**Утверждено**

**Приказом ООО «My Company»**

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

**План аварийного восстановления**

**(Disaster Recovery Plan)**

**ООО «My Company»**

**1. Введение**

**1.1 Цель:**

Цель 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.

**1.2 Область применения:**

Этот план применим ко всем сотрудникам и ресурсам компании My Company, включая офисные помещения, серверы, сети, базы данных, облачные сервисы и клиентские данные.

**1.3 Ответственные лица:**

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

**1.4 Связанные документы:**

* Положение о расследовании инцидентов информационной безопасности. Устанавливает основания, цели, задачи и порядок проведения расследований инцидентов информационной безопасности. Применяется во время мероприятий по реагированию на инциденты информационной безопасности.
* Сценарии реагирования на инциденты. Применяется во время мероприятий по реагированию на инциденты информационной безопасности.
* Политики и процедуры информационной безопасности.
* Контактная информация ответственных лиц.
* Регламент работы с резервными копиями. Применяется во время мероприятий по восстановлению инфраструктуры.

**2. Оценка рисков и воздействий**

**2.1 Идентифицированные угрозы и вероятность их возникновения:**

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

**2.2 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.

**3. Критичные данные и системы**

**3.1 Критичные данные:**

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

В случае инцидента, связанного с нарушением безопасности или техническим сбоем, применяются следующие процедуры 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.

**3.2 Инфраструктура:**

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

**3.3 Системы мониторинга:**

* Zabbix

**3.4 Резервные копии:**

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

**4. Время восстановления и доступность**

**4.1 Время восстановления критической информации:**

* До 12 часов.

**4.2 Время восстановления остальной информации:**

* В течение недели.

**4.3 Доступность:**

* 24/7

**5. Реакция на инциденты и восстановление**

**5.1 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 | 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 | Запись инцидента в журнале инцидентов |
| Региональная блокировка атакующих IP/подсетей |
| Ограничить количество запросов | Отчет о расследовании инцидента |
| Добавить фильтры для отбрасывания пакетов |
|  | Финансовые проблемы | Обещанный платеж. | ИТ  Руководство |  |
| Гарантийное письмо |

**5.2 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 (Selectel) (Регламент резервного копирования и восстановления информации).
* 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

**5.3 Восстановление ИТ-инфраструктуры:**

*Действия:*

* Идентификация затронутых систем и сервисов.
* Восстановление систем из резервных копий (Регламент резервного копирования и восстановления информации).
* 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

**5.4 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 №2/01-07/2024 от 01.07.2024).
* Создание группы реагирования на инциденты (Положение о порядке расследования инцидентов информационной безопасности утв. приказом №2/01-07/2024 от 01.07.2024).
* 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.

**5.5 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

**6. Тестирование и обновление плана**

**6.1 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.

**Приложение 1. Типовые действия сотрудников**

| **Функции** | **Средство** | | **Выполняемые действия** | **События ИБ** |
| --- | --- | --- | --- | --- |
| Мониторинг событий ИБ и выявление инцидентов ИБ | Основное | Мониторинг Zabbix | 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 Zywall | | Мониторинг сетевой активности в инфраструктуре согласно отчетам Zywall | 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** | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |