Утверждено

Приказом ООО «My Company»

от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024г.

Положение

о порядке расследования инцидентов информационной безопасности   
в ООО «My Company»

г. Москва  
2024г.

**Содержание**

[1. Сокращения, термины и определения 3](#_Toc170144458)

[2. Общие положения 3](#_Toc170144459)

[3. Участники Расследования 4](#_Toc170144460)

[4. Основания для проведения Расследования 4](#_Toc170144461)

[5. Цели и задачи Расследования 5](#_Toc170144462)

[6. Этапы Расследования 6](#_Toc170144463)

[7. Порядок проведения Расследования 6](#_Toc170144464)

[8. Мероприятия по результатам Расследования 8](#_Toc170144465)

[9. Права и обязанности работников и должностных лиц Общества при проведении Расследования 9](#_Toc170144466)

# Сокращения, термины и определения

|  |  |
| --- | --- |
| АРМ | - Автоматизированное рабочее место |
| АС | - Автоматизированная система |
| ИБ | - Информационная безопасность |
| ИУС | - Информационно-управляющая система |
| ПАК | - Программно-аппаратный комплекс |
| ПО | - Программное обеспечение |
| ПОИБ | - Подсистема обеспечения информационной безопасности |
| СТИ | - Системно-техническая инфраструктура |
| DLP | - Система предотвращения утечек информации (Data Loss/Leak Prevention) |

**Событие информационной безопасности** - идентифицированное появление определенного состояния бизнес-процесса, информационной системы, сервиса или сети, указывающего на возможное нарушение установленных норм и правил обеспечения информационной безопасности (далее ИБ), включая отказ защитных мер или возникновение неизвестной ранее ситуации, которая может иметь отношение к нарушению безопасности информации.

**Инцидент информационной безопасности (Инцидент)** - появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана фактическая или потенциальная реализация угрозы ИБ в отношении активов и бизнес-процессов ООО «My Company».

**Объект доступа** - физический (материальный) носитель информации, аппаратное или программное средство в составе информационной инфраструктуры, единица электронного хранения информации (файл, массив, таблица или запись базы данных и т.п.).

**Субъект доступа** - физическое лицо или виртуальный объект (учетная запись, программа, системный сервис), действия которого регламентируются правилами разграничения доступа.

**Предполагаемый нарушитель ИБ** - физическое лицо (либо лицо, непосредственно связанное с ним), являющееся субъектом доступа, действия которого стали причиной возникновения инцидента ИБ.

**Нарушитель ИБ** - лицо, вина которого в возникновении инцидента информационной безопасности доказана установленным порядком в ходе проведения расследования.

**Расследование инцидента ИБ (Расследование)** - совокупность мероприятий по установлению обстоятельств, причин и условий возникновения инцидента ИБ, лиц, чьи действия (бездействие) стали причиной возникновения инцидента ИБ, либо создали предпосылки его возникновения, а также последствий инцидента ИБ.

**Вирусное заражение** - наличие на средствах вычислительной техники активного вредоносного ПО или следов его деструктивного воздействия.

# Общие положения

2.1. Настоящее Положение устанавливает основания, цели, задачи и порядок проведения Расследований Инцидентов в ООО «My Company» (далее - Общество).

2.2. Общество является законным обладателем информации, средств связи и вычислительной техники, создаваемых и используемых в процессе деятельности Общества. На этом основании Общество вправе устанавливать в рамках законодательства Российской Федерации порядок использования информации и указанных технических средств, внутренние нормы и правила обеспечения информационной безопасности, а также меры ответственности за их нарушение.

2.3. Расследование Инцидентов является частью мероприятий по реагированию на возникновение Инцидентов, носит внутренний характер и проводится силами участников Расследования из числа работников Общества.

2.4. Результаты Расследования Инцидентов являются основанием для принятия в установленном порядке решения о применении мер ответственности к нарушителям ИБ, а также для предъявления гражданско-правовых исков и обращения в правоохранительные органы с просьбой о преследовании виновных лиц в соответствии с законодательством Российской Федерации.

2.5. Перечень типов Инцидентов, в отношении которых может быть проведено Расследование, определен в разделе 4 настоящего Положения.

# Участники Расследования

Расследование в Обществе осуществляется:

* службой информационной защиты;
* отделом ИТ.

Также к проведению Расследования могут привлекаться должностные лица из числа работников других подразделений Общества, а также иных организаций, состоящих с Обществом в договорных отношениях.

# Основания для проведения Расследования

Основанием для проведения Расследования являются выявленные факты, прямо или косвенно указывающие на нарушение работниками Общества, сотрудниками сторонних организаций, состоящих с Обществом в договорных отношениях, а также иных физических или юридических лиц, не состоящих с Обществом в договорных отношениях:

4.1. Установленного в Обществе режима коммерческой тайны, в том числе:

* утечку конфиденциальной информации;
* утрату конфиденциальных документов, либо электронных носителей конфиденциальной информации;
* обнаружение неучтенных (оставленных без присмотра) документов, или электронных носителей конфиденциальной информации;
* передачу конфиденциальной информации по открытым каналам связи, в том числе по электронной почте и сети Интернет, без выполнения установленных в Обществе требований по технической защите конфиденциальной информации;
* нарушение установленного порядка при передаче (предоставлении доступа) конфиденциальной информации органам государственной власти, иным государственным органам, органам местного самоуправления и контрагентам.

4.2. Принятых в Обществе мер защиты обрабатываемых персональных данных:

* обращение субъектов обрабатываемых Обществом персональных данных с заявлениями о нарушении Обществом своих обязательств как оператора персональных данных;
* выявление фактов утечки или иных грубых нарушений порядка обработки персональных данных и мер по их защите.

4.3. Норм и правил обеспечения ИБ Общества при работе со средствами вычислительной техники, информационными системами и сервисами, в том числе:

* несанкционированный доступ к аппаратным и программным средствам;
* несанкционированное подключение средств связи (телефонов, модемов, адаптеров беспроводного соединения), средств вычислительной техники (персональных компьютеров, ноутбуков, планшетов, смартфонов), и прочего оборудования к информационной инфраструктуре Общества;
* несанкционированное сканирование сети, обход (отключение) или изменение настроек установленных механизмов и средств защиты информации, включая попытки таких действий;
* несанкционированное распространение и использование программного обеспечения (далее - ПО), в том числе вредоносного и шпионского (предназначенного для обнаружения, сканирования, взлома, управления, шпионажа, перехвата и подмены пакетов, заражения и т.п.);
* распространение и использование информации и ПО, нарушающих требования законодательства Российской Федерации, авторского права, либо условий лицензионных соглашений.

4.4. Штатного режима функционирования элементов информационной инфраструктуры Общества, программных или технических средств обработки и передачи информации, эксплуатируемых подразделениями Общества в рамках договорных обязательств, в том числе допущение без своевременного реагирования:

* отказа в обслуживании и (или) выхода из строя серверного или сетевого оборудования;
* проявления недокументированных функциональных особенностей программных и аппаратно-программных средств;
* обнаружения вирусной эпидемии, повлекшей заражение более 5 рабочих станций одним типом вредоносного кода;
* обнаружения вирусного заражения серверов;
* непрогнозируемого (без видимых причин) падения производительности аппаратно-программных средств обработки и передачи информации;

4.5. Штатного режима обработки информации, в том числе допущение:

* несанкционированного удаления и изменения файлов, таблиц или записей баз данных;
* отсутствия работоспособных резервных копий информационных систем, подлежащих обязательному резервированию;
* компрометации ключа электронной подписи, используемого в Обществе.

# Цели и задачи Расследования

5.1. Целями Расследования является:

* установление обстоятельств, условий и причин, повлекших возникновение Инцидента;
* выявление и привлечение к ответственности нарушителей ИБ;
* создание условий для минимизации последствий Инцидента;
* снижение вероятности повторной реализации связанной с Инцидентом угрозы ИБ;
* сбор материалов для планирования последующих работ по совершенствованию системы обеспечения информационной безопасности Общества.

