Утверждено

Приказом ООО «My Company»

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

Политика

управления инцидентами информационной безопасности   
в ООО «My Company»

г. Москва  
2024г.

Содержание

[Используемые понятия, термины и определения 3](#_Toc170138665)

[1. Введение 4](#_Toc170138666)

[1.1. Общие положения 4](#_Toc170138667)

[1.2. Цели и задачи управления инцидентами ИБ 4](#_Toc170138668)

[2. Система управления инцидентами ИБ 4](#_Toc170138669)

[2.1. Требования к программно-техническим средствам объектов информационной инфраструктуры 4](#_Toc170138670)

[2.2. Требования к составу персонала, участвующего в процессах управления инцидентами ИБ 5](#_Toc170138671)

[3. Порядок выявления инцидентов ИБ и реагирования на эти инциденты 6](#_Toc170138672)

[3.1. Выявление инцидентов ИБ 6](#_Toc170138673)

[3.2. Реагирование на инциденты ИБ 7](#_Toc170138674)

[4. Порядок внесения изменений в документ 8](#_Toc170138675)

# Используемые понятия, термины и определения

**Событие информационной безопасности (событие ИБ)** -идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

**Инцидент информационной безопасности (инцидент ИБ)** - появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности.

**Группа реагирования на инциденты информационной безопасности** - группа соответствующим образом подготовленных работников ООО «My Company», на которых возложены обязанности по обработке инцидентов информационной безопасности в течение их жизненного цикла.

**Объект доступа** - логически выделенный объект (ресурс) информационной системы, доступ к которому регламентируется правилами разграничения доступа.

**Субъект доступа** - лицо или процесс, действия которого по доступу к ресурсам (объектам доступа) информационной системы регламентируются правилами разграничения доступа.

**Объект информатизации** - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

**Служба защиты информации** - подразделение ООО «My Company», которое отвечает за организацию, внедрение и контроль мер по обеспечению информационной безопасности в организации.

Отдел ИТ - подразделение ООО «My Company», которое занимается управлением, развитием и поддержкой информационных систем и технологий, ответственное за обеспечение бесперебойной работы информационных систем.

.

# Введение

## Общие положения

Настоящая Политика управления инцидентами информационной безопасности устанавливает правила, порядок и принципы управления инцидентами информационной безопасности.

Положения настоящей Политики управления инцидентами информационной безопасности обязательны для применения работниками структурных подразделений   
ООО «My Company» (далее - Общество).

## Цели и задачи управления инцидентами ИБ

Целью управления инцидентами ИБ является обеспечение непрерывности бизнес-процессов в Обществе за счет минимизации возможных негативных последствий, вызванных инцидентами ИБ.

Управление инцидентами ИБ основывается на результатах мониторинга информационной безопасности.

Задачами управления инцидентами ИБ являются:

* обнаружение событий ИБ и их дальнейшая обработка с целью выявления инцидентов ИБ;
* оценка инцидентов ИБ с целью выработки соответствующих мер реагирования;
* своевременное предотвращение возможных негативных последствий и оперативное восстановление информационной инфраструктуры после инцидента ИБ;
* внесение необходимых изменений в политики информационной безопасности с целью предотвращения подобных инцидентов ИБ в будущем.

Для реализации процесса управления инцидентами ИБ в Обществе создается система управления инцидентами ИБ.

# Система управления инцидентами ИБ

Система управления инцидентами ИБ включает в себя комплекс программно-технических средств объектов информатизации, организационных мер и персонала, взаимосвязанных регулируемыми отношениями.

## Требования к программно-техническим средствам объектов информационной инфраструктуры

Аудит событий ИБ необходимо вести в соответствующих журналах регистрации и учета событий ИБ программно-технических средств объектов информатизации. Журналы регистрации и учета событий ИБ необходимо вести как локально встроенными средствами программно-технических средств, так и централизованно с применением средств централизованного хранения и обработки событий ИБ (при наличии технической возможности).

Журналы регистрации и учета событий ИБ должны быть защищены от несанкционированного просмотра, удаления и изменения.

Для обеспечения точности записей журналов регистрации и учета событий ИБ и обеспечения корреляции событий ИБ должна осуществляться синхронизация системного времени программно-технических средств с единым доверенным источником, который обеспечивает внутренний сервис точного времени.

В обязательном порядке регистрации подлежат:

1. События, фиксирующие получение пользователями доступа (вход/выход) к объектам защиты, которые включают следующие параметры:

* идентификатор пользователя;
* идентификатор терминала или устройства, с которого осуществлялись попытки доступа;
* дата и время регистрации события;
* объект защиты, к которому был осуществлен доступ;
* результат (успешный/не успешный) получения доступа.

1. События, фиксирующие получение привилегированными пользователями (например, администраторами, разработчиками) доступа к объектам защиты, которые включают следующие параметры:

* идентификатор пользователя;
* дата и время регистрации события;
* идентификатор терминала или устройства, с которого осуществлялись попытки доступа;
* объект защиты, к которым был осуществлен доступ;
* действия, выполненные пользователем (изменение параметров конфигураций средств защиты информации, отключение средств защиты информации, запуск и остановка программно-технических средств объекта защиты).

1. События предоставления и изменения прав доступа к объектам защиты (создание/блокирование/удаление/редактирование учетных записей, групп доступа, изменение прав доступа к значимым конфигурационным файлам и ресурсам).
2. События редактирования параметров настроек журналов регистрации и учета событий ИБ.

Вышеприведенный перечень событий является основой для разработки детального перечня с учетом особенностей конкретного объекта информатизации.

Перечни событий ИБ пересматриваются в следующих случаях:

* при внесении изменений в состав, структуру и характеристики объекта информатизации;
* при пересмотре уровня (класса) защищенности объекта информатизации;
* по результатам расследования инцидентов ИБ.

В случае применения автоматизированных средств централизованного хранения и обработки событий ИБ должна обеспечиваться реализация следующих функций:

* сбор событий от источников событий ИБ;
* нормализация событий ИБ;
* хранение событий на серверах долговременного хранения и в оперативном (60 дней) хранилище данных;
* корреляция собранных событий;
* предоставление инструментов для поиска событий;
* предоставление механизмов формирования отчетов;
* обеспечение возможности автоматического оповещения ответственных лиц об обнаружении потенциальных инцидентов ИБ.

## Требования к составу персонала, участвующего в процессах управления инцидентами ИБ

В процессах управления инцидентами ИБ принимают участие работники следующих подразделений:

- служба защиты информации Общества;

- отдел ИТ;

- пользователи объектов информатизации Общества.

Из числа работников указанных подразделений формируются группы реагирования на инциденты информационной безопасности.

Обязанности членов групп реагирования на инциденты ИБ и порядок расследования устанавливаются в Положении о порядке расследования инцидентов информационной безопасности.

# Порядок выявления инцидентов ИБ и реагирования на эти инциденты

В рамках выполнения процедур выявления инцидентов ИБ и реагирования на них должны выполняться следующие мероприятия:

* мониторинг состояния информационной безопасности;
* обнаружение и оповещение о наступлении события(ий) ИБ, которое(ые) прямо или косвенно указывают на инцидент ИБ;
* дополнительный сбор и анализ информации о наступивших событиях, которые косвенно указывают на инцидент ИБ (в случаях, когда инцидент ИБ не связан с конкретным событием ИБ);
* устранение последствий инцидентов ИБ;
* анализ причин возникновения инцидента ИБ;
* разработка мер по минимизации деструктивных воздействий от повторных инцидентов ИБ.

## Выявление инцидентов ИБ

Инциденты ИБ должны выявляться как непосредственно путем регистрации событий ИБ в программно-технических средствах объектов информатизации, так и путем анализа иных событий, зарегистрированных в соответствующих журналах событий.

Выявление событий ИБ, которые прямо или косвенно указывают на инцидент ИБ, осуществляется администраторами серверов, администраторами информационной безопасности и пользователями объектов информатизации.

Источниками информации о событии ИБ, как правило, являются:

* сообщения от аппаратно-программных средств и средств защиты информации объектов информатизации;
* системы централизованного хранения и обработки событий ИБ;
* результаты анализа записей локальных журналов регистрации и учета событий;
* сообщения от пользователей объектов информатизации;
* обращения работников Общества и обращения работников сторонних организаций.

