**ПОРЯДОК**

выявления инцидентов информационной безопасности информационных систем персональных данных в комитете по культуре города Барнаула

**1.ОБЩИЕ ПОЛОЖЕНИЯ**

* Настоящий Порядок устанавливает 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 комитета по культуре города Барнаула.
1. Порядок разработан в соответствии с:

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" и иными нормативными правовыми актами,

а также в соответствии с локальными нормативными актами организации.

* Настоящий Порядок обязателен к соблюдению правил всеми работниками комитета по культуре города Барнаула
1. Участвующими в выявлении, разбирательстве и предотвращении инцидентов ИБ
2. Разбирательство по всем инцидентам ИБ проводится администратором информационной безопасности с привлечением, в необходимых случаях руководителей и сотрудников других подразделений.
* Разбирательство инцидентов ИБ, затрагивающих два или более подразделения комитета по культуре города Барнаула проводится администратором информационной безопасности с привлечением руководителей соответствующих подразделений.
* Разбирательство по вопросам инцидентов ИБ, которые затрагивают ресурсы комитета по культуре города Барнаула в обязательном порядке проводится администратором информационной безопасности, с привлечением сотрудников других структурных подразделений комитета по культуре города Барнаула.

**2. ВЫЯВЛЕНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

2.1. Основными источниками информации об Инцидентах ИБ являются:

* факты, выявленные руководителем структурного подразделения комитета по культуре города Барнаула, администратором информационной безопасности – лицо, назначенное ответственным за информационную безопасность (ИБ) Приказом комитета по культуре города Барнаула, а также другими сотрудниками организации.
* результаты работы средств мониторинга ИБ результаты проверок и аудита (внутреннего или внешнего);
* обращения субъектов персональных данных с указанием Инцидента ИБ;
* запросы и предписания органов надзора за соблюдением прав субъектов ПДн;
* другие источники информации.

2.2. Работник комитета по культуре города Барнаула может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям утвержденных в комитете по культуре города Барнаула. Выявленные несоответствий дают основания предполагать факт возникновения Инцидента ИБ. Любые сведения о Происшествие или Инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником ответственному лицу в подразделение информационной безопасности любым доступным способом:

* по контактам, указанным в внутрикорпоративном справочнике;
* через непосредственного Руководителя.

2.3. Работники комитета по культуре города Барнаула при подозрении на Инцидент ИБ обязаны также дополнительно уведомить Администратора информационной безопасности.

**3.АНАЛИЗ ИСХОДНОЙ ИНФОРМАЦИИ И**

**ПРИНЯТИЕ РЕШЕНИЯ О ПРОВЕДЕНИИ РАЗБИРАТЕЛЬСТВА**

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

3.2. По усмотрению руководителя администратора информационной безопасности единичный Инцидент ИБ, не приведший к негативным последствиям и совершенный сотрудником комитета по культуре города Барнаула впервые, фиксируется администратором информационной безопасности в карточке данных «Инциденты ИБ» *(приложение №1)* с присвоением статуса «Разбирательство не требуется».

3.3. В случае нарушения прав субъекта персональных данных разбирательство и реагирование происходит в порядке и сроки, предусмотренные Регламентом «О порядке действий комитета по культуре города Барнаула при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных»**.**

3.4. В случае наличия признаков Инцидента ИБ в полученной информации, администратор информационной безопасности определяет предварительную степень важности Инцидента ИБ и принимает решение о необходимости проведения разбирательства, информирует руководителя подразделения информационной безопасности об Инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

3.5. В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте ИБ, сотрудник подразделения информационной безопасности по согласованию с руководителем подразделения информационной безопасности определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

3.6. Администратор информационной безопасности определяет сотрудника, осуществляющего разбирательство, и передает ему всю имеющуюся исходную информацию для проведения разбирательства, а также информацию о проведенных мероприятиях по локализации Инцидента ИБ.

**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 комитета по культуре города Барнаула установленных законодательством Российской Федерации;
* защита репутации комитета по культуре города Барнаула и его ресурсов;
* обеспечение безопасности персональных данных;
* обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых комитета по культуре города Барнаула;
* предотвращение несанкционированного доступа к 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;
* 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 комитета по культуре города Барнаула по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
* разработка мероприятий по обнаружению и/или предупреждению инцидентов ИБ.

4.2. Создание Рабочей группы для проведения расследования Инцидента ИБ:

При необходимости администратор информационной безопасности незамедлительно уведомляет руководителя комитета по культуре города Барнаула о факте Инцидента ИБ и инициирует подготовку Приказа о создании Рабочей группы для разбирательства указанного Инцидента ИБ, Подготовка, согласование и организация издания приказа о создании Рабочей группы по разбирательству Инцидента ИБ осуществляется в установленном порядке распоряжением за подписью руководителя комитета по культуре города Барнаула. В приказе по представлению администратора информационной безопасности определяются: Сроки разбирательства Инцидента ИБ, при необходимости определяются дополнительные полномочия.

4.3. Порядок проведения разбирательства Инцидента ИБ:

4.3.1. В процессе проведения разбирательства Инцидента ИБ обязательными для установления являются:

* дата и время совершения Инцидента ИБ;
* ФИО, должность и подразделение Нарушителя ИБ;
* 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.

4.3.2. При Инциденте ИБ, затрагивающем не более одного структурного подразделения, администратор информационной безопасности информирует о факте инцидента руководителя подразделения.

4.3.3. При Инциденте ИБ, затрагивающим более одного структурного подразделения, осуществляющий разбирательство сотрудник информирует руководителей соответствующих подразделений и инициирует проведение разбирательства с привлечением ресурсов сотрудников подразделения информационной безопасности.

4.3.4. В случае проведения временного отключения прав доступа у предполагаемого Нарушителя ИБ информация об отключении прав доступа ответственным за проведение разбирательства направляется руководителю предполагаемого Нарушителя ИБ.

4.3.5. 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).

4.3.6. После получения необходимой информации по Инциденту ИБ осуществляющий разбирательство администратор ИБ проводит анализ полученных данных,

4.3.7. В течение 5 (пяти) рабочих дней с момента назначения осуществляющего разбирательство администратора ИБ (формирования Рабочей группы), осуществляющий разбирательство 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 осуществляющему разбирательство администратору ИБ в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа Нарушителя ИБ предоставить объяснительную записку, осуществляющему разбирательство администратор ИБ предоставляется акт, составленный в соответствии с установленным в комитете по культуре города Барнаула порядке.

4.3.8. Осуществляющий разбирательство 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 комитета по культуре города Барнаула или субъектов персональных данных.

4.3.9. С целью минимизации последствий Инцидента ИБ возможно временное отключение прав доступа сотрудника к Информационным ресурсам (ИР) на время проведения расследования предварительно сделав заявку. Подобное отключение инициируется осуществляющим разбирательство администратором ИБ с обязательным предварительным устным согласованием с руководителем сотрудника.

4.3.10. В случае, если у Нарушителя ИБ были отключены права доступа к ИР на время проведения разбирательства, то по его результатам осуществляющий разбирательство администратор ИБ по согласованию с руководителем Нарушителя ИБ 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 в комитете по культуре города Барнаула. Если Нарушение ИБ было вызвано незнанием Нарушителем ИБ правил (технологии) работы с информационными ресурсами высокого уровня безопасности, то основанием для возврата прав доступа является успешное прохождение повторного инструктажа администратором ИБ, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами Гострудинспекции в комитете по культуре города Барнаула.

4.3.11.Восстановление временно отключенных у Нарушителя ИБ прав доступа к ИР (разблокировка пользователя) может производиться только по заявке руководителя Нарушителя ИБ или осуществляющего разбирательство сотрудника.

**5. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ПРОВЕДЕННОГО РАЗБИРАТЕЛЬСТВА**

5.1. Собранная в процессе разбирательства Инцидента ИБ информация фиксируется осуществляющим разбирательство администратором ИБ в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по Инциденту ИБ *(Приложение №1)*.

5.2. Осуществляющий разбирательство сотрудник формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию Инцидента ИБ.

5.3. Итоговое заключение по Инциденту ИБ осуществляющий разбирательство администратор ИБ направляет руководителям.

5.4. Осуществляющий разбирательство администратор ИБ фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

5.5. Осуществляющий разбирательство администратор ИБ, при необходимости определения правовой оценки Инцидента ИБ, может обратиться за консультациями в юридическое подразделение комитета по культуре города Барнаула. В этом случае информацию по Инциденту ИБ осуществляющий разбирательство администратор ИБ передает с грифом «Конфиденциально» от руководства подразделения информационной безопасности.

О результатах проведенного анализа и других мероприятий, руководство в течение не более 5 (пяти) рабочих дней после получения запроса информирует руководство подразделения информационной безопасности.

* 5.6. В случае выявления в Инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, осуществляющий разбирательство администратор ИБ передает все материалы по Инциденту ИБ руководству комитета по культуре города Барнаула:
* для принятия решения, в соответствии с установленным в комитете по культуре города Барнаула о подаче заявления в правоохранительные органы Российской Федерации.

5.7. Осуществляющий разбирательство администратор ИБ фиксирует полученную дополнительную информацию в карточке данных «Инциденты ИБ» и информирует Руководителя дирекции по безопасности и режиму.

**6. ЗАВЕРШЕНИЕ РАЗБИРАТЕЛЬСТВА, ПРЕВЕНТИВНЫЕ МЕРОПРИЯТИЯ**

6.1. По завершению разбирательства Инцидента ИБ, осуществляющий разбирательство 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.

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

* повторное ознакомление Нарушителя ИБ с Правилами;
* анализ и пересмотр имеющихся прав доступа к информационным ресурсам у Нарушителя ИБ;
* доведение до всех сотрудников структурного подразделения требований внутренних нормативных документов комитета по культуре города Барнаула:
* обсуждение Инцидента ИБ на совещании руководителей или собрании коллектива;
* отмена неактуальных прав доступа к информационным ресурсам;
* проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

и другие обоснованные мероприятия.

