ПРАКТИЧЕСКОЕ ЗАНЯТИЕ

определения недопустимых событий,
сценариев и критериев их реализации

Оглавление

Резюме

Настоящая Методика предназначена для формирования единого подхода к построению процесса управления недопустимыми событиями в целях повышения уровня киберустойчивости и безопасности функционирования организаций.

Киберустойчивость - это способность организации обеспечить стабильное функционирование и развитие направлений своей деятельности, зависящих от информационных и цифровых технологий, путем подготовки к компьютерным атакам, реагирования на них и восстановления после них. Киберустойчивость позволяет организации адаптироваться к известным и неизвестным кризисным ситуациям, угрозам и вызовам цифрового мира для исключения (невозможности реализации) недопустимых событий.

Документ содержит рекомендации в отношении проведения следующих видов работ:

- выявление недопустимых для организации событий;
- моделирование сценариев реализации недопустимых событий;
- определение критериев реализации недопустимых событий.

Для проведения указанных работ рекомендуется сформировать рабочую группу, включающую представителей высшего руководства организации, руководителей функциональных подразделений, специалистов в области информационных технологий и кибербезопасности. Предполагается, что степень вовлечения экспертов в область проводимых работ будет варьироваться в зависимости от вида (этапа) выполняемых работ. Кроме того, возможно привлечение сторонних организаций, имеющих лицензии на осуществление деятельности по технической защите конфиденциальной информации и обладающих подтвержденным опытом проведения подобных работ.

1. Введение

Для каждой организации существуют такие события, которые могут привести к значительному нарушению её основной деятельности и стать непреодолимым препятствием на пути к достижению операционных и стратегических целей.

Недопустимое событие - событие, делающее невозможным достижение операционных и стратегических целей или приводящее к значительному нарушению основной деятельности организации в результате компьютерной атаки

Защищенность современной организации от наступления недопустимого события характеризуется устойчивостью и непрерывностью её основной деятельности. Одним из наиболее существенных факторов, способных оказать негативное влияние на организацию, являются компьютерные атаки.

Компьютерная атака - воздействие с применением технических решений на информационные системы и их пользователей с целью получения доступа к информационным ресурсам, нарушению нормальной работы или доступности систем, кражи, искажения или удаления информации

Правильно сформулированные недопустимые события должны помогать в построении системы управления кибербезопасностью, которая:

- понятна и согласована на всех уровнях управления организацией;
- позволит принимать обоснованные решения при планировании мероприятий, направленных на по повышение киберустойчивости организации;
- даст возможность наглядно оценить результаты работы по обеспечению киберустойчивости организации.

Формулирование, уточнение и проработку недопустимых событий рекомендуется осуществлять в несколько этапов:

1. Определение недопустимых для организации событий.

   Совещание с представителями высшего руководства организации: формулирование недопустимых событий в масштабах деятельности всей организации.

2. Моделирование сценариев реализации недопустимых событий

Взаимодействие с функциональными руководителями: уточнение недопустимых событий исходя из ключевых функций и целевых информационных систем организации.

3. Определение критериев реализации недопустимых событий

Проработка недопустимых событий с экспертами в области ИТ и кибербезопасности: определение технических условий и критериев реализации сценариев недопустимых событий.

2. Определение недопустимых для организации событий

Для решения задачи по формулированию недопустимых событий крайне важным является участие должностных лиц из числа высшего руководства организации, обладающих широким пониманием стратегических и операционных целей, а также направлений деятельности организации. Данные компетенции помогут сформулировать гипотезы по событиям, наступление которых может нанести катастрофический ущерб деятельности всей организации.

Для успешного проведения совещания и корректного формулирования недопустимых событий с участием высшего руководства к обсуждению могут быть привлечены ключевые эксперты организации, обладающие знаниями о функциональном устройстве и корпоративных рисках организации, а также профильные специалисты в области управления кибербезопасностью.

Вспомогательными материалами для подготовки к определению недопустимых событий являются сведения о функциональной структуре, ключевой деятельности и основных показателях эффективности организации. Кроме того, рекомендуется принимать во внимание перечень типовых недопустимых событий для организаций различных направлений деятельности, приведенный в Приложении А к настоящей Методике.

Целью проведения совещания с представителями высшего руководства является сбор и формулирование предварительного перечня недопустимых событий для дальнейшей проработки. На данном этапе основным направлением для формирования гипотез является влияние недопустимых событий на основную деятельность организации. Они могут не учитывать технологическую специфику ведения деятельности и меры контроля, которые уже применяются, но должны формировать представление о том, что может привести к катастрофическому ущербу для организации.

Результатом данного этапа является предварительный перечень недопустимых событий, который далее подлежит уточнению с

функциональными руководителями и со специалистами в области ИТ и кибербезопасности.

3. Моделирование сценариев реализации недопустимых событий

Для уточнения недопустимых событий и моделирования возможных вариантов их реализации проводятся сессии совещаний с руководителями ключевых структурных подразделений, которые обладают пониманием операционных задач, связанных с ними целевых информационных систем и перспектив развития функций в области своей деятельности.

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

В зависимости от масштаба деятельности, функциональной и организационной структуры рекомендуется сформировать список должностных лиц для планирования графика совещаний.

Целью проведения совещаний является уточнение и моделирование возможных вариантов реализации недопустимых событий с учетом специфических аспектов деятельности конкретного подразделения организации. Количество совещаний должно быть соразмерным масштабам деятельности организации и достаточным для подготовки набора вариантов реализации недопустимых событий.

Для полной проработки возможных вариантов реализации недопустимых событий рекомендуется собрать информацию о следующих основных аспектах деятельности подразделений:

- описание основных процессов и области ответственности владельцев процессов в рамках основной деятельности подразделения;
- целевые информационные системы, обеспечивающие выполнение процесса, а также системы, взаимодействующие с целевыми информационными системами организации;
- недопустимые события или сбои, которые присущи данной области;
- последствия, к которым могут привести варианты реализации недопустимых событий;
- недостатки в процессах/информационных системах;
- контрольные или защитные меры, применяющиеся или планируемые к внедрению для исключения недопустимых событий;

- иные важные организационные аспекты в области основной деятельности подразделения.

Дополнительно могут быть использованы инструменты анкетирования для получения уточнений и дополнительной информации. Типовая форма анкеты для определения недопустимых событий приведена в Приложении Б к настоящей Методике.

Результаты обследования рекомендуется оформлять в виде структурированного перечня уточненных недопустимых событий с возможными вариантами их реализации с указанием и связанных с ними:

- возможных причин наступления;
- негативных последствий;
- целевых информационных систем.

Типовая форма Перечня недопустимых событий приведена в Приложении В к настоящей Методике.

4. Определение критериев реализации недопустимых событий

Каждый вариант реализации недопустимых событий анализируется с точки зрения потенциальной возможности проведения компьютерной атаки при участии специалистов в области информационных технологий и кибербезопасности, осуществляющих эксплуатацию и поддержку целевых информационных систем, иных объектов информационной инфраструктуры и средств защиты информации. По результатам данного анализа формируются критерии, выполнение которых подтверждает возможность реализации недопустимого события.

Критерий реализации недопустимого события - крайняя точка потенциальной компьютерной атаки, подтверждающая возможность реализации варианта недопустимого события в условиях повседневной операционной деятельности организации.

Критериями реализации недопустимых событий могут являться крайние точки возможной компьютерной атаки в следующих категориях:

- получение доступа к ОС на целевой системе;
- получение доступа к прикладному ПО;
- получение доступа к целевой системе с определенными привилегиями (правами доступа);
- получение доступа в целевой сегмент сети;

- получение доступа к документам со значимой информацией;
- получение доступа к целевой системе, и удержание этого доступа в течение установленного времени;
- выполнение определенной последовательности действий в прикладном ПО;
- или комбинация из указанных выше критериев.

Целью формирования критериев реализации недопустимых событий является анализ возможности наступления недопустимых событий в условиях повседневно используемой информационно-технологической инфраструктуре организации.

В дальнейшем данные критерии могут быть использованы для подтверждения возможности реализации недопустимых событий путем имитации компьютерных атак с выполнением установленных критериев.

Если для недопустимого события существует несколько независимых друг от друга критериев его успешной верификации, то для подтверждения возможности реализации недопустимого события достаточно выполнить хотя бы один из указанных критериев.

Критерии, которые необходимо выполнить для демонстрации возможности наступления недопустимых событий, рекомендуется зафиксировать в Перечне недопустимых событий.

В случае, если выявляется дополнительный способ реализации недопустимого события, который не учтен в критериях реализации в Перечне недопустимых событий, он дополнительно проверяется и включается в итоговый Перечень недопустимых событий.

Приложение А. Перечень типовых недопустимых событий по отраслям

Приведено в отдельном документе:

Приложение А. Перечень типовых недопустимых событий по отраслям.xlsx

Приложение Б. Типовая форма Анкеты для определения недопустимых событий

Данный опросный лист предназначен для предварительного сбора информации о **недопустимых событиях**, актуальных для организации, исключение реализации которых является одной из ключевых задач результативной кибербезопасности.

> **Недопустимое событие** - событие, делающее невозможным достижение операционных и стратегических целей или приводящее к значительному нарушению основной деятельности организации в результате компьютерной атаки

Ответы на приведенные далее вопросы помогут сформировать гипотезы недопустимых событий, которые будут анализироваться в ходе дальнейших работ.

Анкета для определения недопустимых событий

Вопрос	Ответ		Комментарии
Укажите ключевые направления деятельности организации			Перечислите основные функции организации, на которых нам следует акцентировать внимание при определении недопустимых событий.
Укажите, являются ли, на ваш взгляд, актуальными и критичными для организации недопустимые события в следующих областях:	☐ Финансовые потери (незаконный вывод денежных средств)	*[дополните ответ]*	По возможности, укажите предполагаемый порог критичности ущерба для организации. ***Примеры:*** • *более XX млн.руб* • *10-15% от чистой прибыли организации* • *И т.п.*
	☐ Искажение (утрата) рабочих данных или функциональных сведений	*[дополните ответ]*	Укажите, несанкционированное изменение или полная утрата каких данных и настроек может иметь критические последствия для организации. ***Примеры:*** • *Искажение информации на официальных ресурсах* • *Уничтожение / искажение конструкторской и рабочей документации, исторических сведений* • *Уничтожение / искажение информации в базах данных операционного учета* • *Уничтожение / искажение информации*

Вопрос	Ответ		Комментарии
			в государственных реестрах и информационных системах • *И т.п.*
	☐ Сбои или остановка операционных или технологических процессов из-за недоступности поддерживающих информационных систем	*[дополните ответ]*	Укажите, нарушение каких операционных и (или) технологических процессов может иметь критические последствия для организации. ***Примеры:*** • *Простои в работе корпоративной инфраструктуры* • *Остановка производства или масштабный брак продукции по причине взлома и внесения изменений в производственный процесс;* • *Перебои в работе или недоступность клиентских сервисов;* • *И т.п.*
	☐ Утечка конфиденциальных сведений	*[дополните ответ]*	Укажите, утечка каких категорий сведений может привести к критичным последствиям для организации. ***Примеры**:* • *Персональные данные (укажите категории субъектов – например, работники, клиенты, пользователи и т.п.)* • *НИР, конструкторская документация, объекты интеллектуальной собственности* • *Стратегии, планы развития, маркетинговые программы* • *Исходный код разрабатываемого ПО* • *Сведения о партнерских соглашениях и контрактах* • *И т.п.*

Вопрос	Ответ		Комментарии
	☐ Другое	*[дополните ответ]*	Укажите иные события, которые являются недопустимыми для организации и могут быть реализованы в результате действий киберзлоумышленников
Какие информационные системы, на ваш взгляд, являются наиболее важными для работы организации? (компрометация / взлом которых может привести к реализации недопустимых событий)			Укажите наименование информационных систем и краткое назначение. ***Примеры:*** • *1С Предприятие – оперативное управление организацией* • *СЭД / ЭДО – электронный документооборот* • *CRM – ведение данных по клиентам* • *И т.п.*

Приложение В. Типовая форма Перечня недопустимых событий и критериев их реализации

Утвержденный в _*Наименование организации*_ перечень недопустимых событий, возможные варианты их реализации, а также критерии их реализации приведены ниже в таблице.

Перечень недопустимых событий и критериев их реализации

Наименование недопустимого события	Целевые информационные системы	Вариант реализации недопустимого события	Критерий реализации недопустимого события
Кража денежных средств	1С: Предприятие Система банк-клиент	Оформить заявку на проведение оплаты контрагенту по ложным реквизитам в системе 1С: Предприятие, а затем для вывода денежных средств с расчетного счета компании создать соответствующее платежное поручение в системе банк-клиент и направить его в банк	Получение доступа к системе 1С: Предприятие (прикладное ПО) с правами на создание/редактирование заявок и данных контрагентов, а также демонстрация доступа к системе банк-клиент с правами на отправку платежного поручения в банк