****

**Муниципальное дошкольное образовательное учреждение № 30 «Буратино»**

**поселка Чульман Нерюнгринского района**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

678981, Республика Саха (Якутия), Нерюнгринский район, поселок Чульман, ул. Гагарина 27а,

тел: (8-41147) 7-61-20 [buratino@nerungri.edu.ru](mailto:buratino@nerungri.edu.ru)

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Заведующая МДОУ № 30 «Буратино»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Головченко  Приказ 71 ОД от 26.05.2022 года |

# РЕГЛАМЕНТ

**реагирования на инциденты информационной безопасности в**

**МДОУ № 30 «Буратино» поселка Чульман Нерюнгринского района**

# Общие положения

* 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 МДОУ № 30 «Буратино» (далее – Организация).
  2. Регламент разработан в соответствии с Концепцией информационной безопасности, принятой в Организации, Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании" Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 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.
  3. Настоящий Регламент обязателен к соблюдению всеми работниками Организации, участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности (далее – ИБ).
  4. Разбирательство по всем инцидентам ИБ проводится администратором информационной безопасности.

# Выявление инцидента информационной безопасности

* 1. Основными источниками информации об Инцидентах ИБ являются:
* факты, выявленные руководителем Организации, администратором информационной безопасности – лицом, назначенным ответственным за информационную безопасность, 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.
  1. 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.
  1. Работник Организации может выявить признаки наличия инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям защиты информации, утвержденными в Организации. Выявление несоответствий дают основания предполагать факт возникновения инцидента ИБ. Любые сведения о происшествии или инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником администратору информационной безопасности.

# Анализ исходной информации и принятие решения о проведения разбирательства

* 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.
  2. По усмотрению администратора ИБ единичный инцидент ИБ, не приведший к негативным последствиям и совершенный сотрудником Организации впервые, фиксируется администратором ИБ в карточке данных «Инциденты ИБ» *(приложение №1)* с присвоением статуса «Разбирательство не требуется».
  3. В случае наличия признаков инцидента ИБ, приведшего к негативным последствиям, администратор ИБ 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».
  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.

# Разбирательство инцидента информационной безопасности

* 1. **Цели и этапы разбирательства Инцидента ИБ**:
     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.
  + 1. 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;
* 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.
  1. **Порядок проведения разбирательства инцидента ИБ**:
     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.
  + 1. При Инциденте ИБ, затрагивающем не более одного структурного подразделения, администратор ИБ информирует о факте инцидента руководителя соответствующего структурного подразделения.
    2. При Инциденте ИБ, затрагивающим более одного структурного подразделения, администратор ИБ информирует руководителей соответствующих подразделений и инициирует проведение разбирательства.
    3. В случае проведения временного отключения прав доступа у предполагаемого Нарушителя ИБ информация об отключении прав доступа администратором ИБ направляется руководителю предполагаемого Нарушителя ИБ.
    4. Осуществляющий разбирательство администратор ИБ в процессе проведения расследования Инцидента ИБ при необходимости запрашивает информацию в структурных подразделениях, запрос направляется на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).
    5. После получения необходимой информации по Инциденту ИБ осуществляющий разбирательство администратор ИБ проводит анализ полученных данных,
    6. В течение 5 (пяти) рабочих дней с момента выявления инцидента ИБ администратор ИБ запрашивает у руководителя структурного подразделения объяснительную записку Нарушителя ИБ. 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 Организации порядке.
    7. Администратор ИБ 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.
  + 1. 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 с обязательным предварительным устным согласованием с руководителем.
    2. В случае, если у нарушителя ИБ были отключены права доступа к ИР на время проведения разбирательства, то, по его результатам, администратор ИБ 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.
    3. Восстановление временно отключенных у нарушителя ИБ прав доступа к ИР (разблокировка пользователя) может производиться только по заявке руководителя или осуществляющего разбирательство сотрудника.