* 6.3. О результатах проведенного разбирательства Инцидента ИБ администратор ИБ по необходимости инициирует подготовку сообщения об Инциденте ИБ в адрес руководства комитета по культуре города Барнаула.

**7. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ РАЗБИРАТЕЛЬСТВА**

7.1. Осуществляющий разбирательство администратор ИБ имеет право:

7.1.1. По согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам Инцидента ИБ у Нарушителя ИБ.

* Запрашивать и получать от руководителей и сотрудников комитета по культуре города Барнаула, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства Инцидента ИБ.
* Инициировать на основании заявок отключение от информационных ресурсов сотрудников комитета по культуре города Барнаула
* 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 комитета по культуре города Барнаула
* с целью повышения их защищенности и снижения рисков Инцидентов ИБ.
* Инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной/ материальной ответственность согласно внутренним нормативным документам комитета по культуре города Барнаула

7.2. Осуществляющий разбирательство администратор ИБ обязан:

* Объективно и основательно 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 подразделения информационной безопасности.
* Проводить анализ обстоятельств, способствовавших совершению каждого Инцидента ИБ, и на его основе, совместно с сотрудниками смежных подразделений, разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных Инцидентов ИБ и минимизации возможности их повторения в будущем.
* Составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
* 7.3. Руководители и сотрудники комитета по культуре города Барнаула обязаны:
* предоставлять по запросам Проводящего разбирательство администратора ИБ устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства Инцидента ИБ;
* информировать администратора информационной безопасности о выявленных Инцидентах ИБ;
* информировать администратора информационной безопасности об имеющихся запросах и обращениях субъектов персональных данных.

*Приложение №1 к регламенту разбирательств инцидентов ИБ.*

Карточка данных о инциденте ИБ.

|  |  |  |  |
| --- | --- | --- | --- |
| Дата события |  |  | Стр. 1 |
| Номер события[[1]](#footnote-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 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Дата инцидента |  |  | Стр. 2 |
| Номер инцидента[[2]](#footnote-2)): |  | (Если требуется) соответствующие идентификационные номера событий и (или) инцидентов: |  |
| Информация о сотруднике группы обеспечения эксплуатации |
| Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Адрес | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Телефон | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | 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  |
| Если «да», то уточнить, как долго длился инцидент в днях/часах/минутах. Если «нет», то уточнить, как долго он уже длится |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Стр. 3 |
|  |  |  |  |
| Тип инцидента ИБ |
| (Отметить один квадрат, затем заполнить соответствующие поля ниже) | Действительный  | Попытка  | Подозрение  |
|  |
| (Один из) | Намеренная  | (указать типы угрозы) |  |
|  |
| Хищение (TH) |  | Хакерство/Логическое проникновение (HA) |  |
| Мошенничество (FR) |  | Неправильное использование ресурсов (MI) |  |
| Саботаж/физический ущерб (SA) |  | Другой ущерб (OD) |  |
| Вредоносная программа (MC) |  |  |  |
|  |  | Определить: |  |
|  |
| (Один из) | Случайная  | (указать типы угрозы) |
|  |
| Отказ аппаратуры (HF) |  | Другие природные события (NE) |  |
| Отказ ПО (SF) |  | Определить: |  |
| Отказ связи (CF) |  | Потеря существенных сервисов (LE) |  |
| Пожар (HE) |  | Недостаточное кадровое обеспечение (SS) |  |
| Наводнение (FL) |  | Другие случаи (OA) |  |
|  | Определить: |
|  |
| (Один из) | Ошибка  | (указать типы угрозы) |
|  |
| Операционная ошибка (OE) |  | Ошибка пользователя (UE) |  |
| Ошибка аппаратной поддержки (HE) |  | Ошибка конструкции (DE) |  |
| Ошибка поддержки ПО (SE) |  | Другие случаи (включая истинные заблуждения) (OA) |  |
|  | 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. 4 |
|  |  |  |  |
| 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),(МО) – 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 |
|  |  |  | Стр. 5 |
|  |  |  |  |
| 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) |  | Легально учрежденная организация/учреждение (OI) |  |
| Организованная группа (GR) |  | Случайность (AC) |  |
|  |  | Нет виновного (NP)Например, природные факторы, отказ оборудования, ошибка человека |  |
|  |
| Описание нарушителя |
|  |
| Действительная или предполагаемая мотивация |
|  |
| (Один из) | Криминальная/финансовая выгода(CG) |  | Развлечение/хакерство (PH) |  |
| Политика/Терроризм (PT) |  | Реванш (RE) |  |
|  |  | Другие мотивы (OM) |  |
|  |  | 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. 6 |
|  |  |  |  |
| 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 |  | Председатель комитета по Культуре |  |
| Местный руководитель (уточнить, какого подразделения) |  | Руководитель информационных систем |  |
| Автор отчета |  | Руководитель автора отчета |  |
|  |  | 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 | \_\_\_\_\_\_\_\_\_\_\_\_ |

1. ) (Номера событий назначаются руководителем) [↑](#footnote-ref-1)
2. ) (Номера инцидентов назначаются руководителем) [↑](#footnote-ref-2)