещениям организации;
- превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников школы;
- компрометация учетных записей или паролей;
- вирусная атака или вирусное заражение;
- нарушение или сбои в работе системы резервного копирования;
- нарушение правил использования персональных данных.

2.3. Сотрудник Школы может выявить признаки наличия инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям защиты информации, утвержденным в Школе.

Выявленные несоответствия дают основания предполагать факт возникновения инцидента ИБ. Любые сведения о происшествии или инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником ответственному за информационную безопасность.

3. Анализ исходной информации и принятие решения о проведения разбирательства

3.1. Ответственный за обеспечение ИБ после получения информации о предполагаемом инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа проводит проверку наличия в выявленном факте нарушений.

3.2. По усмотрению ответственного за обеспечение ИБ единичный инцидент ИБ, не повлекший негативные последствия и совершенный сотрудником Школы впервые, фиксируется в карточке данных об инциденте ИБ (приложение 1 к Регламенту на инциденты ИБ) с присвоением статуса «Разбирательство не требуется».

3.3. В случае наличия признаков инцидента ИБ, повлекшего негативные последствия, ответственный за обеспечение ИБ классифицирует инцидент, определяет его предварительную степень важности, принимает решение о необходимости проведения расследования, информирует директора Школы либо его заместителя об инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса в процессе расследования.

3.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте ИБ, ответственный за обеспечение ИБ по согласованию с директорм школы определяет и инициирует первоочередные меры, направленные на локализацию инцидента и минимизацию его последствий.

4. Разбирательство инцидента информационной безопасности

4.1. Цели и этапы разбирательства инцидента ИБ:

4.1.1. Целями разбирательства инцидентов ИБ являются:

- выработка организационных и технических решений, направленных на снижение рисков нарушения ИБ, предотвращение и минимизацию подобных нарушений в будущем;
- защита прав Школы, установленных законодательством Российской Федерации;
- защита репутации Школы и их информационных ресурсов;
- обеспечение безопасности персональных данных;
- защита прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых в Школе;
- предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство инцидента ИБ состоит из следующих этапов:

- подтверждение/опровержение факта возникновения инцидента ИБ;
- классификация 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 персонала школы по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
- переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил ИБ.

4.2. Порядок проведения разбирательства инцидента ИБ:

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

- дата и время совершения инцидента ИБ;
- ФИО и должность нарушителя ИБ;
- классификация инцидента;
- 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.

4.2.2. При инциденте ИБ, ответственный за обеспечение ИБ информирует о факте инцидента директора Школы.

4.2.3. Осуществляющий разбирательство ответственный за обеспечение ИБ в процессе проведения расследования инцидента ИБ, после получения необходимой информации проводит анализ полученных данных.
4.2.4. В течение 5 (пяти) рабочих дней с момента выявления инцидента ИБ ответственный за обеспечение ИБ запрашивает от нарушителя ИБ объяснения. Объяснительная записка должна быть составлена, подписана нарушителем ИБ в течение (двух) рабочих дней и представлена ответственному за обеспечение ИБ в течение 3 (трех) рабочих дней с момента поступления запроса.
4.2.5. Ответственный за обеспечение ИБ проводит оценку негативных последствий инцидента ИБ. В ходе данной 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 субъектов персональных данных.
4.2.6. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа сотрудника к информационным ресурсам (ИР) на время проведения расследования. Подобное отключение инициируется ответственным за обеспечение ИБ при условии его обязательного предварительного устного согласования с директором Школы.
4.2.7. В случае, если у нарушителя ИБ были отключены права доступа к ИР на время проведения расследования, по его результатам ответственный за обеспечение ИБ по согласованию с директором Школы принимает решение о возвращении в полном или ограниченном объеме ранее имеющихся у нарушителя ИБ прав доступа к ИР и инициирует возвращение указанных прав в соответствии в данным решением либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР в соответствии с установленным порядком доступа к информационным, программным и аппаратным ресурсам школы. Если нарушение ИБ было вызвано незнанием нарушителем ИБ правил (технологии) работы с информационными ресурсами, то основанием для возврата прав доступа является успешное прохождение инструктажа по информационной безопасности, по результатам изучения соответствующих локальных нормативных актов школы.
4.2.8. Восстановление временно отключенных у нарушителя ИБ прав доступа к информационным ресурсам (разблокировка пользователя) может производиться только ответственный за обеспечение ИБ.