# Оформление результатов проведенного разбирательства

* 1. Собранная в процессе разбирательства инцидента ИБ информация фиксируется администратором ИБ в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по инциденту ИБ *(Приложение №1)*.
  2. Администратор ИБ формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента ИБ.
  3. Итоговое заключение по инциденту ИБ администратор ИБ направляет руководителю организации.
  4. Администратор ИБ фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».
  5. Администратор ИБ, при необходимости определения правовой оценки инцидента ИБ, может обратиться за консультациями в юридическое подразделение Организации.
  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 Организации для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

# Завершение разбирательства, превентивные мероприятия

* 1. По завершению разбирательства Инцидента ИБ, администратор ИБ передает имеющиеся материалы (в объеме, достаточном для принятия решения) вышестоящему руководителю Нарушителя ИБ для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.
  2. На основании полученных результатов разбирательства руководитель структурного подразделения совместно с администратором ИБ 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 структурного подразделения требований внутренних нормативных документов Организации;
* 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;
  1. О результатах проведенного разбирательства инцидента ИБ администратор ИБ по необходимости инициирует подготовку сообщения об инциденте ИБ в адрес руководства Организации.

# Права, обязанности и ответственность участников разбирательства

* 1. Администратор ИБ имеет право:

По согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставления письменных объяснений по обстоятельствам инцидента ИБ у Нарушителя ИБ.

Запрашивать и получать от руководителей 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.

* 1. Администратор ИБ 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 разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных инцидентов ИБ и минимизации возможности их повторения в будущем.

* 1. Сотрудники Организации обязаны:

предоставлять по запросам администратора ИБ устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента ИБ;

информировать администратора ИБ о выявленных инцидентах ИБ.

Приложение 1 **к Регламенту**

**Карточка данных об инциденте ИБ.**

|  |  |  |  |
| --- | --- | --- | --- |
| Дата события |  |  | Стр. 1 |
| Номер события |  |  |  |
| **Информация о сообщающем лице** | | | |
| Фамилия |  | Адрес |  |
| Организация |  | Телефон |  |
| 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 | |  | |

Стр. 2

# 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)*

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:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Стр. 3 | | | | | |
| **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  *(т. е., несанкционированное раскрытие)* | |  |  |  |  |
| Нарушение целостности  *(т. е., несанкционированная*  *модификация)* | |  |  |  |  |
| Нарушение доступности  *(т. е., недоступность)* | |  |  |  |  |
| Нарушение неотказуемости | |  |  |  |  |
|  |  |  |  |  |  |
| **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** |

Стр. 4

# 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  Легально учрежденная организация/учреждение 

Организованная группа  Случайность 

Нет виновного 

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

**Описание нарушителя**

**Действительная или предполагаемая мотивация**

*(Один из)* Криминальная/финансовая

выгода 

Развлечение/хакерство 

Политика/Терроризм  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)*

Стр. 5

# 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*

Администратор ИБ  Руководитель организации 

*заполняется*

*соответствующим лицом, на которое возложены*

Руководитель подразделения (уточнить

какого)

□ Начальник отдела 

информационных технологий

*обязанности в области ИБ и которое формулирует*

*требуемые действия*

Автор отчета  Начальник отдела кадров 

Полиция  Другое лица 

*(например, служба охраны,*

*регулятивного органа, сторонняя организация)*

*Определить:*

**Привлеченные лица**

Инициатор Аналитик Аналитик

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Подпись |  |  | Подпись |  |  | Подпись |  |  |
|  | \_ |  |  | \_ |  |  | **\_** |  |
| Фамилия |  |  | Фамилия |  |  | Фамилия |  |  |
|  | \_ |  |  | \_ |  |  | **\_** |  |
| Роль |  |  | Роль |  |  | Роль |  |  |
|  | \_ |  |  | \_ |  |  | \_ |  |
| Дата |  |  | Дата |  |  | Дата |  |  |
|  | \_ |  |  | \_ |  |  | \_ |  |