# План реагирования на инциденты кибербезопасности — это свод четко регламентированных правил, где прописаны шаги, которые сотрудники должны выполнять при обнаружении опасности. План разрабатывается совместно с высшим руководством организации и S**План реагирования на инциденты кибербезопасности: что это и почему он нужен каждой организации**

Ранее в своих материалах о том, [как защититься от DDoS-атак](https://ddos-guard.net/ru/blog/sposoby-zashity-ot-ddos-atak), мы неоднократно советовали составить план своей инфраструктуры, ее уязвимых мест и первичных действий при кибератаках. Сегодня поговорим о том, что такое план реагирования на киберинциденты, почему он нужен каждой организации, как его составить и что он в себя включает.

По мере развития изощренности кибератак, должна трансформироваться и стратегия их предотвращения. К сожалению, многие компании полагаются на устаревшие планы, а еще большее количество и вовсе их не имеет.

Чтобы увеличить шансы пережить непредвиденную атаку и сохранить репутацию, любому бизнесу, проекту, компании нужно задуматься о создании плана реагирования на инциденты кибербезопасности.

**Что такое инцидент кибербезопасности**

**Инцидент кибербезопасности**— это ситуация, которая ведет к нарушению политики информационной безопасности организации и подвергает риску ее конфиденциальные сведения: личные данные клиентов, государственные, коммерческие и врачебные тайны. Далее в тексте вы встретите аббревиатуру КБ — это сокращенный вариант термина «кибербезопасность».

**Национальный координационный центр по компьютерным инцидентам (НКЦКИ) выделяет следующие виды инцидентов кибербезопасности:**

|  |  |
| --- | --- |
| 1. DoS-атаки | 8. несанкционированный вывод объекта из строя |
| 2. DDoS-атаки | 9. публикация в объекте мошеннической информации |
| 3. рассылка спама с объекта | 10. использование объекта для распространения вредоносного ПО |
| 4. захват сетевого трафика объекта | 11. социальная инженерия, направленная на компрометацию объекта |
| 5. компрометация учетной записи в объекте | 12. публикация в объекте запрещенной законодательством РФ информации |
| 6. успешная эксплуатация уязвимости в объекте | 13. несанкционированное изменение информации, обрабатываемой в объекте |
| 7. внедрение в объект модулей вредоносного ПО | 14. несанкционированное разглашение информации, обрабатываемой в объекте |

Атаки могут производиться бесчисленным количеством способов, поэтому невозможно разработать единую инструкцию для решения всех нарушений. Каждый отдельный тип инцидента нуждается в уникальной стратегии реагирования. Далее рассмотрим несколько типов угроз, основанных на общих векторах атак. Они помогут определиться с выбором стратегии реагирования.

**Типы инцидентов КБ по вектору атаки:**

**Внешний или съемный носитель:**атака выполняется со съемного носителя (например, флэш-накопителя, компакт-диска) или периферийного устройства.

**Истощение:** атака, в которой используются методы компрометации, ухудшения качества или уничтожения систем, сетей или сервисов. Механизм заключается в подборе учетных данных пользователя для получения несанкционированного доступа.

**Веб:** Атака, осуществляемая с сайта или веб-приложения.

**Email:** атака идет с помощью сообщений на электронную почту или вложения, ее цель — скомпрометировать данные пользователя. Этот вид атаки известен под названием «фишинг» и является одним из наиболее распространенных.

**Ненадлежащее использование:** любой инцидент, возникший в результате нарушения авторизованным пользователем политики организации.

**Потеря или кража оборудования:** потеря ноутбука, смартфона или другого носителя информации, используемого организацией.

**Эксперт компании DDoS-Guard, руководитель направления защиты L7 Дмитрий Никонов, отмечает:** «Мы видим, что атаки становятся более интеллектуальными. Мы активно наблюдаем за созданием геораспределенных ботнет-сетей, которые включают в себя почти все континенты планеты.

Злоумышленники создают и выкладывают проекты с открытым кодом, и инструкцией как развернуть проект у себя на ПК, чтобы стать частью ботнета. Наиболее популярные атаки сейчас: backdoors, malware, ransomware, phishing и website defacement.

Из уникальных примеров можно выделить случай, когда злоумышленники использовали онлайн-игру для атак. Все пользователи, которые заходили в нее, автоматически становились участниками централизованной атаки на определенные веб-ресурсы».

**Возможные цели и мотивы злоумышленников:**

|  |  |
| --- | --- |
| 1. вымогательство | 6. создание нечестной конкуренции |
| 2. похищение средств | 7. демонстрация силы и возможностей |
| 3. уничтожение бизнеса | 8. ущерб репутации компании или государства |
| 4. корпоративный шпионаж | 9. площадка для дальнейших атак на другие компании |
| 5. государственный шпионаж | 10. похищение ценной информации для ее продажи или использования |

**Что такое план реагирования на инцидент кибербезопасности**

**План реагирования на инциденты кибербезопасности** — это свод четко регламентированных правил, где прописаны шаги, которые сотрудники должны выполнять при обнаружении опасности. План разрабатывается совместно с высшим руководством организации и SOC (Центр информационной безопасности). Составляются сценарии по реагированию на самые распространенные методы атак. Это поможет сотрудникам правильно и оперативно действовать в любой критической ситуации.

**План реагирования может использоваться в качестве руководства при ряде действий:**

* обнаружение угроз;
* реагирование на инциденты;
* анализ и документирование инцидента;
* взаимодействие между подразделениями внутри организации;
* определение необходимых шагов для повышения эффективности процедур реагирования.

Необходимо регулярно проводить тестовый контроль обучения, чтобы план реагирования был знаком команде. Реакция должна быть чёткой и быстрой. Ошибки крайне нежелательны, поэтому важно проверять план на практике и анализировать скорость устранения инцидента.

**Почему каждой организации нужен план реагирования**

Злоумышленники атакуют как небольшие проекты, так и крупные компании, среди которых банки, энергетические компании, медиаресурсы, ИТ-предприятия и другие. Сегодня кибербезопасность —  стратегическая необходимость для каждой организации.

В 2020 году компания IBM опубликовала [отчет](http://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue), согласно которому, лишь 26% компаний имеют четкий план реагирования на киберинциденты. Низкий уровень защищенности чреват для бизнеса и общества серьезными последствиями. Общее число происшествий растет ежеквартально, злоумышленники постоянно совершенствуют атаки, а их эффективность только повышается, поэтому важно быть начеку.

Согласно[анализу](https://www.dragos.com/resource/2021-state-of-industrial-cybersecurity-ponemon/) компании Dragos, которая занимается вопросами кибербезопасности, средняя стоимость одного киберинцидента обходится пострадавшей стороне почти в $3 миллиона. В сумму включены расходы на устранение пришествия, и при этом они не включают упущенную выгоду.

Компания Veeam опубликовала [отчет](https://www.veeam.com/ru/wp-data-protection-trends-infographic.html) о тенденциях в области защиты данных за 2022 год, согласно которому:

* **76%** организаций подверглись хотя бы одной атаке программ-вымогателей;
* **24%**либо не подвергались атаке, либо еще не знают об этом;
* **42%** сотрудников компаний активировали фишинговые ссылки;
* **43%** инцидентов были вызваны невнимательностью со стороны администратора.

По данным опроса, в котором участвовали 1376 непредвзятых организаций, в среднем, пострадавшим удалось восстановить только 64% своих данных. Это означает, что более 1/3 данных невозможно восстановить.

**Три причины, почему вам нужен план реагирования на киберинциденты**

**1. Сотрудники будут готовы к сложным ситуациям.** Грамотно составленный план поможет вашей команде чувствовать себя уверенно. В критической ситуации каждый сотрудник будет знать, что ему делать. Это сохранит время и позволит быстро среагировать на инцидент.

**2. Сохраните репутацию, деньги и нервы**. Чем быстрее обнаружите вторжение злоумышленников, тем безболезненнее предотвратите возможные последствия. Хакеры не смогут завершить процесс взлома, а значит не потребуют выкуп за украденные данные или не навредят другим способом.

**3. Компания будет под надежной защитой надолго**. Невозможно гарантировать, что после одной атаки не последует следующей. Если у вас будет четкий план реагирования, вы не только сможете им воспользоваться, но и неоднократно улучшить, чтобы все последующие атаки все меньше воздействовали на инфраструктуру компании. Ваша команда разберет все шаги и ошибки, которые привели к атаке, что позволит действовать эффективнее в будущем.

**Как составить план реагирования на инциденты кибербезопасности**

План реагирования на киберинциденты должен включать в себя понятную схему действий и подробные пошаговые инструкции к ним. Для разработки плана привлекайте специалистов, которые будут участвовать в реагировании и устранении угроз.

План должен быть согласован и утвержден с высшим руководством организации. К разработке и процессу согласования могут быть привлечены также юридические специалисты и другие ответственные лица.

**6 этапов создания плана реагирования на киберинциденты**



**1. Подготовка**

На этом этапе строится вся архитектура вашего плана. Формируются основные компоненты процесса реагирования и выполняются следующие задачи:

**1.1.** Создать и описать стандарты политики безопасности.

**1.2.** Создать команду реагирования и определить роли сотрудников.

**1.3.** Создать и описать политику реагирования.

**1.4.** Определить план коммуникации для команды реагирования и всех заинтересованных сторон.

**1.5.** Создать журнал документирования инцидентов, в котором каждая ответственная сторона должна описать свои шаги на каждом этапе реагирования:

* **кто**отреагировал?
* **что**было затронуто?
* **где**произошел инцидент?
* **почему**было принято то или иное действие?
* **как**действие помогло и если нет, то описать возможную причину.

**1.6.** Провести обучение команды.

**1.7.** Проверить контроли доступа.

**2. Обнаружение**

На этом этапе команда должна оперативно определить, следует ли реализовывать план реагирования. Необходимо тщательно анализировать сообщения об ошибках и следить за состоянием системы.

При обнаружении подозрительной активности, предупредите всех членов команды реагирования как можно скорее. На этом этапе эффективно настроенная коммуникация критически важна.

Следует убедиться, что вся команда после обнаружения угрозы начала документировать свои действия по реагированию в журнале инцидентов (см. раздел 1.5.)

Обнаружение потенциальных угроз является обязанностью всех сотрудников компании вне зависимости, входят они в команду по реагированию на инциденты или нет. Это должно быть четко отражено в политике безопасности и регулярно повторяться на учебных мероприятиях.

Например, отдел маркетинга обнаружил странную активность на своем компьютере после открытия ссылки, которая пришла на почту. Сотрудник должен незамедлительно сообщить ответственному лицу из команды реагирования о ситуации.

**3. Сдерживание**

Цель данного этапа — оперативно предотвратить повреждение сети, даже если это задерживает основные бизнес-процессы. Сдерживание состоит из следующих шагов:

**3.1. Краткосрочное сдерживание.** Постарайтесь предотвратить дальнейшее повреждение сети и сделать это быстро. Несколько примеров краткосрочной стратегии сдерживания:

* отключение зараженных устройств из сети;
* изоляция зараженного элемента сети;
* отключение маршрутизатора в зараженных сетях.

**3.2.** Выполните судебную экспертизу, если того требует устав вашей компании.

**3.3.** Регулярно делайте резервные копии системы. Это образ диска с программным обеспечением и данные, которые сохранены на нем. Процедура необходима для того, чтобы в случае критических изменений была возможность вернуть систему в исходное рабочее состояние. Также сохраните копию зараженной системы, чтобы в дальнейшем была возможность проанализировать инцидент.

**3.4.** **Долгосрочное сдерживание.** Восстановите работоспособность бизнеса путем исправления затронутых систем, удаления backdoor, либо перенаправьте сетевой трафик для очистки систем резервного копирования.

**3.5.** Протестируйте бизнес-операции, чтобы убедиться, что они вернулись к рабочему состоянию.

**4. Ликвидация**

Первые шаги по ликвидации киберугрозы предпринимаются уже на 3 этапе (сдерживание). Они продолжаются до завершения этапа ликвидации.

Условия по устранению включают:

* Сканирование зараженных систем на наличие вредоносных программ и их следов.
* Отключение зараженных систем, чтобы защитить сеть.
* Устранение уязвимостей в исправных резервных копиях.

**5. Восстановление**

На этом этапе идет возвращение систем в их первоначальное состояние. Процесс начинается с замены сред, уже прошедших стадию ликвидации, безопасными резервными копиями.

Важно помнить, что копии могут содержать те же уязвимости, которые и привели к инциденту. Поэтому зараженные файлы необходимо устранить в первую очередь.

Перед повторным подключением всей восстановленной системы рекомендуется проверить журнал событий системы на предмет аномалий, которые укажут на продолжающееся заражение вредоносным ПО или же наличие АРТ-атак (Advanced Persistent Threat).

**6. Получение знаний**

Цель этапа — завершение документации по прошедшему циклу атаки. В отчете следует четко прописать всю последовательность действий. Описание должно быть понятно заинтересованным сторонам.

Рекомендуется собраться всем участникам инцидента не позднее двух недель после события. На встрече следует обсудить киберинцидент, его обнаружение, обработку и устранение, а также предложить варианты по возможному улучшению каждого из этапов.

**На обсуждении участники могут обсудить следующие вопросы:**

* Кто обнаружил инцидент?
* Кто сообщил об инциденте?
* Как локализовали инцидент?
* Когда был обнаружен инцидент?
* Кому было сообщено об инциденте?
* Как очищали скомпрометированные системы?
* Какие процессы задействовали для восстановления?
* В какой области команда наиболее эффективно сработала?
* Какие шаги были приняты для анализа успеха мер по ликвидации?
* Как можно улучшить действия по реагированию на возможные киберугрозы?

Подходите к составлению плана как к жизненному циклу, где каждая фаза реагирования идет в правильной последовательности. Шаги должны основываться на понимании и четкой работе.