5. Оформление результатов проведенного разбирательства
5.1. Собранная в процессе разбирательства инцидента ИБ информация фиксируется ответственным за обеспечение ИБ в карточке данных об инциденте ИБ и учитывается при подготовке итогового заключения по инциденту ИБ.
5.2. Ответственный за обеспечение ИБ формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента ИБ.
5.3. Итоговое заключение по инциденту ИБ ответственный за обеспечение ИБ направляет директору Школы.
5.4. Ответственный за обеспечение ИБ фиксирует завершение разбирательства в карточке инцидента ИБ и присваивает инциденту статус «Разбирательство завершено».
5.5. В случае выявления в инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, ответственный за обеспечение ИБ передает все материалы по инциденту ИБ директору Школы для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

6. Завершение разбирательства, превентивные мероприятия
6.1. По завершении расследования инцидента ИБ ответственный за обеспечение ИБ передает имеющиеся материалы (в объеме, достаточном для принятия решения) директору Школы для решения вопроса о целесообразности привлечения нарушителя ИБ к дисциплинарной ответственности.
6.2. На основании полученных результатов расследования директор Школы совместно с ответственным за обеспечение ИБ в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков ИБ в будущем:
- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя ИБ;
- доведение до всех сотрудников структурного подразделения требований внутренних нормативных документов Школы;
- обсуждение инцидента ИБ на оперативном совещании;
- отмена неактуальных прав доступа к информационным ресурсам;

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

6.3. О результатах проведенного расследования инцидента ИБ ответственный за обеспечение ИБ письменно докладывает директору Школы.

7. Права, обязанности и ответственность участников разбирательства

7.1. Ответственный за обеспечение ИБ имеет право:

- по согласованию с директором Школы требовать у нарушителя ИБ письменные объяснения по обстоятельствам инцидента ИБ;
- запрашивать и получать от сотрудников Школы, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для расследования инцидента ИБ;
- инициировать отключение от информационных ресурсов сотрудников школы, нарушивших правила или требования ИБ, на период проведений расследования инцидента ИБ, если имеется существенный риск того, что продолжение работы сотрудника с информационными ресурсами может повлечь значительное увеличение ущерба или новые инциденты ИБ;
- по результатам расследования инцидента ИБ инициировать изменения в процессах и информационных ресурсах школы с целью повышения их защищенности и снижения рисков инцидентов ИБ;
- инициировать процедуры привлечения нарушителя ИБ к дисциплинарной и (или) материальной ответственность согласно требованиям внутренних нормативных документов Школы.

7.2. Ответственный за обеспечение ИБ обязан:

- объективно проводить расследование каждого инцидента ИБ;
- определять первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий;
- фиксировать в карточке данных об инцидентах ИБ всю исходную информацию об инциденте ИБ и результаты его расследования;
- предоставлять отчеты и рекомендации по результатам проведенных расследований директору Школы;
- проводить анализ обстоятельств, способствовавших возникновению каждого инцидента ИБ, и на его основе совместно с отделом информационных технологий разрабатывать рекомендации и предложения по оптимизации процессов, снижению ущерба от подобных инцидентов ИБ и предотвращению возможности их повторения в будущем.

7.3. Сотрудники школы обязаны:

- предоставлять по запросам ответственного за обеспечение ИБ устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения расследования инцидента ИБ;
- информировать ответственный за обеспечение ИБ о выявленных инцидентах ИБ;

Приложение 1
к Регламентуреагирования на инциденты
информационной безопасности,
утверждено приказом директора
от _____ № _____

Карточка данных об инциденте ИБ

Дата события
Номер события

Информация о сообщающем лице

Фамилия _____
Организация _____
Адрес _____
Электронная почта _____
Телефон _____

Описание события ИБ Описание события:

- Что произошло
- Как произошло
- Почему произошло
- Пораженные компоненты
- Негативное воздействие на ИСПДн
- Любые идентифицированные уязвимости

Детали события ИБ

Дата и время возникновения события_____
Дата и время обнаружения события_____
Дата и время сообщения о событии_____
Классификация события_____
Закончилось ли событие? *(отметить квадрат*) Да □ Нет □
Если «да», то уточнить, как долго длилось событие в днях/часах/минутах_____
_____

Тип инцидента ИБ *(Отметить один квадрат, затем заполнить соответствующие поля ниже)*
Действительный □ Попытка □ Подозрение □

(один из) Намеренная □ *(указать типы угрозы)*
Хищение □ Хакерство/Логическое проникновение □
Мошенничество □ Неправильное использование ресурсов □
Саботаж/физический ущерб □ Другой ущерб □
Вредоносная программа □

Определить:
(один из) Случайная □ *(указать типы угрозы)*
Другие природные события □

Отказ ПО □ *Определить:*

Отказ связи □ Потеря существенных сервисов □

Отказ аппаратуры □ Недостаточное кадровое обеспечение □

Пожар, наводнение □ Другие случаи □

Отказ электропитания □ *Определить:*

(Один из) Ошибка □ *(указать типы угрозы)*

Операционная ошибка □ Ошибка пользователя □

Ошибка аппаратной поддержки □ Ошибка конструкции □

Ошибка поддержки ПО □ Другие случаи (включая истинные заблуждения) □

Неизвестно □

Определить:

(Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)

Определить:

Пораженные активы

Пораженные активы (если есть) *(Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности)*

Информация/Данные _____

Аппаратура _____

Программное обеспечение _____

Средства связи _____

Документация _____

Негативное воздействие/влияние инцидента

Отметить соответствующие квадраты для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на бизнес по шкале 1+10, используя сокращения (указатели категорий): (ФП) - финансовые потери/разрушение бизнес-операций, (КИ) - коммерческие и экономические интересы, (ПД) - информация, содержащая персональные данные, (ПО) - правовые и нормативные обязательства, (БО) - менеджмент и бизнес-операции, (ПП) - потеря престижа. Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость»

	Значимость	Указатели	Стоимость
Нарушение конфиденциальности *(т. е., несанкционированное раскрытие)*	□		
Нарушение целостности *(т. е., несанкционированная модификация)*	□		
Нарушение доступности *(т. е., недоступность)*	□		
Нарушение неотказуемости	□		
Уничтожение	□		

Полные стоимости восстановления после инцидента

(Где возможно, необходимо указать общие расходы на восстановление после инцидента в целом по шкале 1+10 для «значимости» и в деньгах для «стоимости»)	Значимость	Указатели	Стоимость

Разрешение инцидента

Дата начала расследования инцидента _____
Фамилия лица (лиц), проводившего (их) расследование инцидента _____
Дата окончания инцидента _____
Дата окончания воздействия _____
Дата завершения расследования инцидента _____
Ссылка и место хранения отчета о расследовании_____

(один из)

Лицо
Причастные лица
Организованная группа
Легально учрежденная организация/учреждение
Случайность
Нет виновного

Например, природные факторы, отказ оборудования, ошибка человека

Описание нарушителя

Действительная или предполагаемая мотивация

(один из)

Криминальная/финансовая выгода
Развлечение/хакерство
Политика/Терроризма
Реванш
Другие мотивы
Определить:

Действия, предпринятые для разрешения инцидента *(например, «никаких Действий», «поДручными средствами», «внутреннее расследование», «внешнее расследование с привлечением...»)*

Действия, запланированные для разрешения инцидента *(например, см. выше)*

Прочие действия *(например, по-прежнему требуется проведение расследования для другого персонала)*

Заключение

(Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения)

Значительный
Незначительный

(Укажите любые Другие заключения) _____

Ознакомленные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые Действия

Администратор ИБ
Руководитель подразделения (уточнить какого)
Автор отчета
Полиция
Руководитель организации
Начальник отдела информационных технологий
Начальник отдела кадров
Другое лицо

(например, служба охраны, регулятивного органа, сторонняя организация) Определить:

Привлеченные лица

Инициатор
Подпись _____
Фамилия _____
Роль _____
Дата _____

Аналитик
Подпись _ _____
Фамилия_____
Роль _____
Дата _____

Аналитик
Подпись _ _____
Фамилия_____
Роль _____
Дата _____