# **План реагирования на инцидент кибербезопасности**

Данный план разработан на основе документа NIST SP 800-61, Computer Security Incident Handling Guide.

1. **Подготовка**

Контактная информация членов команды реагирования на инциденты ИБ, сотрудников компании, внешних контрагентов: номера телефонов, адреса эл. почты, псевдонимы в мессенджерах, а также способы проверки аутентичности контакта:

|  |  |  |  |
| --- | --- | --- | --- |
| **Имя** | **Номер телефона** | **Адрес эл. почты** | **Способ проверки** |
|  |  |  |  |
|  |  |  |  |

Способы сообщения пользователями информации об инцидентах: телефонные номера, адрес эл. почты, веб-форма или мессенджеры; при этом как минимум один способ должен позволять передавать информацию анонимно:

|  |  |
| --- | --- |
| **Способ** | **Детали** |
|  |  |
|  |  |

Система регистрации заявок для хранения информации об инциденте и мониторинга его статуса:

|  |  |
| --- | --- |
| **Описание** | **Ссылка** |
|  |  |
|  |  |

Устройства для связи и работы членов команды реагирования (с установленным необходимым ПО, например для анализа данных и сетевого трафика, расследования инцидентов, подготовки отчетов и т.д.), устройства для выхода в интернет (LTE-роутер), а также устройства видео- и аудио-фиксации:

|  |  |  |
| --- | --- | --- |
| **Устройство** | **Расположение** | **Детали** |
|  |  |  |
|  |  |  |

Заранее подготовленное место для встречи и совместной работы членов команды реагирования: переговорная комната, выполняющая функцию «командного пункта».

Рекомендуется заранее позаботиться о наличии в данном помещении необходимых канцелярских принадлежностей, маркеров, интерактивной доски, а также пакетов и конвертов для хранения улик.

|  |  |
| --- | --- |
| **Место** | **Детали** |
|  |  |
|  |  |

Место для защищенного хранения предметов и документов, имеющих отношение к инциденту:

|  |  |
| --- | --- |
| **Место** | **Детали** |
|  |  |
|  |  |

Программное и аппаратное обеспечение для анализа кибер-инцидентов: устройства и накопители для создания резервных копий, хранения логов и любой другой информации:

|  |  |  |
| --- | --- | --- |
| **Устройство** | **Расположение** | **Детали** |
|  |  |  |
|  |  |  |

Запасное оборудование: принтеры, сетевое оборудование, компьютеры и серверы, образы ПО и виртуальных машин, необходимых для восстановления информации и работоспособности ИТ-инфраструктуры:

|  |  |  |
| --- | --- | --- |
| **Устройство или ПО** | **Расположение** | **Детали** |
|  |  |  |
|  |  |  |

Техническая документация ИТ-инфраструктуры и оборудования, а также методические документы для анализа инцидентов:

|  |  |
| --- | --- |
| **Документация** | **Детали** |
|  |  |
|  |  |

1. **Обнаружение**

Ответственному за кибербезопасность следует заблаговременно оценить текущее состояние кибербезопасности в организации и определить наиболее вероятные типовые методы атак, которые могут быть использованы злоумышленниками в отношении данной организации.

Чтобы не перебирать все возможные объекты воздействия, можно начать с анализа рисков и таким образом выяснить, какие из рисков точно будут иметь негативные последствия для организации: финансовые, правовые, репутационные и т.д. Исходя именно из последствий, вы сможете определить возможные события, способные к ним привести.

В качестве методического материала рекомендуется использовать матрицу MITRE ATT&CK: <https://attack.mitre.org/>. С её помощью вам будет легче выделить наиболее вероятные техники атак для вашей организации, а следовательно, найти способ правильно отреагировать на каждый из типов инцидентов (заражение вредоносным кодом, истощение ресурсов, несанкционированный доступ и прочие) в отдельности.

|  |  |
| --- | --- |
| **Тип инцидента** | **Стратегия реагирования** |
|  |  |
|  |  |

Определение признаков инцидентов кибербезопасности, согласно данным из систем мониторинга, систем защиты от вредоносного ПО и спама, IDS/IPS-систем или SIEM-систем, указывающие на то, что инцидент кибербезопасности может произойти в будущем или происходит в данный момент:

|  |  |  |  |
| --- | --- | --- | --- |
| **Дата** | **Время** | **Событие** | **Описание** |
|  |  |  |  |
|  |  |  |  |

1. **Анализ**

Документирование и регистрация инцидентов кибербезопасности (шаблон):

|  |  |
| --- | --- |
| **Номер инцидента** |  |
| **Статус** |  |
| **Оценка последствий** |  |
| **Приоритет** |  |
| **Индикаторы** |  |
| **Доказательства и улики** |  |
| **Предпринятые меры** |  |
| **Запланированные меры** |  |
| **Связанные события** |  |
| **Команда реагирования** |  |
| **Заинтересованные лица** |  |

Уведомление об инциденте:

|  |  |  |  |
| --- | --- | --- | --- |
| **Дата** | **Время** | **Инцидент** | **Список лиц** |
|  |  |  |  |
|  |  |  |  |

1. **Сдерживание**

План сдерживания и снижения уровня ущерба:

|  |  |  |  |
| --- | --- | --- | --- |
| **Дата** | **Время** | **Предпринимаемое действие** | **Ответственный за выполнение** |
|  |  |  |  |
|  |  |  |  |

1. **Устранение**

План устранения уязвимостей и последствий:

|  |  |  |  |
| --- | --- | --- | --- |
| **Дата** | **Время** | **Предпринимаемое действие** | **Ответственный за выполнение** |
|  |  |  |  |
|  |  |  |  |

1. **Восстановление**

План восстановления:

|  |  |  |  |
| --- | --- | --- | --- |
| **Дата** | **Время** | **Предпринимаемое действие** | **Ответственный за выполнение** |
|  |  |  |  |
|  |  |  |  |

1. **Анализ «выученных уроков»**

Что произошло и как команда реагирования справилась с ситуацией? Что следует улучшить и какие ресурсы могут для этого потребоваться?

|  |  |  |
| --- | --- | --- |
| **Что произошло** | **Анализ** | **Меры по улучшению** |
|  |  |  |
|  |  |  |