

СОГЛАСОВАНО  
Председатель профсоюзного  
комитета МОБУ ООШ  
с.Староиликово  
\_\_\_\_\_  
З.М. Галлямова  
Протокол № 11  
от « 27 » марта 2025 г.

УТВЕРЖДАЮ  
Директор МОБУ ООШ  
с.Староиликово  
\_\_\_\_\_  
Э.А. Гайсина  
Приказ № 49  
от « 27 » марта 2025 г.

## **ПОРЯДОК**

### **реагирования на инциденты информационной безопасности**

#### **1. Общие положения**

1.1. Настоящая инструкция реагирования на инциденты информационной безопасности (далее - Инструкция реагирования) 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 МОБУ ООШ с.Староиликово (далее – ОО)

1.2. Инструкция реагирования разработана 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. Настоящая Инструкция реагирования обязательна к соблюдению всеми работниками МОБУ СОШ № 4 им. А.Я. Першина г. Благовещенска, 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) с привлечением в необходимых случаях сотрудников других подразделений.

#### **2. Выявление инцидента информационной безопасности**

2.1. Основными источниками информации об инцидентах ИБ являются:

- факты, выявленные руководителем, заместителями руководителя, членами ПДК по ИБ, лицом ответственным по обеспечению информационной безопасности в школе, администратором информационной безопасности, 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 ОО;
- компрометация учетных записей или паролей;
- вирусная атака или вирусное заражение;
- нарушение или сбой в работе системы резервного копирования; - нарушение правил использования персональных данных.

2.3. Сотрудник ОО 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 администратору информационной безопасности.

### **3. Анализ исходной информации и принятие решения о проведения разбирательства**

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

3.2. По усмотрению администратора ИБ единичный инцидент ИБ, не повлекший негативные последствия и совершенный сотрудником ОО впервые, фиксируется администратором ИБ в карточке данных об инциденте ИБ (приложение 1 к инструкции реагирования на инциденты информационной безопасности) с присвоением статуса «Разбирательство не требуется».

3.3. В случае наличия признаков инцидента ИБ, повлекшего негативные последствия, администратор ИБ классифицирует инцидент, определяет его предварительную степень важности, принимает решение о необходимости проведения расследования, информирует руководителя ОО 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, администратор ИБ по согласованию с руководителем ОО 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 информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
- защита прав ОУ, установленных законодательством Российской Федерации;
- защита репутации ОУ и их информационных ресурсов;
- обеспечение безопасности персональных данных;

- защита прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых в ОУ;
- 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 ОО 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, должность и подразделение 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, затрагивающем не более одного структурного подразделения, администратор ИБ информирует о факте инцидента руководителя соответствующего структурного подразделения.

4.2.3. При инциденте ИБ, затрагивающем более одного структурного подразделения, администратор ИБ информирует руководителей соответствующих подразделений и инициирует проведение разбирательства.

4.2.4. В случае проведения временного отключения прав доступа у предполагаемого нарушителя ИБ информация об отключении прав доступа администратором ИБ направляется руководителю предполагаемого нарушителя ИБ.

4.2.5. Осуществляющий разбирательство администратор ИБ в процессе проведения расследования инцидента ИБ при необходимости запрашивает информацию в структурных подразделениях, направляя запрос на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

4.2.6. После получения необходимой информации по инциденту ИБ осуществляющий расследование администратор ИБ проводит анализ полученных данных.

4.2.7. В течение 5 (пяти) рабочих дней с момента выявления инцидента ИБ администратор ИБ запрашивает у руководителя структурного подразделения полученные от нарушителя ИБ объяснения. Объяснительная записка должна быть составлена, подписана нарушителем ИБ в течение (двух) рабочих дней и представлена его непосредственным руководителем администратору ИБ в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа нарушителя ИБ предоставить объяснительную записку администратор ИБ составляет акт, составленный в соответствии с установленным в школе порядком.

4.2.8. Администратор 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 Администрации или субъектов персональных данных.

4.2.9. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа сотрудника к информационным ресурсам (ИР) на время проведения расследования. Подобное отключение инициируется администратором ИБ при условии его обязательного предварительного устного согласования с руководителем сотрудника.

4.2.10. В случае если у нарушителя ИБ были отключены права доступа к ИР на время проведения расследования, по его результатам администратор ИБ по согласованию с руководителем нарушителя ИБ 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 с данным решением либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР в соответствии с установленным порядком доступа к информационным, программным и аппаратным ресурсами ОО. 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 ОО.

4.2.11. Восстановление временно отключенных у нарушителя ИБ прав доступа к информационным ресурсам (разблокировка пользователя) может производиться только администратором ИБ.

## **5. Оформление результатов проведенного разбирательства**

5.1. Собранная в процессе разбирательства инцидента ИБ информация фиксируется администратором ИБ в карточке данных об инциденте ИБ и учитывается при подготовке итогового заключения по инциденту ИБ.

5.2. Администратор ИБ формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента ИБ.

5.3. Итоговое заключение по инциденту ИБ администратор ИБ направляет всем заинтересованным руководителям структурных подразделений.

5.4. Администратор ИБ фиксирует завершение разбирательства в карточке инцидента ИБ и присваивает инциденту статус «Разбирательство завершено».

5.5. Администратор ИБ, при необходимости определения правовой оценки инцидента ИБ, может обратиться за консультациями в юридическое подразделение Администрации.

5.6. В случае выявления в инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, администратор ИБ передает все материалы по инциденту ИБ руководству ОО для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

## **6. Завершение разбирательства, превентивные мероприятия**

6.1. По завершении расследования инцидента ИБ администратор ИБ передает имеющиеся материалы (в объеме, достаточном для принятия решения) руководителю нарушителя ИБ для решения вопроса о целесообразности привлечения нарушителя ИБ к дисциплинарной ответственности.

6.2. На основании полученных результатов расследования руководитель структурного подразделения совместно с администратором ИБ в срок не более 3 (трех) рабочих дней организывает 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 ОО;
- обсуждение инцидента ИБ на совещании руководителей или собрании коллектива;
- 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 администратор ИБ письменно докладывает руководству ОО.

## **7. Права, обязанности и ответственность участников разбирательства**

7.1. Администратор ИБ имеет право:

- по согласованию с непосредственным руководителем нарушителя ИБ требовать у нарушителя ИБ письменные объяснения по обстоятельствам инцидента ИБ;
- запрашивать и получать от руководителей и сотрудников ОО, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для расследования инцидента ИБ;
- инициировать отключение от информационных ресурсов сотрудников ОО, нарушивших правила или требования ИБ, на период проведения 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 бизнес-процессах и информационных ресурсах ОО с целью повышения их защищенности и снижения рисков инцидентов ИБ;
- инициировать процедуры привлечения нарушителя ИБ к дисциплинарной и (или) материальной ответственности согласно требованиям внутренних нормативных документов Администрации.

#### 7.2. Администратор 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 руководству  
ОО;
- проводить анализ обстоятельств, способствовавших возникновению каждого инцидента ИБ, и на

его основе совместно с отделом информационных технологий разрабатывать рекомендации и предложения по оптимизации бизнес-процессов, снижению ущерба от подобных инцидентов ИБ и предотвращению возможности их повторения в будущем.

#### 7.3. Руководители структурных подразделений и сотрудники ОО обязаны:

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

## Карточка данных о инциденте ИБ.

Дата события  
Номер события

### Информация о сообщаемом лице

|             |       |                   |       |
|-------------|-------|-------------------|-------|
| Фамилия     | _____ | Адрес             | _____ |
| Организация | _____ |                   | _____ |
| Телефон     | _____ | Электронная почта | _____ |
| _____       |       |                   |       |

### Описание события ИБ

Описание события:

- Что произошло
- Как произошло
- Почему произошло
- Пораженные компоненты
- Негативное воздействие на бизнес
- 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  
Вредоносная программа

☐
☐

Другой ущерб

☐

Определить:

(Один из)

Случайная ☐

(указать типы угрозы)

Отказ аппаратуры

☐

Другие природные события

☐

Отказ ПО

☐

Определить:

Отказ связи

☐

Потеря существенных сервисов

☐

Пожар, наводнение

☐

Недостаточное кадровое обеспечение

☐

Отказ электропитания

☐

Другие случаи

☐

Определить:

(Один из)

Ошибка ☐

(указать типы угрозы)

Операционная ошибка

☐

Ошибка пользователя

☐

Ошибка аппаратной поддержки

☐

Ошибка конструкции

☐

Ошибка поддержки ПО

☐

Другие случаи (включая истинные заблуждения)

☐

Определить:

Неизвестно

☐

(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 на бизнес

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<br>(т. е., несанкционированное раскрытие) | <input type="checkbox"/> |           |           |
| Нарушение целостности<br>(т. е., несанкционированная модификация)      | <input type="checkbox"/> |           |           |
| Нарушение доступности<br>(т. е., недоступность)                        | <input type="checkbox"/> |           |           |
| Нарушение неотказуемости                                               | <input type="checkbox"/> |           |           |
| Уничтожение                                                            | <input type="checkbox"/> |           |           |

### 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                |  |

Причастные лица

|           |                       |                          |                                                                  |                          |
|-----------|-----------------------|--------------------------|------------------------------------------------------------------|--------------------------|
| (Один из) | Лицо                  | <input type="checkbox"/> | Легально учрежденная организация/учреждение                      | <input type="checkbox"/> |
|           | Организованная группа | <input type="checkbox"/> | Случайность                                                      | <input type="checkbox"/> |
|           |                       |                          | Нет виновного                                                    | <input type="checkbox"/> |
|           |                       |                          | Например, природные факторы, отказ оборудования, ошибка человека |                          |

Описание нарушителя

Действительная или предполагаемая мотивация

|           |                                |                          |                       |                          |
|-----------|--------------------------------|--------------------------|-----------------------|--------------------------|
| (Один из) | Криминальная/финансовая выгода | <input type="checkbox"/> | Развлечение/хакерство | <input type="checkbox"/> |
|           | Политика/Терроризм             | <input type="checkbox"/> | Реванш                | <input type="checkbox"/> |
|           |                                |                          | Другие мотивы         | <input type="checkbox"/> |
|           |                                |                          | 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 организации ☐
- Руководитель подразделения (уточнить какого) ☐
- Начальник отдела информационных технологий ☐
- Автор отчета ☐
- Начальник отдела кадров ☐
- Полиция ☐
- Другое лица ☐

Определить:

Привлеченные лица

| Инициатор           | Аналитик            | Аналитик            |
|---------------------|---------------------|---------------------|
| Подпись <div></div> | Подпись <div></div> | Подпись <div></div> |
| Фамилия <div></div> | Фамилия <div></div> | Фамилия <div></div> |
| Роль <div></div>    | Роль <div></div>    | Роль <div></div>    |
| Дата <div></div>    | Дата <div></div>    | Дата <div></div>    |

