Утверждаю
Директор МБОУ ООШ № 16
им. В.В. Сальникова
А.Л. Махновский

**Регламент**
**реагирования на инциденты информационной безопасности**

**1.Общие положения**

1.1. Настоящий Регламент устанавливает 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 МБОУ ООШ № 16 им.В.В. Сальникова (далее - Организация).

1.2. Регламент разработан в соответствии с Концепцией информационной безопасности, принятой в Организации, Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании» Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» иными нормативными правовыми актами, а также в соответствии с локальными нормативными актами Организации.

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

1.4. Разбирательство по всем инцидентам ИБ проводится ответственным за информационную безопасность с привлечением в необходимых случаях руководителей и сотрудников организации.

1.5. Разбирательство инцидентов ИБ проводится ответственным за информационную безопасность.

**2. Выявление инцидента информационной безопасности**

2.1. Основными источниками информации об Инцидентах ИБ являются:

- факты, выявленные руководителем Организации, лицом, назначенным ответственным за информационную безопасность Приказом по Организации, а также другими сотрудниками организации.

- результаты работы средств мониторинга ИБ, результаты 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 Организации являются:

- разглашение конфиденциальной или внутренней информации, либо угроза такого разглашения;

- несанкционированный доступ - доступ лиц, которые не имеют никакого легального доступа к ресурсам или помещениям организации;

- превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников Организации;

- 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. Работник Организации может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям защиты информации, утвержденными в Организации. Выявленные несоответствий дают основания предполагать факт возникновения Инцидента ИБ. Любые сведения о Происшествие или Инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником администратору информационной.

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

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

3.2. По усмотрению ответственного за информационную безопасность единичный Инцидент ИБ, не приведший к негативным последствиям и совершенный сотрудником Организации впервые, фиксируется в карточке данных «Инциденты ИБ» (приложение № 1) с присвоением статуса «Разбирательство не требуется».

3.3. В случае наличия признаков Инцидента ИБ, приведшего к негативным последствиям, ответственный за информационную безопасность классифицирует инцидент, определяет предварительную степень важности Инцидента ИБ и принимает решение о необходимости проведения

разбирательства, информирует руководителя Организации об Инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

3.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте ИБ, администратор ИБ по согласованию с руководителем Организации определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на 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 Организации, установленных законодательством Российской Федерации;
- защита репутации Организации и ее информационных ресурсов;
- обеспечение безопасности персональных данных;
- обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых Организацией;
- 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 Организации 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, затрагивающим 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 ответственным за информационную безопасность направляется руководителю Организации.

4.2.5. Осуществляющий разбирательство ответственный за информационную безопасность в процессе проведения расследования Инцидента ИБ при необходимости запрашивает информацию 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 разбирательство ответственный за информационную безопасность проводит анализ полученных данных.

4.2.7. В течение 5 (пяти) рабочих дней с момента выявления инцидента ИБ ответственный за информационную безопасность запрашивает объяснительную записку Нарушителя ИБ. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение (двух) рабочих дней и представлена ответственному за информационную безопасность в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа Нарушителя ИБ предоставить объяснительную записку, ответственный за информационную безопасность составляет акт, в соответствии с установленным в Организации порядке.

4.2.8. Ответственный за информационную безопасность проводит оценку негативных последствий от реализации 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 Организации 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 ответственным за информационную безопасность с обязательным

предварительным устным согласованием с руководителем организации.

4.2.10. В случае, если у Нарушителя ИБ были отключены права доступа к ИР на время проведения разбирательства, то по его результатам ответственный за информационную безопасность по согласованию с руководителем принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у Нарушителя ИБ прав доступа к ИР либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР в соответствии с установленным Порядком доступа к информационным, программным и аппаратным ресурсам Организации. 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, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами Организации.

4.2.11. Восстановление временно отключенных у Нарушителя ИБ прав доступа к ИР (разблокировка пользователя) может производиться только ответственным за информационную безопасность.

## 5. Оформление результатов проведенного разбирательства

5.1. Собранная в процессе разбирательства Инцидента ИБ информация фиксируется ответственным за информационную безопасность в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по Инциденту ИБ (приложение № 1).

5.2. Ответственный за информационную безопасность, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию Инцидента ИБ.

5.3. Итоговое заключение по Инциденту ИБ ответственный за информационную безопасность направляет руководителю Организации.

5.4. Ответственный за информационную безопасность фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

5.5. Ответственный за информационную безопасность, при необходимости определения правовой оценки Инцидента ИБ, может обратиться за юридической помощью.

5.6. В случае выявления в Инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, ответственный за информационную безопасность передает все материалы по Инциденту ИБ руководству Организации для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

## 6. Завершение разбирательства, превентивные мероприятия

6.1. По завершению разбирательства Инцидента ИБ, ответственный за информационную безопасность передает имеющиеся материалы (в объеме, достаточном для принятия решения) руководителю Организации для решения

вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.

6.2. На основании полученных результатов разбирательства руководитель совместно с ответственным за информационную безопасность в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у Нарушителя ИБ;
- доведение до всех сотрудников требований внутренних нормативных документов Организации;
- обсуждение Инцидента ИБ на совещании 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.

## 7. Права, обязанности и ответственность участников разбирательства

7.1. Ответственный за информационную безопасность имеет право:

- По согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам Инцидента ИБ у Нарушителя ИБ.
- Запрашивать и получать от руководителя и сотрудников Организации, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства Инцидента ИБ.
- Инициировать отключение от информационных ресурсов сотрудников Организации, нарушивших правила или требования ИБ, на период проведений расследования Инцидента ИБ в случае если имеется существенный риск того, что продолжение работы сотрудника с ИР может повлечь значительное увеличение ущерба или новые инциденты ИБ.
- По результатам расследования Инцидента ИБ инициировать изменения в бизнес-процессах и информационных ресурсах Организации с целью повышения их защищенности и снижения рисков Инцидентов ИБ.
- Инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной и (или) материальной ответственность согласно внутренним нормативным документам Организации.

7.2. Ответственный за информационную безопасность обязан:

- Объективно 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 руководству Организации.

- Проводить анализ обстоятельств, способствовавших совершению каждого Инцидента ИБ, и на его основе, совместно с отделом информационных технологий, разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных Инцидентов ИБ и минимизации возможности их повторения в будущем.

Приложение 1
к Регламенту о реагировании на инциденты информационной безопасности в МБОУ ООШ № 16 им.В.В. Сальникова

# Карточка данных о инциденте ИБ.

Дата события



Номер события[1]); (Если требуется) соответствующие идентификационные номера событий и (или) инцидентов:

**Информация о сообщающем 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

Закончилось ли событие? *(отметить квадрат)* Да □ Нет □

Если «да», то уточнить, как долго длилось событие в днях/часах/минутах

[1]) (Номера событий назначаются руководителем)

Дата инцидента

Номер инцидента[2]-[1]: (Если требуется) соответствующие идентификационные номера событий и (или) инцидентов:

Фамилия
Телефон

**Информация о сотруднике группы обеспечения эксплуатации**

Адрес _____

Электронная почта _____

**Информация о сотруднике ISIRT**

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____

**Описание инцидента ИБ**

Дальнейшее описание инцидента:

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

**Детали инцидента ИБ**

Дата и время возникновения инцидента

Дата и время обнаружения инцидента

Дата и время сообщения об инциденте

Закончился ли инцидент? *(отметить квадрат)* Да □ Нет □

[2] Если «да», то уточнить, как долго длился инцидент в днях/часах/минутах. Если «нет», то уточнить, как долго он уже длится (Номера инцидентов назначаются руководителем)

# Тип инцидента ИБ

*(Отметить один квадрат, затем заполнить соответствующие поля ниже)*

Действительный □ Попытка □ Подозрение □

*(Один из)* Намеренная □

*(указать типы угрозы)*

□ Хакерство/Логическое проникновение (HA) □
□ Неправильное использование ресурсов (MI) □
□ Другой ущерб (OD) □

Хищение (TH) □
Мошенничество (FR) □
Саботаж/физический ущерб (SA) □
Вредоносная программа (MC)

*Определить:*

*(Один из)* Случайная □

*(указать типы угрозы)*

□ Другие природные события (NE) □
□ *Определить:*
□ Потеря существенных сервисов (LE) □
□ Недостаточное кадровое обеспечение (SS) □
□ Другие случаи (OA) □

Отказ аппаратуры (HF)
Отказ ПО (SF)
Отказ связи (CF) Пожар (HE)
Наводнение (FL)

*Определить:*

*(Один из)* Ошибка □

*(указать типы угрозы)*

□ Ошибка пользователя (UE) □
□ Ошибка конструкции (DE) □
□ Другие случаи (включая истинные заблуждения) (OA) □

Операционная ошибка (OE)
Ошибка аппаратной поддержки (HE) Ошибка поддержки ПО (SE)

*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): (FD) - финансовые потери/разрушение бизнес-операций, (CE) - коммерческие и экономические интересы, (PI) - информация, содержащая персональные данные, (LR) - правовые и нормативные обязательства(это необходимо сличить с английским оригиналом),(MO) - менеджмент и бизнес-операции, (LG) - 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 _____

**Причастные лица**

*(Один из)*

Лицо (PE) □

Организованная группа (GR) □

Легально учрежденная организация/учреждение (OI) □

Случайность (AC) □

Нет виновного (NP) □

*Например, природные факторы, отказ оборудования, ошибка человека*

**Описание нарушителя**

**Действительная или предполагаемая мотивация**

*(Один из)*

Криминальная/финансовая выгода(CG) □

Политика/Терроризм (PT) □

Развлечение/хакерство (PH) □

Реванш (RE) □

Другие мотивы (OM) □

*Определить:*

**Действия, <u>предпринятые</u> 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. Обычно этим лицом является руководитель ИБ организации).*

| | | | |
|---|---|---|---|
| Руководитель ИБ | □ | Руководитель ГРИИБ | □ |
| Местный руководитель (уточнить, какого подразделения) | □ | Руководитель информационных систем | □ |
| Автор отчета | □ | Руководитель автора отчета | □ |
| Полиция | □ | Другое лица | □ |

*(например, справочная служба, отдела кадров, менеджмента, внутреннего аудита, регулятивного органа, сторонняя КСБР) Определить:*

**Привлеченные лица**

| Инициатор | Аналитик | Аналитик |
|---|---|---|
| Подпись _____ | Подпись _____ | Подпись _____ |
| Фамилия _____ | Фамилия _____ | Фамилия _____ |
| Роль _____ | Роль _____ | Роль _____ |
| Дата _____ | Дата _____ | Дата _____ |

| Аналитик | Аналитик | Аналитик |
|---|---|---|
| Подпись _____ | Подпись _____ | Подпись _____ |
| Фамилия _____ | Фамилия _____ | Фамилия _____ |
| Роль _____ | Роль _____ | Роль _____ |
| Дата | Дата | Дата |