МЕТОДИЧЕСКИЙ ДОКУМЕНТ

Методические рекомендации по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности организаций при выполнении показателей оперативного рейтинга эффективности и результативности ответственных за цифровую трансформацию

Термины и определения

1. **Антропогенные причины недопустимого события** — лица (группа лиц), осуществляющие реализацию рисков информационной безопасности путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей.

2. **Вектор компьютерной атаки** — последовательность действий злоумышленника в рамках компьютерной атаки, произведенная им в отношении определенного набора ресурсов автоматизированной информационной системы и позволившая ему получить определенный уровень доступа (привилегий) на этих ресурсах.

3. **Компьютерная атака** — целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

4. **Критерий реализации недопустимого события** — факт, технологическое условие или граничные значения длительности, масштаба или сценария воздействия (либо промежуточного результата), отражающий условие и возможность реализации варианта недопустимого события в повседневной операционной деятельности организации (например, факт получения максимальных привилегий в прикладном программном обеспечении на целевой информационной системе в результате реализации вектора компьютерной атаки). Метрика, которая позволяет однозначно подтвердить и зафиксировать наступление недопустимого события в отличие от инцидента информационной безопасности.

5. **Недопустимое событие** — отдельное событие, цепочка или сочетание событий, вызванных компьтерной атакой, в результате которых прерывается операционная деятельность организации.

6. **Непрерывность операционной деятельности организации** — способность организации обеспечить стабильное функционирование и развитие своей деятельности при использовании информационных технологий.

7. **Последствия реализации недопустимых событий** — все виды ущерба и убытков организации, региона, отрасли, государства, вызванные реализацией рисков информационной безопасности вследствие компьютерной атаки на объекты информационной инфраструктуры, приводящие к прерыванию операционной деятельности организации.

8. **Целевая информационная система** — информационная система, в результате воздействия злоумышленника на которую может наступить недопустимое событие.

9. **Целевой сегмент сети** — сегмент сети организации, в котором расположена целевая информационная система.

□□. Общие положения□

□

Настоящие Методические рекомендации по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности организаций при выполнении показателей оперативного рейтинга эффективности и результативности ответственных за цифровую трансформацию (далее – Методические рекомендации) разработаны в соответствии с пунктами 1 и 5.2.22 постановления Правительства Российской Федерации от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» в целях оказания операторам информационных систем (за исключением информационных систем критически важных объектов и объектов критической информационной инфраструктуры) методологической помощи в формировании перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий.

Для достижения указанной цели наравне с настоящими методическими рекомендациями организации рекомендуется использовать положения национального стандарта Российской Федерации ГОСТ Р 53647.1-2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство», национального стандарта Российской Федерации ГОСТ Р 53647.2-2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования», национального стандарта Российской Федерации ГОСТ Р 53647.3-2015 «Менеджмент непрерывности бизнеса. Часть 3. Руководство по обеспечению соответствия требованиям ГОСТ Р ИСО 22301», национального стандарта Российской Федерации ГОСТ Р 53647.4-2011/ISO/PAS 22399:2007 «Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности» и национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска».

Выполнение рекомендаций для целей обеспечения непрерывности операционной деятельности при использовании информационных технологий

рекомендуется осуществлять с учетом иных положений технического регулирования Российской Федерации (национальные стандарты, рекомендации в области стандартизации).

Сфера действия Методических рекомендаций

Методические рекомендации рекомендованы к использованию операторами информационных систем (за исключением информационных систем критически важных объектов и объектов критической информационной инфраструктуры).

Методические рекомендации охватывают деятельность по формированию верифицированного перечня недопустимых событий, не включают ни подходы к обоснованию выбора организационных и технических мер по защите информации и противодействию угрозам безопасности информации, ни рекомендации по выработке мер защиты от угроз безопасности информации и повышению уровня информационной безопасности организаций. Конечный перечень защитных мер, а также алгоритм их выбора определяется организацией самостоятельно либо с привлечением организаций, аккредитованных ФСБ России на выполнение работ по обнаружению, предупреждению и ликвидации последствий компьютерных атак (либо имеющих соответствующее соглашение с Национальным координационным центром по компьютерным инцидентам), руководствуясь действующими нормативными правовыми актами в области защиты информации.

Взаимодействие с уполномоченными федеральными органами исполнительной власти по формированию и актуализации отраслевых, региональных перечней недопустимых событий не покрывается положениями Методики.

Организация работ

Для обеспечения надежности операционной деятельности при использовании информационных технологий организации рекомендуется регламентировать технологические и бизнес-процессы.

Для каждого процесса рекомендуется определить и соблюдать показатели надежности операционной деятельности, например, время простоя или нарушения режима работы каждого процесса.

Для обеспечения надежности операционной деятельности при использовании информационных технологий организации рекомендуется сформировать перечень недопустимых событий.

Для снижения влияния возможных субъективных факторов при формировании перечня недопустимых событий рекомендуется сформировать постоянно действующую Рабочую группу.

Руководство Рабочей группой рекомендуется возложить на заместителя руководителя организации, в чью зону ответственности входит управление рисками и обеспечение непрерывности деятельности организации.

Состав и задачи Рабочей группы закрепить внутренним распорядительным документом организации.

В состав участников Рабочей группы рекомендуется включить руководителей подразделений ответственных за:

- управление рисками и обеспечение непрерывности деятельности;
- сопровождение и развитие информационных технологий;
- обеспечение информационной безопасности.

Деятельность Рабочей группы может быть организована в виде стратегических сессий, совещаний, круглых столов, мозговых штурмов, к участию в которых на разных этапах привлекаются высшее руководство, ключевые эксперты организации, обладающие знаниями о функциональном устройстве и корпоративных рисках организации, а также профильные специалисты в области информатизации и управления информационной безопасностью. Формирование списка руководителей и экспертов, привлекаемых к работе, проводится Рабочей группой на основе информации об организационной структуре организации, паспортов и карт бизнес-процессов, а также результатах проведения оценки влияния чрезвычайных ситуаций на бизнес и оценки рисков. Список должен включать руководителей по ключевым критичным областям/бизнес-процессам организации. Допускается привлечение к отдельным этапам работ представителей экспертных организаций, имеющих лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации и (или) аккредитованных ФСБ России на выполнение работ по обнаружению, предупреждению и ликвидации последствий компьютерных атак (либо имеющих соответствующее соглашение с Национальным координационным центром по компьютерным инцидентам), а также представителей разработчиков программного обеспечения и поставщиков информационно-телекоммуникационного оборудования.

Вспомогательными материалами для подготовки к определению недопустимых событий, которые рекомендуется использовать участникам Рабочей группы, могут являться сведения о (включая, но не ограничиваясь):

- основных отслеживаемых показателях эффективности организации;
- результатах оценки рисков (ущерба);
- результатах стратегического планирования, включая результаты анализа слабых и сильных сторон, возможностей и угроз, и анализа политических, экономических, социальных и технологических аспектов внешней среды;
- системе менеджмента качества;
- элементах бизнес- и технологических процессов организации;
- критичных информационных системах;

- статистике инцидентов информационной безопасности;
- отраслевых и общегосударственных перечнях недопустимых событий.

Этапы работ

Формирование перечня последствий реализации недопустимых событий и их ранжирование по степени значимости для деятельности организации.

При формировании перечня последствий реализации недопустимых событий рекомендуется отталкиваться от видов ущерба, которые являются неприемлемыми и (или) нежелательными для организации:

- угрозы жизни и здоровью;
- техногенные или экологические катастрофы;
- угрозы технических происшествий (пожары, затопления, выход из строя техники, программного обеспечения, отключение электроэнергии, связи и т.п.);
- прекращение функционирования организации;
- недостижение стратегических целей компании и ключевых бизнес-показателей;
- угроза репутации компании и (или) её руководителей и публичных представителей;
- нарушение законных прав;
- снижение маржинальности, доли рынка;
- недопустимое снижение качества продукции;
- и др.

При определении последствий реализации недопустимого события должны рассматриваться антропогенные причины их возникновения, а также отбираться последствия, характерные для отрасли и региона.

Для каждого идентифицированного последствия реализации недопустимого события должна быть сформулирована метрика измерения и оценка критичности, выше которого ущерб считается неприемлемым.

В дальнейшую работу и детализацию описания отбираются наиболее критичные последствия, те, для которых оценка критичности ущерба потенциально может достигать неприемлемого значения.

Определение бизнес- и технологических процессов и связанных с ними информационных систем.

На данном этапе критичные последствия реализации рисков связываются с бизнес- и технологическими процессами, в которых они могут возникнуть.

При описании связки «последствие – процесс – информационная система» необходимо принимать во внимание, что одинаковое последствие может возникать

различными способами в различных процессах и реализовываться в одном или нескольких информационных ресурсах.

Перечень процессов необходимо дополнить возможными недостатками их функционирования, а среди перечня информационных ресурсов отметить целевые информационные системы и применяемые или планируемые к внедрению контрольные и защитные меры информационной безопасности.

Формирование гипотетических сценариев реализации недопустимых событий

В рамках данного этапа на основе доступной информации, а также с привлечением представителей экспертного сообщества в области информационной безопасности и разработчиков программного обеспечения, Рабочей группой определяются действия, направленные на информационные системы, и формируются сценарии, в ходе которых реализуются недопустимые события, приводящие к критичным последствиям. Сценарии должны предусматривать имитацию действий злоумышленников для достижения целевых информационных систем. Гипотетические сценарии должны быть реалистичными и применимыми к информационным системам организации.

На основе списка сценариев Рабочая группа формирует проект перечня недопустимых событий (далее - Перечень). Для этого можно использовать методы выявления корневых причин и группировки по однородным признакам.

Определение критериев реализации недопустимых событий.

Рабочей группе рекомендуется оценить каждый сценарий реализации недопустимых событий с точки зрения потенциальной возможности проведения компьютерной атаки при участии специалистов в области информационных технологий и информационной безопасности, осуществляющих эксплуатацию и поддержку целевых информационных систем, иных объектов информационной инфраструктуры и средств защиты информации. По результатам данного анализа для каждой целевой системы формируются критерии, выполнение которых подтверждает возможность реализации недопустимых событий и, как следствие, возникновения критичных последствий реализации недопустимых событий.

На следующем этапе критерии используются в качестве метрики подтверждения возможности реализации недопустимых событий, инициированных злоумышленниками путем моделирования и имитации компьютерных атак.

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

Критериями реализации недопустимых событий могут являться результаты реализации злоумышленником вектора компьютерной атаки в следующих категориях при одновременном соблюдении условий, характера и (или) периода и длительности воздействия:

- получение доступа к операционной системе на целевой системе;
- получение доступа к прикладному программному обеспечению;
- 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 программном обеспечении;
- комбинация из указанных выше критериев;
- иные категории, указанные в Банке данных угроз безопасности информации.

Критерии, свидетельствующие о возможности наступления недопустимых событий, рекомендуется зафиксировать в Перечне. Типовая форма Перечня приведена в Приложении к настоящей Методике.

Моделирование гипотетических сценариев реализации недопустимых событий.

Для получения объективной картины реализуемости сценариев рекомендуется проводить практическую имитацию компьютерных атак на системы организации в условиях, приближенных к реальным. На этом этапе рекомендовано привлечение представителей экспертных организаций, аккредитованных ФСБ России на выполнение работ по обнаружению, предупреждению и ликвидации последствий компьютерных атак (либо имеющих соответствующее соглашение с Национальным координационным центром по компьютерным инцидентам), а также служб обеспечения информационной безопасности организации.

При практической имитации могут отрабатываться разные варианты участия служб обеспечения информационной безопасности организаций: с использованием систем мониторинга в режиме наблюдения и не противодействуя атакам, либо активно противодействуя и блокируя действия злоумышленников. В результате формируется оценка покрытия и эффективности мониторинговых систем, определяются слепые зоны, а недопустимые события получают дополнительную оценку вероятности реализации.

В случае практической имитации компьютерных атак подтверждением гипотезы о реализации сценария недопустимого события является достижение критерия реализации недопустимых событий. При этом, в ходе тестирования могут реализоваться не предусмотренные сценарии и варианты недопустимых событий. В таком случае проект перечня недопустимых событий дополняется, проводится оценка последствий реализации рисков и определяется критерий реализации недопустимых событий.

Формирование перечня недопустимых событий.

По итогам проведения практической имитации компьютерных атак Рабочая группа формирует итоговый перечень недопустимых событий с указанием критериев их реализации и соответствующих целевых информационных систем. Опционально указываются перечень уязвимостей информационных систем, дается оценка достаточности технологических и организационных мер защиты, квалификации персонала и в целом готовности организации к отражению угроз безопасности информации.

Перечень недопустимых событий рекомендуется утвердить руководителем организации или коллегиальным органом управления или заместителем руководителя организации, в чью зону ответственности входит управление рисками и обеспечение непрерывности деятельности.

Утвержденный верифицированный перечень недопустимых событий, а также дополнительную информацию, собранную Рабочей группой в ходе определения этого перечня, рекомендуется использовать при разработке мер по предотвращению наступления недопустимых событий, а также повышению защищенности и обеспечению информационной безопасности организации.

Организациям рекомендуется разработать план восстановления непрерывности операционной деятельности при использовании информационных технологий и ликвидации последствий компьютерных атак.

Организациям рекомендуется актуализировать перечень недопустимых событий организации по мере:

- появления новых или исключения действующих бизнес- или технологических процессов организации;
- изменения профиля риска организации в зависимости от влияния внешних факторов (экономических, политических, регуляторных и т.п.);
- изменения информационно-технологического ландшафта организации;
- появления достоверных сведений о новых методах кибератак, которые могут быть применены для реализации недопустимых событий.

Не реже одного раза в год организациям рекомендуется проводить верификацию недопустимых событий (моделирование гипотетических сценариев реализации недопустимых событий) и при необходимости актуализацию перечня недопустимых событий.

Организациям рекомендуется проводить тренировки сотрудников по отработке навыков по обеспечению непрерывности деятельности и по результатам проведения учений, при необходимости, корректировать значения показателей надежности операционной деятельности при использовании информационных технологий.

Приложение
к Методическим рекомендациям

Типовая форма перечня недопустимых событий организации

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 недопустимых событий	Пороговое значение	Целевые информационные системы	Сценарии реализации недопустимых событий	Критерий реализации
Кража денежных средств	Свыше 500 млн. руб.	Учетная система Система банк-клиент	Оформить заявку на проведение оплаты контрагенту по ложным реквизитам в Учетной системе, 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 Учетной системе (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