**ПРИКАЗ**

**«\_\_»\_\_\_\_\_\_\_\_\_\_2024 г. №\_\_\_\_\_\_\_**

О реализации мер по обеспечению безопасности информационной инфраструктуры ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_»

Для обеспечения информационной безопасности информационной инфраструктуры ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_» должны быть реализованы отдельные меры, приведенные в Политиках ниже.

**ПРИКАЗЫВАЮ:**

1. Утвердить План аварийного восстановления (Приложение 1).

Контроль за исполнением настоящего приказа оставляю за собой.

|  |  |
| --- | --- |
| Генеральный директор |  |

|  |  |
| --- | --- |
|  | Приложение 1  Утверждено приказом  Генерального директора  ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_»  № \_\_\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |

**План восстановления после катастроф**

**(Disaster Recovery Plan)**

**ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_»**

# Содержание

[1. Содержание 3](#_Toc175570983)

[2. Введение 5](#_Toc175570984)

[2.1 Назначение 5](#_Toc175570985)

[2.2 Область применения 5](#_Toc175570986)

[2.3 Определения 5](#_Toc175570987)

[2.4 Ответственные лица 6](#_Toc175570988)

[2.5 Связанные документы 6](#_Toc175570989)

[3. Оценка рисков и воздействий 7](#_Toc175570990)

[3.1 Идентифицированные угрозы и вероятность их возникновения 7](#_Toc175570991)

[3.2 Последствия инцидентов 7](#_Toc175570992)

[4. Критичные данные и системы 7](#_Toc175570993)

[4.1 Критичные данные 7](#_Toc175570994)

[4.2 Инфраструктура 7](#_Toc175570995)

[4.3 Системы мониторинга 8](#_Toc175570996)

[4.4 Резервные копии 8](#_Toc175570997)

[5. Время восстановления и доступность 8](#_Toc175570998)

[5.1 Время восстановления критической информации 8](#_Toc175570999)

[5.2 Время восстановления остальной информации 8](#_Toc175571000)

[5.3 Доступность 8](#_Toc175571001)

[6. Реакция на инциденты и восстановление 9](#_Toc175571002)

[6.1 Сценарии реагирования 9](#_Toc175571003)

[6.2 Восстановление данных 12](#_Toc175571004)

[6.3 Восстановление ИТ-инфраструктуры 12](#_Toc175571005)

[6.4 Организация работы сотрудников в чрезвычайной ситуации 13](#_Toc175571006)

[6.5 Коммуникация с клиентами и партнерами: 13](#_Toc175571007)

[7. Тестирование и обновление плана 14](#_Toc175571008)

[7.1 Тестирование восстановления 14](#_Toc175571009)

[8. Приложения 15](#_Toc175571010)

[8.1 Приложение 1. Типовые действия сотрудников 15](#_Toc175571011)

[9. Приложение 2. к Положению о порядке расследования инцидентов информационной безопасности 17](#_Toc175571012)

[9.1 КОНТАКТНАЯ ИНФОРМАЦИЯ для информирования должностных лиц, участвующих в процессе восстановления 17](#_Toc175571013)

|  |  |
| --- | --- |
|  | Содержащаяся в данном документе информация является конфиденциальной и не может распространяться без разрешения и упоминания ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_». |

# Введение

## Назначение

**Назначение плана восстановления после катастроф (DRP) - обеспечить непрерывность бизнес-процессов и минимизировать время простоя в случае чрезвычайных ситуаций. DRP направлен на быстрое восстановление критичных бизнес-функций, данных и ИТ-инфраструктуры.**

## Область применения

В настоящем документе установлены требования к действиям сотрудников организации ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_», направленным на восстановление работоспособности после возникновения инцидентов, снижения вероятности их реализации.

Этот документ применим ко всем сотрудникам и ресурсам компании ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_», включая офисные помещения, серверы, сети, базы данных, облачные сервисы и клиентские данные.

## Определения

| **Термин** | **Обозначение** |
| --- | --- |
| **Деятельность** | Процесс или система процессов, осуществляемых организацией с целью производства одного или более видов продукции, оказания услуг или их поддержки. |
| **Непрерывность бизнеса** | Стратегическая и тактическая способность организации планировать свою работу в случае инцидента и нарушения её деятельности, направленная на обеспечение непрерывности деловых операций на установленном приемлемом уровне. |
| **Документ** | Информация и её носитель. |
| **Инцидент** | Ситуация, которая может произойти и привести к нарушению деятельности организации, разрушениям, потерям, чрезвычайной ситуации или кризису в бизнесе. |
| **Заинтересованная сторона, причастная сторона** | Лицо или организация, которые могут влиять на решения или деятельность, а также быть затронуты или ощущать себя затронутыми ими. |
| **Роль** | описание ограниченного множества действий, выполняемых персоналом в рамках определённого процесса. |
| **Персонал** | Люди, работающие в организации и находящиеся под её управлением. |
| **Процедура** | Совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующих входы в выходы. |
| **Риск** | Следствие влияния неопределенности на достижение поставленных целей. |
| **Оценка риска** | Процесс, охватывающий идентификацию риска, анализ риска и сравнительную оценку риска. |
| **Мониторинг** | Определение состояния системы, процесса или деятельности. |
| **Цель** | Результат, который должен быть достигнут. |
| Организация | Группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений. |
| **Высшее руководство** | Лицо или группа работников, осуществляющих направление деятельности и управление организацией на высшем уровне. |