В рамках выполнения процедур отнесения события ИБ к инцидентам ИБ обеспечивается:

* получение сведений о наступлении событий ИБ, которые прямо или косвенно указывают на инцидент ИБ;
* регистрация и учет фактов наступления событий ИБ, которые прямо или косвенно указывают на инцидент ИБ;
* оповещение руководства Общества, службы защиты информации Общества в установленном порядке о наступлении событий ИБ, которые прямо или косвенно указывают на инцидент ИБ;
* документирование осуществляемых действий в целях обеспечения расследования инцидента ИБ.

По результатам оповещения руководства Общества осуществляется оценка инцидента ИБ, которая проводится с учетом анализа событий на других объектах защиты и средствах защиты информации объекта информатизации, а также смежных однотипных объектах информатизации.

В рамках оценки должна проводиться категоризация событий ИБ по следующим признакам:

* по объекту возникновения (объектам защиты);
* по субъекту возникновения (пользователь, группа пользователей, администратор, вспомогательный персонал, работники сторонних организаций и т.д.);
* по источнику (SIEM, IDM, МЭ, IPS/IDS; сетевое оборудование, операционные системы, прикладные системы и т.д.);
* по методу нарушения (вредоносное ПО, использование уязвимостей, несанкционированное сканирование, разглашение информации, отказ в обслуживании, нарушение политик информационной безопасности и т.д.);
* по типу действий при доступе, обработке, хранении и обмене информации (вход, выход, добавление, уничтожение, создание, модификация; начало, окончание выполнения; изменения, поиск и т.д.);
* по результату действий (успех, отказ);
* по степени критичности.

Порядок оповещения и категоризации событий ИБ детализируется в локальных документах Общества, регулирующих вопросы управления инцидентами ИБ.

По результатам повторной оценки ответственные лица принимают решения о необходимых мерах немедленного реагирования на инцидент ИБ.

## Реагирование на инциденты ИБ

Процедурами реагирования на инциденты ИБ являются:

* немедленное реагирование;
* оценка контроля над инцидентами ИБ;
* последующее реагирование.

В рамках **немедленного реагирования** возможно применение аварийных мер и средств (например, отключение электроэнергии информационной системы (сервиса, сегмента вычислительной сети), в которой выявлен инцидент ИБ, по предварительному согласованию с руководителем структурного подразделения, ответственного за эксплуатацию информационной системы, и (или) определение дополнительных постоянных мер и средств контроля и управления, а также уведомление руководства Общества о принятии этих мер).

Целью немедленного реагирования на инцидент ИБ является минимизация последствий возможного деструктивного воздействия инцидентов ИБ на ИТ-актив.

В рамках оценки контроля над инцидентом ИБ необходимо удостовериться, что в отношении смежных (однотипных) объектов информатизации установленный тип инцидента ИБ не распространяется (выполняется в зависимости от типа инцидента ИБ).

В рамках последующего реагирования должны выполняться в установленном в Обществе порядке:

* восстановительные работы на пораженных в результате инцидента ИБ объектах информатизации до штатного рабочего состояния;
* дополнительные меры для снижения вероятности повторения инцидента ИБ.

После закрытия инцидента ИБ ответственные лица определяют и анализируют причины его возникновения.

В процессе анализа причин возникновения инцидента ИБ необходимо рассматривать не только конкретный инцидент, но и возможно связанные с ним инциденты ИБ и/или события ИБ на предмет:

* тенденций/закономерностей;
* проблемных областей;
* дополнительных или предупредительных мер защиты для снижения вероятности появления инцидентов в будущем.

В качестве источников для анализа необходимо также использовать информацию об инцидентах ИБ и соответствующих им уязвимостях, полученную из общедоступных источников (профильные интернет ресурсы производителей программного и аппаратного обеспечения объектов защиты, специализированных организаций в области выявления уязвимостей и т.д.).

Анализ причин возникновения и разработка мер по недопущению в будущем подобных инцидентов ИБ проводится в рамках процедур расследования инцидентов.

# Порядок внесения изменений в документ

Предложения по изменению настоящего документа могут вносить все участники процесса управления инцидентами ИБ. Предложения направляются в службу информационной защиты Общества, специалисты которого проводят их накопление, обобщение и учитывают в ходе корректировки документа. Изменения в документе вступают в силу в составе новой редакции Политики управления инцидентами информационной безопасности, согласованной и утвержденной установленным в Обществе порядком.