Муниципальное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 95 г. Нижний Тагил

ОБСУЖДЕН
Педагогическим советом
МБОУ СОШ № 95
(протокол от 28.08.2025г. № 1)

УТВЕРЖДЕН
Директор МБОУ СОШ № 95
Е. В. Репина
(приказ от 30.08.2025г. № 141/2
приложение № 12)

РЕГЛАМЕНТ
РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ (УТЕЧКИ), СВЯЗАННЫЕ С ОБРАБОТКОЙ И ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящий Регламент реагирования на инциденты (утечки), связанные с обработкой и защитой персональных данных, определяет порядок выявления, фиксации, оценки, локализации, расследования, устранения последствий и уведомления об инцидентах безопасности персональных данных (далее – Инциденты, ПДн) в МБОУ СОШ № 95 г. Нижнего Тагила (далее – Школа, Оператор).
1.2. Регламент разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ-152), Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Трудовым кодексом РФ, Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Политикой в отношении обработки ПДн МБОУ СОШ № 95, Положением об обработке и защите ПДн сотрудников, обучающихся и третьих лиц МБОУ СОШ № 95, Порядком уничтожения и обезличивания ПДн МБОУ СОШ № 95, Методическими рекомендациями Роскомнадзора по реагированию на инциденты в сфере ПДн.
1.3. Регламент обязателен для исполнения всеми работниками Школы, имеющими доступ к ПДн, а также контрагентами, обрабатывающими ПДн по поручению Оператора.
1.4. Основные понятия, используемые в Регламенте:
1) инцидент безопасности ПДн – любое событие, приведшее или способное привести к несанкционированному или неправомерному доступу, копированию, передаче, изменению, блокированию, уничтожению ПДн, либо к нарушению их конфиденциальности, целостности или доступности.
2) утечка ПДн – факт неправомерной передачи или распространения ПДн за пределы контролируемой среды Школы.
3) время обнаружения – момент, когда Оператор получил достоверную информацию о возможном или состоявшемся Инциденте.

2. Классификация инцидентов (утечек), связанных с обработкой и защитой персональных данных

2.1. Инциденты классифицируются по уровню критичности для определения масштаба реагирования:
1) Уровень 1 (Критический): массовая утечка (более 100 субъектов), компрометация специальных/биометрических данных, внешняя хакерская атака, шифрование данных (программы-вымогатели), угроза жизни/здоровью субъектов.
2) Уровень 2 (Значительный): утечка/доступ к данным отдельных субъектов (менее 100), несанкционированное копирование внутренних баз, утеря носителей с ПДн, нарушение прав доступа.
3) Уровень 3 (Низкий): технические ошибки конфигурации, единичные случаи несанкционированного просмотра без извлечения, подозрительная активность без подтверждения компрометации.
2.2. Классификация проводится должностным лицом, ответственным за организацию обработки ПДн, назначаемым приказом директора Школы, в течение 4 часов с момента первичного оповещения.

3. Группа реагирования и распределение ответственности между членами группы

3.1. Для реагирования на Инциденты приказом директора Школы создается постоянно действующая Группа реагирования (далее – Группа) в следующем составе:
1) Руководитель Группы: должностное лицо, ответственное за организацию обработки ПДн (назначается приказом директора);
2) Технический специалист: системный администратор / специалист по информационной безопасности (ИБ);
3) Специалист по кадровому делопроизводству (при наличии).
4) Секретарь/Делопроизводитель (документальное сопровождение).
3.2. Директор Школы принимает окончательные решения о направлении уведомлений в государственные органы, приостановке обработки и привлечении внешних экспертов.
3.3. Все работники Школы обязаны в срок не более 1 рабочего часа сообщить руководителю Группы о любых признаках Инцидента (п. 2.5 Обязательства о неразглашении Положения об обработке и защите персональных данных сотрудников (соискателей), обучающихся и третьих лиц, Приложение № 1 к Положению).

4. Порядок выявления и первичного реагирования на инциденты (утечки), связанные с обработкой и защитой персональных данных

4.1. Выявление осуществляется посредством мониторинга информационных систем персональных данных (ИСПДн), анализа журналов доступа, сообщений сотрудников, обращений субъектов ПДн, уведомлений от государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации **(**ГосСОПКА), правоохранительных органов или СМИ.
4.2. Руководитель Группы регистрирует событие в «Журнале учета инцидентов ПДн» (Приложение № 1) с указанием даты, времени, источника информации и предварительных признаков.

4.3. Первичные меры локализации осуществляются в последующие за Инцидентом 2-а часа и включают в себя следующие действия:
1) Изоляцию затронутых АРМ, серверов или учетных записей от сети;
2) Блокировку учетных записей, сброс паролей;
3) Запрет на копирование, удаление или перезапись данных на затронутых носителях;
4) Фиксацию состояния системы (скриншоты, экспорт логов, сохранение метаданных).
4.4. Запрещается самостоятельно устранять последствия Инцидента до проведения технического анализа и фиксации доказательной базы.

5. Оценка, локализация и расследование Инцидента

5.1. Оценка масштаба Инцидента проводится в срок до 4 часов с момента его возникновения и включает в себя следующие действия:
Группа определяет:
1) Категорию и объем затронутых ПДн;
2) Количество затронутых субъектов;
3) Канал и причину компрометации;
4) Наличие признаков состава преступления (ст. 137, 272, 273 УК РФ).
5.2. Технический специалист проводит анализ журналов событий, проверку на наличие вредоносного ПО, выявление вектора атаки, оценку эффективности применяемых средств защиты.
5.3. По итогам оценки, локализации и расследования Инцидента составляется «Акт расследования инцидента ПДн» (Приложение № 2), содержащий причины, последствия, принятые меры и рекомендации по предотвращению повторения.
5.4. Срок проведения расследования не должен превышать 5 рабочих дней с момента обнаружения, за исключением случаев, требующих привлечения правоохранительных органов.

6. Уведомление и взаимодействие с государственными органами и субъектами ПДн

6.1. Оператор обязан направить уведомление об Инциденте в территориальный орган Роскомнадзора по Свердловской области в срок не более 24 часов с момента обнаружения (ч. 1 ст. 22.1 ФЗ № 152-ФЗ). Уведомление направляется в электронной форме через личный кабинет Оператора или на бумажном носителе и содержит:
1) дату и время обнаружения;
2) описание характера и объема затронутых ПДн;
3) принятые меры по локализации и минимизации вреда;
4) контактные данные ответственного лица.
6.2. При установлении факта утечки, создающей риск нарушения прав и законных интересов субъектов персональных данных, Школа информирует их в 5-дневный срок о характере Инцидента, возможных последствиях и рекомендациях по защите.
6.3. При наличии признаков уголовного правонарушения Школа направляет заявление в органы внутренних дел или Следственный комитет РФ в установленном порядке.
6.4. Все уведомления регистрируются в Журнале учета инцидентов с указанием реквизитов отправленных документов.

7. Устранение последствий и восстановление работоспособности

7.1. После локализации и расследования Группа разрабатывает План устранения последствий, утверждаемый директором Школы.

7.2. Мероприятия плана могут включать: устранение выявленных уязвимостей (обновление ПО, настройка прав доступа, замена сертификатов); восстановление данных из верифицированных резервных копий (если применимо); проверку целостности ИСПДн средствами антивирусной защиты и контроля целостности; дополнительный инструктаж или дисциплинарные взыскания (при выявлении вины сотрудников).

7.3. Контроль эффективности принятых мер осуществляется ответственным лицом за организацию обработки ПДн в течение 30 дней после закрытия Инцидента.

8. Документирование, учет и хранение

8.1. Каждый Инцидент подлежит обязательной регистрации в «Журнале учета инцидентов ПДн». Документация по Инциденту (журнал, акты расследования, копии уведомлений, протоколы заседаний Группы, технические отчеты) ведется в электронном виде лицом, ответственным за обработку и защиту персональные данных с его добровольного согласия и за дополнительную оплату хранится в защищенном виде у ответственного лица в течение не менее 3 (трех) лет с даты закрытия Инцидента, если иное не установлено законодательством РФ.

8.2. Доступ к документации Инцидентов ограничен. Выдача копий осуществляется только по письменным запросам Роскомнадзора, суда или правоохранительных органов на основании официальных запросов.

9. Профилактика, обучение и внутренний контроль

9.1. Школа проводит не реже одного раза в год плановый аудит соответствия обработки ПДн требованиям ФЗ № 152-ФЗ и настоящего Регламента.

9.2. Все работники, имеющие доступ к ПДн, проходят вводный и периодические инструктажи по информационной безопасности и действиям при Инцидентах под подпись.

9.3. Не реже одного раза в год проводятся учебные тренировки (учения) по отработке алгоритма реагирования на Инциденты ПДн с фиксацией результатов в акте.

9.4. По результатам расследования Инцидентов Регламент, действующие в Школе технические меры защиты и локальные акты Школы актуализируются приказом Директора.

10. Заключительные положения

10.1. Настоящий Регламент вступает в силу с даты утверждения приказом Директора Школы и действует бессрочно до его отмены или замены новой редакцией.

10.2. Изменения вносятся приказом Директора при изменении законодательства РФ, внедрении новых ИСПДн или изменении организационной структуры.

10.3. Контроль за исполнением Регламента осуществляет должностное лицо, ответственное за организацию обработки ПДн.

10.4. С текущей редакцией Регламента можно ознакомиться на официальном сайте МБОУ СОШ № 95 и в канцелярии Школы.

Приложение № 1

ЖУРНАЛ УЧЕТА ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

№ п/п	Дата и время обнаружения	Источник информации / Кто сообщил	Описание инцидента (кратко)	Уровень критичности	Дата и способ уведомления Роскомнадзора	Ответственный за расследование	Дата закрытия инцидента	Примечание

Журнал ведется непрерывно, страницы нумеруются, прошиваются и скрепляются печатью Школы.
Ответственный за ведение: _____ (ФИО, должность).

Приложение № 2

ФОРМА АКТА РАССЛЕДОВАНИЯ ИНЦИДЕНТА (УТЕЧКИ) ПЕРСОНАЛЬНЫХ ДАННЫХ

Муниципальное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 95 г. Нижний Тагил Свердловской области
(МБОУ СОШ № 95)

«___» _____ 20___ г. г. Нижний Тагил

1. Общие сведения:
1) Дата/время обнаружения: _____
2) Дата/время локализации: _____
3) Выявлено (ФИО, должность): _____
2. Характер и масштаб инцидента:
1) Тип инцидента: [ ] несанкционированный доступ [ ] утеря носителя [ ] внешняя атака [ ] ошибка сотрудника [ ] иное: _____
2) Затронутые категории ПДн: _____
3) Ориентировочный объем/количество субъектов: _____
3. Причины и вектор компрометации: _____
_____
_____
4. Принятые меры локализации и минимизации вреда: _____
_____
_____
5. Уведомлены:
1) Роскомнадзор: дата/номер исходящего документа _____
2) Субъекты ПДн: дата/способ _____
3) Правоохранительные органы: дата/орган _____
6. Выводы и рекомендации по устранению уязвимостей: _____
_____
_____
7. Состав комиссии/Группы реагирования:
_____ (подпись, ФИО, должность)
_____ (подпись, ФИО, должность)
_____(подпись, ФИО, должность)

УТВЕРЖДАЮ
Директор МБОУ СОШ № 95
_____ /_____/
«____» _____ 20___ г.

М.П.

Приложение № 3

АЛГОРИТМ ДЕЙСТВИЙ ПРИ ОБНАРУЖЕНИИ ИНЦИДЕНТА (УТЕЧКИ) ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Сотрудник обнаруживает признаки Инцидента → Немедленно (≤1 часа) сообщает ответственному за обработку и защиту ПДн по Школе.
2. Ответственный за обработку и защиту ПДн по Школе регистрирует событие в Журнале, собирает Группу реагирования.
3. Технические меры (≤2 часов): изоляция систем, блокировка учеток, фиксация логов, запрет на удаление данных.
4. Оценка и классификация (≤4 часов): определение уровня, объема, категорий ПДн.
5. Расследование и Акт (≤5 рабочих дней): выявление причин, оформление Акта расследования.
6. Уведомление (≤24 часов от обнаружения): направление отчета в Роскомнадзор, информирование субъектов (при риске), заявление в ОВД/СК (при признаках преступления).
7. Устранение и восстановление: патч-менеджмент, смена паролей, восстановление из бэкапов, проверка защищенности.
8. Закрытие инцидента: утверждение Акта Директором, архивирование документации, проведение внепланового инструктажа при необходимости.
9. Внесение изменений в локальные акты/технические настройки (при выявлении системных недостатков).