5.2. Задачами Расследования является:

* выявление объектов и субъектов доступа, связанных с Инцидентом;
* выявление фактов действия либо бездействия лиц, причастных к Инциденту;
* выявление нарушений норм и правил ИБ лицами, чьи действия либо бездействие стали причиной возникновения Инцидента или создали условия и/или предпосылки его возникновения;
* сбор доказательств вины нарушителя(ей) норм и правил ИБ;
* формирование рекомендаций по организации и проведению мероприятий, направленных на устранение причин и условий, способствовавших возникновению Инцидента;
* подготовка материалов для совершенствования организационных и технических мер обеспечения ИБ Общества.

# Этапы Расследования

Расследование осуществляется в два этапа.

Первый этап Расследования включает в себя:

* первичное выяснение обстоятельств и причин возникновения Инцидента;
* сбор документальных материалов по Инциденту;
* анализ и обобщение документальных материалов;
* выявление лиц, причастных к возникновению Инцидента, и предполагаемых нарушителей ИБ.

По результатам первого этапа участниками Расследования принимается решение о необходимости проведения мероприятий второго этапа Расследования.

Второй этап Расследования включает в себя:

* получение объяснений от предполагаемых нарушителей ИБ и иных причастных лиц;
* анализ объяснений предполагаемых нарушителей ИБ и выявление в их действиях (бездействии) нарушений установленных в Обществе норм и правил обеспечения ИБ, установление фактических нарушителей ИБ;
* детальный анализ обстоятельств Инцидента, определение степени вины нарушителей ИБ;
* формирование служебной записки на имя генерального директора Общества с приложением необходимых материалов по результатам проведенного Расследования.

# Порядок проведения Расследования

7.1. Расследованию инцидента предшествует его фиксация, включающая установление факта произошедшего инцидента, его первичная обработка.

В случае, когда событие ИБ привело к деструктивному информационному воздействию на элементы инфраструктуры, мероприятия по нейтрализации деструктивных воздействий начинаются незамедлительно.

К лицам, уполномоченным на фиксацию событий ИБ, относятся работники:

* Службы информационной защиты Общества в части объектов информатизации Общества;
* Отдел ИТ в части объектов информатизации Общества;

Информация о фиксируемом событии ИБ должна содержать:

* дата, время и место возникновения события ИБ;
* контактные данные источника информирования о событии ИБ (Фамилия, Имя, Отчество, должность, телефон);
* контактные данные лица (Фамилия, Имя, Отчество, должность, телефон), зафиксировавшего событие ИБ;
* категорию события ИБ в соответствии с Приложением к Положению;
* объекты доступа, в отношении которых обнаружено событие И Б (документ, объект данных, экземпляр ПО, АРМ, активное сетевое оборудование и т.п.);
* субъекты доступа, фактически или предположительно связанные с событием ИБ (работники, ответственные за объекты доступа, пользователи АРМ, исполнители документов или работ, администраторы и т.п.).

После фиксации события ИБ осуществляется его первичная обработка подразделениями в соответствии с распределением, указанным в Приложении. Первичная обработка события ИБ проводится с целью подтверждения факта нарушения ИБ (возникновения инцидента ИБ), и включает:

* проверку и уточнение исходных данных об инциденте ИБ;
* определение требований ИБ, нарушение которых привело к инциденту ИБ.

Информация об подтвержденных инцидентах ИБ (нарушениях ИБ) незамедлительно докладывается генеральному директору, в службу информационной безопасности Общества.

7.2. По результатам рассмотрения информации об инциденте ИБ генеральным директором принимается решение о проведении Расследования инцидента ИБ.

Проведение Расследования в зависимости от объектов доступа поручается Службе информационной защиты Общества и/или отделу ИТ и других подразделений (при необходимости).

7.3. В рамках Расследования проводится детальное выяснение обстоятельств и причин инцидента, включающее:

* - сбор документальных материалов, подтверждающих факт нарушения ИБ и поясняющих обстоятельства инцидента ИБ (выписки из системных журналов, журналов средств защиты информации, журналов учета документов и проведения работ, снимки экрана и т.п.);
* - детальный анализ обстоятельств инцидента ИБ, в том числе косвенно способствовавших возникновению инцидента ИБ:
* причины возникновения Инцидента;
* временные характеристики событий ИБ;
* данные об используемой учетной записи пользователя;
* качественные характеристики Инцидента (например, используемые протоколы, приложения, ресурсы);
* количественные характеристики Инцидента (например, количество зараженных компьютеров, количество отправленных документов, содержащих информацию ограниченного доступа);
* характер переданной/принятой информации (например, наличие категории переданной/принятой информации в перечне сведений, содержащих коммерческую тайну Общества).
* выявление лиц, причастных к инциденту ИБ, получение от них письменных объяснений;
* определение обстоятельств, влияющих на степень и характер ответственности нарушителя ИБ;
* установление причины и условий, которые способствовали совершению нарушения ИБ, повлекшего возникновение Инцидента;
* блокировка доступа лиц, причастных к инциденту ИБ, к информационному ресурсу на время расследования (при необходимости);
* установление фактического нарушителя требований ИБ.

Одновременно с проведением Расследования структурными подразделениями Общества в соответствии с распределением ответственности могут проводиться работы по локализации и ликвидации последствий инцидента ИБ.

Результаты и материалы Расследования инцидента ИБ доводятся участником Расследования до нарушителя ИБ под личную подпись.

При отказе нарушителя ИБ от ознакомления с результатами Расследования или от личной подписи об ознакомлении, данная информация указывается в служебной записке, оформляемой по результатам Расследования.

7.4. Результаты Расследования оформляются служебной запиской на имя генерального директора Общества с приложением необходимых материалов (включая объяснительные записки и справочные материалы), которые должны содержать следующую информацию:

* основания для проведения Расследования;
* сведения о дате, месте, обстоятельствах возникновения Инцидента;
* сведения о работниках Общества ИБ (фамилия, имя, отчество, должность, при наличии взысканий, в том числе и снятых - вид взыскания, дата и номер приказа) и иных лицах, виновных в возникновении инцидента ИБ, с указанием допущенных ими нарушений требований локальных нормативных документов Общества, законодательства Российской Федерации;
* краткое изложение обстоятельств и причин инцидента ИБ, а также сути действий (бездействия) предполагаемого нарушителя ИБ, находящихся в причинно-следственной связи с Инцидентом;
* предложения по привлечению виновных лиц к мерам дисциплинарной ответственности, предъявлению исковых требований и/или привлечению к дальнейшему расследованию правоохранительных органов или сторонних экспертов.

Также в служебную записку могут быть включены предложения по совершенствованию системы защиты информации для своевременного реагирования на инциденты ИБ и предотвращения нарушений ИБ.

# Мероприятия по результатам Расследования

По результату рассмотрения представленных материалов Расследования генеральный директор Общества принимает решение о применении к нарушителям ИБ из числа работников Общества мер дисциплинарной ответственности и дает соответствующие указания Управлению по работе с персоналом об оформлении решения установленным в Обществе порядком.

По решению генерального директора Общества результаты и материалы Расследования также могут быть переданы постоянно действующей комиссии по установлению фактов нарушения трудовых обязанностей, обстоятельств и причин, приведших к совершению проступков, а также степени вины и персональной ответственности за них, которая:

* - принимает решение о мере ответственности нарушителя (ей) ИБ;
* - проводит, при необходимости, рабочее совещание по Инциденту;
* - утверждает рекомендации по устранению причин возникновения инцидента ИБ.

В случае выявления по результатам Расследования фактов нанесения ущерба интересам Общества, в том числе в случаях, когда такой ущерб стал следствием нарушения своих обязательств контрагентами Общества или действий третьих лиц, материалы Расследования по решению генерального директора Общества передаются в Управление по работе с персоналом для организации претензионной работы и/или подготовки материалов для обращения в правоохранительные органы.

# Права и обязанности работников и должностных лиц Общества при проведении Расследования

9.1. Участник Расследования

Участник Расследования при проведении Расследования имеет право:

* требовать от предполагаемого нарушителя ИБ участия в получении документальных материалов по Инциденту и, при необходимости, в предоставлении доступа к объекту доступа, в отношении которого обнаружено событие ИБ;
* получать доступ к событиям и отчетам специализированного программного или программно-аппаратного обеспечения с последующим их сохранением;
* запрашивать блокировку доступа предполагаемого нарушителя ИБ к информационным ресурсам на время Расследования у должностных лиц, в чьем ведении находятся данные информационные ресурсы, предварительно согласовав данное действие с руководителем подразделения, в котором работает предполагаемый нарушитель ИБ;
* получить от предполагаемого нарушителя ИБ, а также лиц, причастных к инциденту ИБ, необходимые для проведения Расследования материалы, в том числе объяснительные записки в рукописном виде;
* проводить личную беседу в рамках проведения Расследования с предполагаемым нарушителем ИБ или лицами, причастными к инциденту ИБ;
* привлекать должностных лиц по согласованию с соответствующими руководителями структурных подразделений Общества в качестве специалистов для выполнения (в пределах их компетенции) мероприятий в интересах расследования Инцидента.

9.2. Руководитель подразделения

Руководитель подразделения, в подчинении которого находится предполагаемый нарушитель ИБ, при проведении Расследования имеет право запрашивать от участника Расследования информацию об Инциденте, подтверждающую факт нарушения ИБ работником подчиненного ему подразделения.

Руководитель подразделения, в подчинении которого находится предполагаемый нарушитель ИБ, при проведении Расследования обязан:

* обеспечить в кратчайшие сроки предоставление объяснительной записки по Инциденту по требованию участника Расследования;
* обеспечить предоставление доступа к объекту доступа предполагаемого нарушителя ИБ, в отношении которого обнаружено событие ИБ.

9.3. Предполагаемый нарушитель ИБ

Предполагаемый нарушитель ИБ при проведении Расследования имеет право:

* ознакамливаться с результатами Расследования;
* требовать приобщения к материалам Расследования представляемых им документов и материалов;
* подавать мотивированное заявление на имя генерального директора Общества о несогласии с результатами и материалами Расследования.

Предполагаемый нарушитель ИБ при проведении Расследования обязан давать письменные объяснения с изложением своего мнения по поводу возникновения Инцидента, предъявлять доказательства по существу своего объяснения.

ПРИЛОЖЕНИЕ. Схема оповещения подразделении и должностных лиц об инцидентах информационной безопасности

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Категория события/инцидента информационной безопасности** | **Источник информирования о событии ИБ** | **Подразделение, ответственное за фиксацию события ИБ** | **Подразделение, ответственное за первичную обработку события IIБ** | **Дополнительное информирование** |
| 1. **Нарушение режима коммерческой тайны:** | | | | | |
| 1.1 | Фактическая или потенциальная утечка конфиденциальной информации Общества | работник Общества, мониторинг SIEM | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство, при фактической утечке |
| 1.2 | Утрата конфиденциальных документов и/или электронных носителей конфиденциальной информации | работник Общества, служба ИБ | служба ИБ | служба ИБ |  |
| 1.3 | Обнаружение неучтенных либо оставленных без присмотра документов и/или электронных носителей конфиденциальной информации | работник Общества, служба ИБ | служба ИБ | служба ИБ |  |
| 1.4 | Передача конфиденциальной информации по открытым каналам связи, в том числе по электронной почте и сети Интернет | работник Общества, мониторинг SIEM, DLP | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство |
| 1.5 | Нарушение установленного порядка при передаче (предоставлении доступа) конфиденциальной  информации органам государственной власти, иным государственным органам, органам местного самоуправления и контрагентам | служба ИБ | служба ИБ | служба ИБ |  |
| 1. **Нарушение норм н правил обеспечения ИБ Общества при работе со средствами вычислительной техники, информационными системами и сервисами:** | | | | | |
| 2.1 | Несанкционированный доступ к аппаратным и программным средствам в инфраструктуре Общества | работник Общества, служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ |  |
| 2.2 | Несанкционированное подключение средств связи (телефоны, модемы, адаптеры) и средств вычислительной техники (персональные компьютеры, ноутбуки, планшеты, смартфоны), а также другого оборудования к информационной инфраструктуре Общества | работник Общества, служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство |
| 2.3 | Несанкционированное сканирование сети, обход (отключение), несанкционированное изменение настроек установленных механизмов и средств защиты информации, включая попытки таких действий | служба ИБ, отдел ИТ, мониторинг SIEM | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство |
| 2.4 | Несанкционированное распространение и использование программного обеспечения (далее -ПО), в том числе вредоносного и шпионского (обнаружения,  сканирования, взлома, управления, шпионажа, перехвата и подмены пакетов, инфицирования) | служба ИБ, отдел ИТ, мониторинг SIEM | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство |
| 2.5 | Распространение и использование информации и ПО, нарушающих требования законодательства  Российской Федерации, авторские права, условия лицензионных соглашений | работник Общества, служба ИБ, отдел ИТ | служба ИБ | служба ИБ, отдел ИТ |  |
| 1. **Нарушение штатного режима функционирования элементов информационной инфраструктуры Общества, программных или технических средств обработки и передачи информации, эксплуатируемых подразделениями Общества в рамках договорных обязательств:** | | | | | |
| 3.1 | Отказ в обслуживании и (или) выход из строя серверного или сетевого оборудования (включая отсутствие удаленного доступа к инфраструктуре) | работник Общества, отдел ИТ | отдел ИТ | отдел ИТ | руководство (за исключением случаев технической неисправности) |
| 3.2 | Обнаружение (подозрение) вирусного заражения рабочей станции | работник Общества, служба ИБ, отдел ИТ, мониторинг SIEM, антивирусное АО | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ |  |
| 3.3 | Обнаружение вирусной эпидемии (заражение) более 5 рабочих станций | работник Общества, служба ИБ, отдел ИТ, мониторинг SIEM, антивирусное ПО | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство |
| 3.4 | Обнаружение (подозрение) вирусного заражения серверов | служба ИБ, отдел ИТ, мониторинг SIEM, антивирусное ПО | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство |
| 3.5 | Проявление недокументированных функциональных возможностей программных и аппаратно-программных средств | работник Общества | отдел ИТ | отдел ИТ | руководство |
| 3.6 | Непрогнозируемое (без видимых причин) падение производительности аппаратно-программных средств обработки и передачи информации | работник Общества, отдел ИТ, мониторинг SIEM | отдел ИТ | отдел ИТ |  |
| 1. **4. Нарушение штатного режима обработки информации:** | | | | | |
| 4.1 | Несанкционированное удаление, блокирование и изменение файлов, таблиц или записей баз данных | работник Общества, отдел ИТ, мониторинг SIEM | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство, в отношении БД связанных с контрагентами |
| 4.2 | Несанкционированное изменение прав доступа и полномочий в информационных системах и сервисах | работник Общества, служба ИБ, отдел ИТ, мониторинг SIEM | служба ИБ, отдел ИТ | служба ИБ, отдел ИТ | руководство, в отношении БД связанных с контрагентами |
| 4.3 | Отсутствие работоспособных резервных копий информационных систем/СЗИ, подлежащих обязательному резервированию | служба ИБ, отдел ИТ, мониторинг SIEM | отдел ИТ | отдел ИТ | руководство, в отношении БД связанных с контрагентами |
| 4.4 | Компрометация ключа электронной подписи, используемого в Обществе | работник Общества | отдел ИТ | служба ИБ, отдел ИТ |  |

Приложение

к Положению о порядке расследования инцидентов  
 информационной безопасности

**КОНТАКТНАЯ ИНФОРМАЦИЯ**

**для информирования должностных лиц,**

**участвующих в процессе реагирования на события информационной безопасности**

**Взаимодействия по электронной почте осуществляются с работниками, представленными в следующей таблице:**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия Имя Отчество** | **Электронная почта** | **Телефон** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |