positive technologies

Что такое недопустимые события?

Недопустимое событие — событие в результате кибератаки, делающее невозможным достижение операционных и (или) стратегических целей организации или приводящее к значительному нарушению ее основной деятельности

Для каждой организации существуют такие события, наступление которых может иметь катастрофические последствия. Кибератаки являются одной из причин, которая может привести к значительному нарушению деятельности организации и стать непреодолимым препятствием на пути к достижению ее операционных и стратегических целей.

Примеры

- остановка производства или масштабный брак продукции из-за взлома и внесения изменений в производственный процесс;
- подмена транслируемого контента с целью дестабилизации социально-политической обстановки;
- полная или частичная потеря данных из государственных фондов, реестров и ведомственных баз данных.

Понимание того, что действительно важно для организации и каких событий нельзя допустить, является одним из ключевых шагов на пути к построению результативной кибербезопасности.

Как определить недопустимые события

Чтобы определить недопустимые для организации события, рекомендуется сформировать рабочую группу, включающую:

- представителей высшего руководства организации;
- руководителей функциональных подразделений, ответственных за ключевые направления деятельности организации;
- экспертов в области информационных технологий и кибербезопасности.

Руководство

Знает, что действительно недопустимо для организации

Перечень недопустимых событий

Операционные руководители

Помогают понять, как недопустимое может быть реализовано

Сценарии реализации недопустимых событий

IT-специалисты и эксперты по ИБ

Помогают обозначить системы, в которых может быть реализовано недопустимое

Системы, взлом которых повлечет недопустимое событие

Работы по определению недопустимых событий целесообразно проводить в несколько этапов.

Формулирование недопустимых событий в масштабах всей организации с представителями высшего руководства

Топ-менеджмент обладает широким пониманием стратегических и операционных целей компании и знает, что́ действительно может нанести катастрофический ущерб деятельности всей организации. В качестве отправной точки при подготовке к обсуждению с высшим руководством рекомендуется сформировать перечень гипотез, отталкиваясь от негативных последствий кибератак, которые могут являться неприемлемыми для организации (то есть от ущерба).
Следует принимать во внимание:

- перечень типовых недопустимых событий для организаций различных направлений деятельности;
- ключевые направления деятельности;
- стратегические цели и ключевые бизнес-показатели организации.

В рамках совещания с представителями топ-менеджмента рекомендуется проранжировать предварительные гипотезы по степени важности и сформулировать, что́ является самым опасным для организации. В некоторых случаях могут быть предварительно определены пороговые значения возможного ущерба, превышение которых недопустимо.

Следует учитывать, что при обсуждении с высшим руководством может не приниматься во внимание технологическая специфика деятельности организации. Фокусом для гипотез является влияние недопустимых событий на бизнес-уровне.

Сформированный предварительный перечень недопустимых событий далее подлежит уточнению с функциональными руководителями организации.

Целевая информационная система — информационная система, в результате воздействия злоумышленника на которую может непосредственно произойти недопустимое для организации событие.

Уточнение недопустимых событий с функциональными руководителями ключевых направлений

Уточнение недопустимых событий рекомендуется осуществлять совместно с руководителями ключевых функциональных направлений организации, которые понимают специфические аспекты деятельности конкретных подразделений, операционные задачи и могут определить целевые информационные системы.

- **При моделировании сценариев реализации недопустимых событий с функциональными руководителями рекомендуется учитывать:**
  1. какие бизнес- и технологические процессы подвержены влиянию рассматриваемых недопустимых событий:
  2. какие информационные системы обеспечивают выполнение данных процессов;
  3. какие есть недостатки в процессах;
  4. какие компенсирующие меры применяются для контроля этих недостатков;
- **к каким последствиям могут привести обсуждаемые сценарии реализации недопустимых событий и каково пороговое значение возможного ущерба.**

Определение пороговых значений может осуществляться как экспертно, так и с применением количественных подходов к расчету — например, используемых при управлении

операционными рисками. Порог может быть выражен временными параметрами (например, длительность простоя системы), периодом наступления рассматриваемого события (например, остановка работы клиентских сервисов в рабочее время), финансовыми показателями (например, потеря определенной суммы, доли от оборота), объемом продукции (например, недопустимая доля брака), количеством клиентов и т. п.

Если необходимо рассчитать финансовые потери, для дополнительного обоснования порогов ущерба могут использоваться показатели финансовой и операционной отчетности. Так, имея сведения о среднем суточном обороте, можно определить, во сколько обойдется простой в работе розничных точек крупного ритейлера. Исходя из этого понимания можно определить пороговое значение допустимого ущерба, выраженного в длительности простоя того или иного количества магазинов.

Следует также принимать во внимание, что для ряда недопустимых событий пороговые значения могут быть не определены. К примеру, может быть нецелесообразно определять порог ущерба в отношении утечки конфиденциальной информации или искажения информации, публикуемой на официальных ресурсах организации.

Примеры

Недопустимое событие	Порог ущерба
Потеря VIP-клиента	Один клиент и более
Остановка производственного процесса	Более чем на 5 часов
Вывод денежных средств	Более 15% от чистой прибыли
Утечка персональных данных клиентов	Неприменимо

Проработка недопустимых событий с экспертами по ИТ и ИБ: определение технических условий реализации

Ключевая информационная система — это объект в информационной инфраструктуре, несанкционированный доступ к которому или воздействие на который необходимы нарушителю, чтобы развить атаку на целевую систему, или такая система, взлом которой существенно упростит сценарий атаки или повысит ее эффективность.

Дальнейшую проработку сценариев реализации недопустимых событий следует осуществлять с привлечением экспертов, ответственных за сопровождение и развитие ИТ и обеспечение кибербезопасности. Эксперты помогают оценить рассматриваемые сценарии и определить:

- целевые и ключевые информационные системы, при воздействии злоумышленника на которые могут быть реализованы недопустимые события;
- недостатки и уязвимости в информационных системах и IT-инфраструктуре;
- меры защиты, применяемые или планируемые к внедрению для исключения недопустимых событий;
- критерии, выполнение которых подтверждает возможность реализации недопустимого события.

Согласование перечня недопустимых событий

Результаты обследования рекомендуется оформлять в виде структурированного перечня недопустимых событий. Перечень рекомендуется расширить описанием:

- возможных негативных последствий от реализации недопустимых событий;
- возможных сценариев реализации недопустимых событий;
- целевых информационных систем;
- критериев реализации недопустимых событий.

К согласованию перечня рекомендуется привлекать участников рабочей группы. Итоговый перечень недопустимых событий рекомендуется утвердить на уровне высшего руководства организации.

Чек-лист для определения недопустимых событий

- ☐ Сформировать рабочую группу
- ☐ Подготовить перечень гипотез недопустимых событий для обсуждения с топ-менеджментом
- ☐ Сформулировать недопустимые события в масштабе организации (совместно с высшим руководством)
- ☐ Смоделировать сценарии реализации недопустимых событий — совместно с представителями бизнес-подразделений
- ☐ Декомпозировать сценарии реализации недопустимых событий на уровень IT-инфраструктуры
- ☐ Сформировать итоговый перечень недопустимых событий, учитывающий сценарии реализации и перечень целевых и ключевых систем
- ☐ Утвердить перечень недопустимых событий на уровне руководства организации