## **Ответственные лица**

* Руководитель ИТ-отдела.
* Специалисты по информационной безопасности.
* Руководители подразделений.
* Сотрудники, назначенные для реагирования на инциденты.

## **Связанные документы**

* Положение о порядке расследования инцидентов информационной безопасности утв. приказом №\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* Сценарии реагирования на инциденты.
* Политика информационной безопасности утв. приказом №\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* Регламент резервного копирования и восстановления данных утв. приказом   
  № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-.
* Контактная информация ответственных лиц.

# Оценка рисков и воздействий

## Идентифицированные угрозы и вероятность их возникновения

* Хакерские атаки (небольшая вероятность).
* Человеческий фактор (небольшая вероятность).
* Технические сбои (небольшая вероятность).
* Финансовые проблемы (небольшая вероятность).

## Последствия инцидентов

* Технический сбой: остановка бизнес-процессов, потеря доступности ИТ-ресурсов.
* Человеческий фактор: утечка данных клиентов, компрометация внутренней информации.
* Хакерские атаки: захват управления инфраструктурой, кража исходного кода и данных клиентов.
* Финансовые проблемы: остановка бизнес-процессов, потеря доступности ИТ-ресурсов.

# Критичные данные и системы

## Критичные данные

* Данные клиентов.
* Базы данных клиентов.
* Исходный код программного обеспечения.

В случае инцидента, связанного с нарушением безопасности или техническим сбоем, применяются следующие меры для защиты критичных данных:

* Изоляция сетевого сегмента: в случае выявления инцидента, который может угрожать безопасности критичных данных (например, хакерская атака или вирусное заражение), осуществляется немедленная изоляция соответствующего сетевого сегмента, в котором хранятся или обрабатываются данные.
* Ограничение доступа к ресурсам: в ходе инцидента доступ к критичным данным и системам может быть временно ограничен или полностью заблокирован для всех пользователей, кроме лиц, непосредственно участвующих в реагировании на инцидент.
* Уведомление ответственных лиц: все ответственные лица, включая специалистов по информационной безопасности, администраторов баз данных и системных администраторов, незамедлительно уведомляются о происшествии.
* Контроль доступа и мониторинг: после изоляции сетевого сегмента и ограничения доступа ведется усиленный мониторинг событий и действий, связанных с доступом к критичным данным. Вся активность записывается и анализируется для выявления потенциальных угроз и их устранения.

## Инфраструктура

* Облачные платформы: Cloud.
* Почта на Яндексе.
* 8 физических серверов, 120 виртуальных серверов.
* Операционные системы: Windows Server, Linux.
* Сетевой периметр: межсетевой экран, VPN (l2tp).

## Системы мониторинга

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

## Резервные копии

* Все системы разработчиков и данные клиентов.
* Хранятся физически отдельно и в облачной инфраструктуре (Cloud).

# Время восстановления и доступность

## Время восстановления критической информации

* До 12 часов.

## Время восстановления остальной информации

В течение недели.

## Доступность

24/7.

# Реакция на инциденты и восстановление

## Сценарии реагирования

Таблица 1. Сценарии реагирования

| № | Инцидент | Сценарии реагирования (в соответствии со сценарием реагирования) | Ответственные лица | Документация |
| --- | --- | --- | --- | --- |
|  | Антивирусное заражение | Изоляция зараженного устройства от сети | ИТ/ИБ | Запись инцидента в журнале инцидентов |
| Сканирование и удаление вируса с помощью антивирусного ПО |
| Восстановление данных из резервных копий (если требуется). | Отчет о расследовании инцидента |
| Проведение расследования для выявления источника заражения и предотвращения повторного инцидента. |
|  | Заражение сети | Изоляция зараженного сегмента сети. | ИТ/ИБ  Руководство | Запись инцидента в журнале инцидентов |
| Полное сканирование всей сети с использованием антивирусного ПО. |
| Восстановление нормальной работы сети. | Отчет о расследовании инцидента |
| Обновление политик безопасности для предотвращения повторных заражений. |
|  | Атака программ шифровальщиков | Изоляция зараженного устройства от сети | ИТ/ИБ | Запись инцидента в журнале инцидентов |
| Сканирование и удаление вредоносного ПО |
| Проведение расследования для выявления источника заражения и предотвращения повторного инцидента. | Отчет о расследовании инцидента |
| Обновление политик безопасности для предотвращения повторных заражений. |
|  | Brute-force атака на учетную запись | Блокировка учетной записи. | ИТ/ИБ | Запись инцидента в журнале инцидентов |
| Смена пароля и применение многофакторной аутентификации. |
| Анализ логов для выявления источника атаки. | Отчет о расследовании инцидента |
| Уведомление пользователей о необходимости смены паролей. |
|  | Несанкционированный доступ | Немедленная блокировка доступа. | ИТ/ИБ | Запись инцидента в журнале инцидентов |
| Проведение расследования инцидента. |
| Уведомление заинтересованных сторон. | Отчет о расследовании инцидента |
| Обновление политик безопасности и проверка логов. |
|  | Повышение привилегий | Блокировка учетной записи. | ИТ/ИБ | Запись инцидента в журнале инцидентов |
| Возврат в исходное состояние |
| Анализ логов для выявления источника атаки. | Отчет о расследовании инцидента |
|  | DDoS на инфраструктуру | Задействовать резервный VPN сервер | ИТ/ИБ  Руководство | Запись инцидента в журнале инцидентов |
| Региональная блокировка атакующих IP/подсетей |
| Ограничить количество запросов | Отчет о расследовании инцидента |
| Добавить фильтры для отбрасывания пакетов |
|  | Ошибочное развертывание в продуктивной среде | Немедленное откатывание изменений | ИТ/ИБ/DevOps | Пересмотр процедур развертывания |
| Анализ причин и обновление процедур развертывания | Запись инцидента в журнале инцидентов |
|  | Неправильная конфигурация серверов | Отключение или изоляция проблемного сервера | ИТ/ИБ/DevOps | Проведение анализа причин ошибки |
| Восстановление сервера из резервной копии или конфигурации | Обучение администратора |
|  | Ошибки в коде, влияющие на безопасность | Немедленное исправление уязвимости | ИБ/Dev | Обновление процедур безопасности при написании кода |
| Проведение проверки безопасности всего кода |
|  | Нарушение процедур безопасности (логин/пароль доступным для других) | Немедленное исправление нарушений (например, смена паролей, усиление контроля доступа) | ИТ/ИБ  Руководство | Обучение сотрудников |
| Отчет о расследовании инцидента |
|  | Финансовые проблемы | Обещанный платеж. | ИТ  Руководство |  |
| Гарантийное письмо |

## Восстановление данных

Действия:

* Определение данных, которые необходимо восстановить.
* Идентификация последней доступной резервной копии.
* Восстановление данных из резервных копий, расположенных физически отдельно и в облачной инфраструктуре (Cloud \_\_\_\_) (Регламент резервного копирования и восстановления информации утв. приказом № \_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_).
* Проверка целостности данных после восстановления.
* Уведомление пользователей о завершении восстановления и доступности данных.

Ответственные лица:

* Сотрудники ИТ-отдела

***Документация:***

* Запись процесса восстановления в журнале инцидентов
* Отчет о проверке целостности данных и результатах восстановления

## Восстановление ИТ-инфраструктуры

Действия:

* Идентификация затронутых систем и сервисов.
* Восстановление систем из резервных копий (Регламент резервного копирования и восстановления информации утв. приказом № \_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_).
* Переподключение всех пользователей к восстановленным системам.
* Проверка всех систем на работоспособность после восстановления.
* Проведение тестирования всех критичных систем для подтверждения их корректной работы.

Ответственные лица:

* Сотрудники ИТ-отдела

Документация:

* Запись процесса восстановления в журнале инцидентов
* Отчет о проверке работоспособности систем и результатах тестирования

## Организация работы сотрудников в чрезвычайной ситуации

Действия:

* Назначение ответственных лиц за реагирование на инциденты информационной безопасности (Положение о порядке расследования инцидентов информационной безопасности утв. приказом №\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_).
* Создание группы реагирования на инциденты (Положение о порядке расследования инцидентов информационной безопасности утв. приказом №\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_).
* Организация удаленной работы через VPN (дублирующий сервер VPN).
* Создание временных рабочих мест в случае недоступности офиса.
* Обеспечение сотрудников необходимыми ресурсами для удаленной работы (ноутбуки, доступ к необходимым системам).
* Проведение инструктажа сотрудников по новым условиям работы.

Ответственные лица:

* Руководители подразделений
* Сотрудники ИТ-отдела

Документация:

* Запись мер по организации работы в чрезвычайной ситуации.
* Отчет о проведенном инструктаже сотрудников.

## Коммуникация с клиентами и партнерами:

Действия:

* Создание системы уведомлений и информирования клиентов.
* Назначение ответственного за коммуникацию с клиентами.
* Использование электронной почты, SMS, социальных сетей и других каналов связи для информирования клиентов о текущем статусе и мерах, принимаемых для восстановления нормальной работы.
* Обеспечение прозрачности и регулярных обновлений информации для клиентов.

Ответственные лица:

* Руководители подразделений
* Маркетинговый отдел

Документация:

* Запись всех уведомлений и коммуникаций с клиентами
* Отчет о результатах и обратной связи от клиентов

# Тестирование и обновление плана

## Тестирование восстановления

Действия:

* Проведение ежегодного тестирования восстановления из резервных копий.
* Включение всех критичных систем и данных в процесс тестирования.
* Проведение тестирования в условиях, максимально приближенных к реальным.
* Анализ результатов тестирования и выявление проблемных областей.
* Обновлять DRP по мере выявления новых рисков и изменения ИТ-инфраструктуры (например, раз в год).
* Вести журнал проведенных тестирований и изменений DRP.

# Приложения

## Приложение 1. Типовые действия сотрудников

| **Функции** | **Средство** | | **Выполняемые действия** | **События ИБ** |
| --- | --- | --- | --- | --- |
| Мониторинг событий ИБ и выявление инцидентов ИБ | Основное | Мониторинг \_\_\_\_\_\_\_\_\_\_\_\_ | Мониторинг и направление на предварительный анализ (при необходимости) поступающих сообщений об авариях, недоступности каналов связи, инфраструктурных сервисов, средств защиты, инцидентах ИБ и подозрениях на инциденты, информирование работников о поступающих событиях недоступности каких-либо инфраструктурных сервисов, компонентов, либо каналов связи | Все сообщения об авариях, затрагивающие те или иные сервисы |
| Электронная почта | Мониторинг сообщений, поступающих персональный корпоративный почтовый ящик от МЭ | Неверный логин/пароль, детект атаки |
| Kaspersky Security Center | Подробный анализ событий в части САЗ, поступивших от средств мониторинга (напрямую или в KAV), подтверждение фактов того, что зараженный объект не был вылечен/удален/заблокирован | Связанные с САЗ в соответствии с классификацией |
| Microsoft Active Directory | Получение сведений о доменных учетных записях и группах, объектах полномочий, фигурирующих в событиях ИБ, поступивших от средств мониторинга | Все поступившие сообщения (особое внимание следует уделять сообщениям, поступившим от службы ИБ) |
| Вспомогательное | Журнал ИТ активов | Просмотр информации об установленных обновлениях на объектах, подвергшихся, об учетных записях пользователей в Unix-системах | В соответствии с классификацией (при необходимости получения дополнительных сведений) |
| ИТ-календарь | Просмотр работ, зафиксированных работниками других подразделений в ИТ-календаре |  |
| Открытие и обработка карточек инцидентов ИБ | Получение информации о закреплении АРМ за пользователями, получение данных о пользователях, сбор логов и событий, связанных с АРМ | В соответствии с классификацией |
| Обработка событий ИБ | Все источники мониторинга и сбора событий | | Анализ событий, при помощи всех доступных средств мониторинга (основных и вспомогательных) с целью получения максимально полной информации по ним, обработка (внесение записей и закрытие событий) событий в системе, запрос информации по ним у лиц, отвечающих за эксплуатацию объекта информатизации, фигурирующего в событии | Все события ИБ |
| Просмотр ИТ-календаря | ИТ-календарь | | Выполнение рассылок, согласно утвержденным сценариям реагирования, информирование администраторов ИТ-активов, АИБ, руководителей, | Все записи в ИТ-календаре, приходящиеся на смену работника |
| Регистрация событий ИБ и направление запросов на устранение недостатков | Журнал инцидентов ИБ | | Открытие и обработка карточек инцидентов ИБ | По решению руководства отдела или Управления |
| Мониторинг сетевой активности | Панель управления \_\_\_\_\_\_\_\_\_, журнал сервера VPN | | Мониторинг сетевой активности в инфраструктуре согласно отчетам \_\_\_\_\_\_\_\_\_\_\_\_ | Блокировка трафика |

# Приложение 2. к Положению о порядке расследования инцидентов информационной безопасности

## КОНТАКТНАЯ ИНФОРМАЦИЯ для информирования должностных лиц, участвующих в процессе восстановления

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия Имя Отчество** | **Электронная почта** | **Телефон** |
| **Руководство** | | | |
|  |  |  |  |
|  |  |  |  |
| **ИТ отдел** | | | |
|  |  |  |  |
|  |  |  |  |
| **Служба информационной безопасности** | | | |
|  |  |  |  |
| **Отдел маркетинга** | | | |
|  |  |  |  |
| **Структурное подразделение** | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |