Методика проведения Кибериспытания

V1.23

Открытая лицензия

Продолжая ознакомление с текстом этого документа, вы подтверждаете и соглашаетесь с нижеследующим.

Настоящая Методика проведения кибериспытания (далее – Методика) является объектом авторских прав. Исключительные права на результаты интеллектуальной деятельности и средства индивидуализации, содержащиеся в Методике, принадлежат правообладателю – АО «УК Большая история» (ИНН 9722013510). Исключительные права защищаются по российскому законодательству и нормам международного права.

Если иное не предусмотрено соглашением с правообладателем, ваши права по использованию Методики ограничиваются правом на ознакомление с текстом в личных целях под контролем правообладателя. Такое право может быть прекращено в любое время по волеизъявлению правообладателя.

В случае получения соответствующего уведомления правообладателя, вы обязуетесь в течение 2 (двух) рабочих дней с момента направления такого уведомления вернуть правообладателю документы, содержащие Методику, и иные документы, созданные с помощью Методики, на материальном или электронном носителе, а также уничтожить и удалить все сведения и их копии со своих электронных носителей информации и ЭВМ, включая резервные копии, созданные на внешних (виртуальных) серверах, и предоставить об этом письменное подтверждение по требованию правообладателя.

Запрещено, в том числе, несанкционированное копирование (воспроизведение), обнародование, распространение и использование в любой иной форме в коммерческих, некоммерческих или личных целях Методики или любых её частей без предварительного согласования с правообладателем.

Запрещается присваивать Методику, или материальные носители, содержащие Методику, в том числе уничтожать или изменять сведения о правообладателе, публиковать полученные сведения о Методике и тексты Методики в качестве собственных, включать их в состав сведений, составляющих собственную коммерческую тайну и (или) ноу-хау, за исключением случаев, разрешенных правообладателем.

В случаях, разрешенных правообладателем или применимым законодательством, использование осуществляется с обязательным указанием правообладателя – АО «УК Большая история» и сайта cyberfy.ru как источника заимствования

Создание нового результата интеллектуальной деятельности на основании Методики и его последующее использование требует согласования с правообладателем.

Методика может быть использована на условиях возмездной лицензии. Сроки и территория использования Методики согласуются с правообладателем.
По всем вопросам использования Методики следует обращаться к АО «УК Большая история» по электронной почте info@cyberfy.ru. В теме письма необходимо указать, что сообщение относится к «Методике проведения кибериспытания».

Методика предоставляется правообладателем в состоянии «как есть», без каких-либо гарантийных обязательств правообладателя или какой-либо обязанности по устранению недостатков Методики, технической поддержке и усовершенствованию.

Правообладатель не несёт ответственности за коммерческую пригодность Методики, не гарантирует соответствие Методики специальным требованиям клиентов и/или лицензиатов или возможность адаптации в соответствии с

предпочтениями клиентов и/или лицензиатов, а также не гарантирует, что Методика полностью свободна от дефектов и ошибок, и должна функционировать бесперебойно и в обязательном порядке.

Любые заинтересованные лица в случае выявления нарушения интеллектуальных прав и иных противоправных действий, обязуются прежде всего сообщить Правообладателю о подобных нарушениях, обратившись с электронным сообщением по адресу info@cyberfy.ru. В случае получения в письменной форме заявления лица о нарушении его интеллектуальных прав с указанием раздела Методики, где размещен такой материал, правообладатель своевременно принимает необходимые и достаточные меры для прекращения нарушения интеллектуальных прав.

Оглавление

1. Термины и определения

Bug Bounty (Баг Баунти) — принятый на рынке анализа защищенности способ оказания услуг поиска уязвимостей, который заключается в предложении Заказчику получить за вознаграждение результат услуги по обнаружению исследователем уязвимости в инфраструктуре, продукте или технологии Заказчика.

Аккредитованный посредник – юридическое лицо, осуществляющее сопровождение Заказчика при подготовке и проведении Кибериспытания.

Заказчик — юридическое лицо, в интересах которого проводится Кибериспытание.

Заключение – составленный Сертификационной организацией документ по итогам анализа Отчёта Площадки, содержащий выводы об отсутствии достижения целей Кибериспытания или их достижения.

Значимое событие – результат действий Исследователя, производимых им в ходе Кибериспытания, который может существенно повлиять на ход Кибериспытания или деятельность Заказчика.

Информация от Исследователей – совокупность всех предпринятых и задокументированных действий Исследователей с целью проверки возможности реализации Недопустимых событий.

Исследователь — специалист или команда специалистов в области информационной безопасности, привлекаемые Площадкой, принимающие участие в Кибериспытании с целью оценки защищенности инфраструктуры, продукта или технологии Заказчика и возможности реализации недопустимых событий.

Критерий реализации недопустимого события организации (далее — критерий НС) — факт, технологическое условие или граничные значения длительности, масштаба или сценария воздействия (либо промежуточного результата), отражающие условие и возможность реализации варианта недопустимого события в повседневной деятельности организации. В отличие от инцидента информационной безопасности, критерий НС позволяет однозначно подтвердить и зафиксировать наступление недопустимого события.

Кибериспытание (далее – КИ) — анализ защищённости инфраструктуры, продукта или технологии Заказчика с целью оценки уровня защищенности и возможности реализации Недопустимых событий, выявленных путём испытания инфраструктуры, продукта или технологии Заказчика силами независимых Исследователей или группы Исследователей, привлекаемых Площадкой, способами и приёмами, допущенными в соответствии с требованиями данной Методики и Условиями проведения кибериспытания.

Кибериспытание-экспресс (далее – КИ-экспресс) — формат проведения Кибериспытания, отличающийся по условиям проведения кибериспытания, ограниченный по перечню доступных НС и сроку проведения КИ, количеству привлекаемых экспертов, величине вознаграждения и формату итоговой отчетности.

Недопустимое событие(я) (далее — НС) — одно или несколько событий, которые могут происходить в результате несанкционированных действий третьих лиц, направленных на получение конфиденциальной информации, нарушающих или создающих угрозу нарушения целостности и доступности инфраструктуры, продукта или технологии, и (или) режима эксплуатации, которые могут приводить к значимым потерям (финансовым, репутационным, регуляторным и т.д.), способным оказать критическое влияние на деятельность компании, ее руководство, клиентов и партнеров.

Организованная площадка (далее — Площадка) — юридическое лицо, обладающее необходимой инфраструктурой привлечения Исследователей для проведения Кибериспытания в соответствии с настоящей Методикой и имеющее аккредитацию от АО «Кибериспытание» на предоставление услуг по проведению Кибериспытания Заказчикам с применением настоящей Методики.

Отчёт по кибериспытанию – составленный Сертификационной организацией документ на основе отчета Площадки, являющийся результатом оказания услуг Кибериспытания, содержащий результаты Кибериспытания инфраструктуры, продукта или технологии Заказчика, выводы о возможности или невозможности реализации недопустимых событий по согласованному реестру.

Отчёт Площадки – составленный Площадкой документ на базе Информации от Исследователей, содержащий данные о ходе и результатах

Кибериспытания, подготовленный по требованиям Методики и подлежащей экспертизе со стороны Сертификационной организации.**Платформа** – программное и (или) программно-аппаратное обеспечение Площадки, с помощью которого Площадка привлекает Исследователей и публикует условия Кибериспытания.

Период активного проведения Кибериспытания — время, в течение которого Исследователи ведут активные действия по проведению Кибериспытания. Из периода активного проведения Кибериспытания исключаются периоды, в течение которых услуги фактически не оказывались (по причине их приостановки, либо иным причинам).

Реестр недопустимых событий (далее — реестр НС) — список всех Недопустимых событий Заказчика, подготовленных на основе Методики определения недопустимых событий (доступна по ссылке).

Сертификационная организация — АО «Кибериспытание» юридическое лицо, организующее аккредитацию компании Площадки, как лица, оказывающего услуги по привлечению Исследователей для проведения Кибериспытания в соответствии с Методикой аккредитации на основании договора, заключаемого с Площадкой, а также проверяющее соответствие Условий проведения кибериспытания, процесса Кибериспытания и Отчёта Площадки Методике кибериспытания, и готовящее Отчёт о кибериспытании на его основе на основании отдельного договора, заключаемого с Заказчиком.

Сертификат об успешном прохождении Кибериспытания - документ, составленный Сертификационной организацией по итогам анализа отчёта Площадки, содержащий выводы о достижении целей Кибериспытания, описанных в Условиях проведения кибериспытания, с определённым в нём сроком и требованиями.

Скоринговый балл Кибериспытания – цифровое значение результатов Кибериспытания в пределах 0-100, которое показывает полноту исследования и прозрачность условий. Чем выше балл, тем более приближено исследование к реальному уровню возможности реализации киберугроз в контексте инфраструктуры, продукта или технологии Заказчика, и тем больше вероятность того, что исследователи проверили все возможные методы и

способы реализации НС. Балл может использоваться для сравнения исторической динамики Кибериспытания организации и сравнения с другими организациями.

Условия проведения КИ (далее — УП) — документ, разработанный Заказчиком и утверждённый Экспертным советом, определяющий состав услуг Кибериспытания, оказываемых Площадкой, а также порядок их оказания в инфраструктуре Заказчика или в отношении продукта, или технологии Заказчика.

Экспертный совет (далее — ЭС) — группа экспертов, контролирующая соответствие проведения Площадкой Кибериспытания Методике кибериспытания, утверждающая Условия проведения кибериспытания и Отчёт о кибериспытаниях на основании договора с Заказчиком, являющаяся структурным подразделением Сертификационной организации и не являющаяся самостоятельным юридическим лицом.

2. Общие положения

Методика разработана с целью стандартизировать подход к оценке эффективности защиты инфраструктуры, продукта или технологии Заказчика от противоправных действий злоумышленников.

В документе описан процесс подготовки, проведения и оценки результатов Кибериспытания.

Цель Кибериспытания — получить наиболее точную и достоверную оценку степени защищенности инфраструктуры, продукта или технологии Заказчика при реализации Недопустимых событий.
Методика предполагает, что перед проведением Кибериспытания Заказчик выполнил весь комплекс мер, необходимый для защиты от реализации Недопустимых событий.

Комплекс подготовки включает три этапа:

- определение целей, то есть формирование Реестра недопустимых событий;
- построение защиты на основе определенных целей и Реестра недопустимых событий;
- внутренняя проверка эффективности защиты от реализации Недопустимых событий и механизмов оперативного реагирования на угрозы информационной безопасности.

3. Сфера действия

Методика рекомендована к применению государственными органами, организациями, в том числе субъектами критической информационной инфраструктуры Российской Федерации.

Методика охватывает деятельность предприятий, организаций, органов власти по проведению Кибериспытания. Методика включает описание жизненного цикла Кибериспытания.

Методика не содержит рекомендаций Исследователям о том, какие конкретные действия необходимо выполнить, чтобы достичь реализации Недопустимого события. Методика не содержит описания организационных и технических мер для защиты информации, а также рекомендаций по их выбору.
Методика не применима на объектах информатизации, предназначенных для обработки сведений, составляющих государственную тайну.

4. Порядок проведения

В настоящем разделе описан жизненный цикл проведения Кибериспытания — от формирования заявки до подведения итогов. Диаграмма процесса представлена на Диаграмме 1.

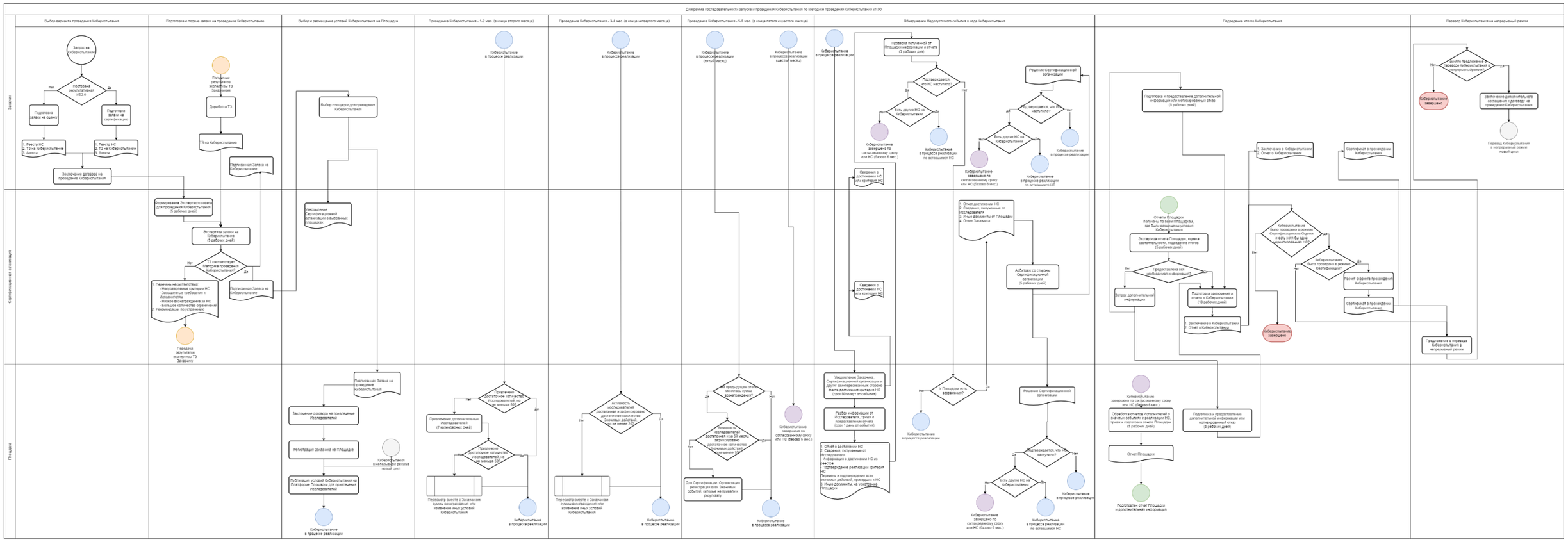

Диаграмма 1. Диаграмма жизненного цикла Кибериспытания по Методике проведения Кибериспытания v1.23.

4.1 Решение о проведении

Методика определяет вознаграждение Исследователям за реализацию НС со стороны Заказчика.

Решение о проведении Кибериспытания принимается Заказчиком после реализации следующих ключевых этапов:

1. Определены цели информационной безопасности, которые должны быть реализованы для успешного протекания критических процессов Заказчика. Сформулированы Недопустимые события Заказчика, которые могут нарушить критические процессы и приостановить деятельность Заказчика.
2. Рализован комплекс организационных, правовых и технологических мероприятий, которые обеспечат защиту от возможной реализации Недопустимых событий.
3. Пройдены внутренние испытания эффективности защиты от реализации Недопустимых событий.

Однако это не ограничивает возможность выхода Заказчика на Кибериспытание без реализации вышеперечисленных этапов.

При проведении Кибериспытания в формате Кибериспытание-экспресс, используется ограниченный предопределенный перечень недопустимых событий.

4.2 Подготовка к проведению

Обязательная подготовка к проведению Кибериспытания состоит из следующих этапов:

1. Подготовка реестра Недопустимых событий, возможность реализации которых будет проверяться во время Кибериспытания (см. Раздел 5).
2. Заполнение стандартной анкеты о текущем состоянии функции информационной безопасности в организации – «Анкета о текущем состоянии функции ИБ») (далее - «Анкета») (шаблон и пример заполнения предоставляется по запросу Заказчика).

3. Разработка Условий проведения Кибериспытания в соответствии с настоящей Методикой (шаблон и пример заполнения предоставляется по запросу Заказчика).

Указанные этапы Заказчик может выполнить самостоятельно, руководствуясь Методикой, или с привлечением третьих лиц с необходимыми компетенциями. Если Заказчик не выполняет обязательную подготовку, то провести Кибериспытание невозможно.

При проведении Кибериспытания в формате Кибериспытание-экспресс, может использоваться иной алгоритм подготовки и создаваться иной набор артефактов. Также, в данном формате может использоваться упрощенный формат написания УП, отличный от приведенного в рамках настоящего документа.

4.3 Подача заявки

После формирования Реестра недопустимых событий, Анкеты и Условий проведения кибериспытания (далее — Артефакты), Заказчик подает заявку на проведение Кибериспытания.

Для рассмотрения заявки и начала процесса Кибериспытания, Сертификационная организация должна рассмотреть и утвердить Условия проведения кибериспытания Заказчика.

Для этого Заказчик и Сертификационная организация подписывают договор на экспертное сопровождение. Форму договора Сертификационная организация предоставляет по запросу Заказчика.

После подписания договора на экспертное сопровождение, Заказчик передает Артефакты Сертификационной организации тем способом, который обозначен в договоре.

При проведении Кибериспытания в формате Кибериспытание-экспресс, подача заявки может проводиться в упрощенном формате. Конкретный порядок действий Сертификационная организация предоставляет по запросу Заказчика и публикует на своем ресурсе http://cyberfy.ru/.

4.4 Рассмотрение заявки

После получения требуемых Артефактов, Экспертный совет в течение 5 (пяти) рабочих дней рассматривает, насколько Условия проведения кибериспытания соответствуют настоящей Методике. В результате Экспертный совет выполняет одно из действий:

1. Если Условия проведения кибериспытания соответствуют Методике, Сертификационная организация отправляет Заказчику заключение, позволяющее запустить Кибериспытание.
2. Если Условия проведения кибериспытания не соответствуют Методике, Сертификационная организация отправляет Заказчику список несоответствий и рекомендации, которые необходимо учесть перед повторной подачей заявки.

При проведении Кибериспытания в формате Кибериспытание-экспресс, рассмотрение заявки происходит в упрощенном режиме, при этом участие Экспертного совета является ограниченным и опциональным.

4.5 Выбор площадки проведения

Заказчик выбирает конкретную Площадку для привлечения Исследователей для проведения Кибериспытания из перечня аккредитованных Сертификационной организацией Площадок. Заказчик может запустить Кибериспытания одновременно у нескольких аккредитованных Сертификационной организацией Площадок. Если у Заказчика есть техническая возможность, в качестве Площадки может выступать Платформа Заказчика. Более подробно требования к Площадке описаны в разделе Требования к площадке.

4.6 Запуск

При запуске Кибериспытания Заказчик предоставляет площадке УП на проведение Кибериспытания и положительное заключение Сертификационной организации.

Заказчик имеет право запустить Кибериспытание одновременно по всем Недопустимым событиям, по отдельному списку, либо одному Недопустимому событию.

Датой начала проведения Кибериспытания по Недопустимому событию(ям) считается дата его (их) публикации на Платформе Площадки. Если Кибериспытание запускается у нескольких Площадках, то датой начала считается дата размещения на Платформе первой из Площадок.

При проведении Кибериспытания в формате Кибериспытание-экспресс, документы, необходимые для старта Кибериспытания, передаются Площадке аккредитованным посредником или Сертификационной организацией.

4.7. Сроки проведения Кибериспытания

Минимальный срок Кибериспытания от начала проведения Кибериспытания до момента формирования Отчета по Кибериспытанию и передаче его Заказчику составляет 6 (шесть) календарных месяцев, то есть 183 (сто восемьдесят три) дня Активного периода Кибериспытания, при условии заключения договора на Кибериспытание по конкретному Недопустимому событию с Сертификационной организацией впервые.

При проведении Кибериспытания в формате Кибериспытание-экспресс срок от начала проведения КИ-экспресс до момента формирования Отчета по КИ-экспресс и передаче его Заказчику составляет 3 (три) календарных месяца, то есть 91 (девяносто один) календарный день. По окончанию срока КИ-экспресс, Заказчик получает отчет, содержащий сокращенную информацию о результатах.

4.8 Подведение итогов

По истечению минимального срока Кибериспытания по каждому Недопустимому событию, Площадка готовит Отчет Площадки и передает его в Сертификационную организацию в срок не более 5 (пяти) рабочих дней. Возможность передачи Отчётов Площадки в Сертификационную организацию прописывается в договоре между Заказчиком и Площадкой.
На основании предоставленного Отчёта Площадки, Экспертный совет подводит итоги проведенного Кибериспытания по конкретным Недопустимым событиям, готовит Заключение или готовит Отчёт по Кибериспытанию.

Экспертный совет может запросить дополнительную информацию у Площадки/Заказчика, которая необходима для проведения оценки. В случае такого запроса, Заказчик/Площадка должны предоставить запрошенную информацию в течение 5 (пяти) рабочих дней в письменной форме. В случае отсутствия возможности предоставить такую информацию, Заказчик/Площадка должны предоставить письменный мотивированный отказ.

Экспертный совет в течение 10 (десяти) рабочих дней с момента получения Отчёта Площадки и всей необходимой информации, должен подготовить Заключение или сформировать Отчет по Кибериспытанию. В эти сроки Сертификационная организация рассчитывает скоринговый балл, который принимает значение от 0 до 100, и позволяет дать сравнительную оценку проведенного Кибериспытания. Оценка может использоваться для сравнения с другими завершенными Кибериспытаниями.

Расчет скорингового балла Кибериспытания

Расчет балла производится на базе скоринговой модели, разработанной АО «Кибериспытание». Фактически она связывает оценки и параметры Кибериспытания с уровнем защищенности организации и полнотой оценки этой защищенности в конкретных условиях через систему скоринговых баллов.

Результаты расчета нормируются и приводятся к шкале, которая может принимать значение от 0 до 100 баллов – на выходе модели формируется интегрированный показатель – скоринговый балл.

Выпуск сертификата

В случае, если Экспертный совет признает Кибериспытание состоявшимся и успешным, Сертификационная организация выпускает Сертификат об успешном прохождении Кибериспытания по НС/списку НС Заказчика.

Сертификат об успешном прохождении Кибериспытания направляются Заказчику и Площадке в течение 10 (десяти) рабочих дней одновременно с Отчётом по кибериспытанию.

После выдачи сертификат действует в течение всего срока пока Заказчик находится на Кибериспытании в постоянном режиме.

Если Экспертный совет не признает Кибериспытание успешным полностью или в части, Сертификационная организация выпускает Заключение по НС/списку НС Заказчика, в котором содержится подробное разъяснение причин признания Кибериспытания несостоявшимся полностью или в части.

4.9 Постоянный режим

Методика закрепляет постоянный режим Кибериспытания после его первого состоявшегося и успешного результата, то есть после получения Сертификата об успешном прохождении кибериспытания. Постоянный режим позволяет Заказчикам проводить непрерывную оценку своей защищенности с учетом проходящих в организации изменений (изменений бизнес-процессов, технологий и информационной безопасности).

В режиме постоянного Кибериспытания Площадка готовит Отчет Площадки каждые 183 (сто восемьдесят три) календарных дня Активного периода. Площадка отправляет Отчет Площадки в течение 5 (пяти) рабочих дней после

завершения 183 (сто восемьдесят три) календарных дней Активного периода. На основании Отчёта Площадки Экспертный совет подводит результаты, готовит Отчет о кибериспытании и выпускает Сертификат об успешном прохождении Кибериспытания или Заключение, и передаёт данные результаты Заказчику.

Если Экспертный совет признает Кибериспытание в постоянном режиме состоявшися и успешным, Сертификационная организация выпускает Сертификат об успешном прохождении Кибериспытания по НС/списку НС Заказчика, который действует на условиях, указанных в Сертификате.

Если Экспертный совет признает Кибериспытание в постоянном режиме несостоявшимся и неуспешным, Сертификационная организация выпускает Заключение по НС/списку НС Заказчика, в котором содержится подробное разъяснение причин признания Кибериспытания несостоявшимся или неуспешным.

После подведения итогов Кибериспытание продолжается циклично в таком же порядке следующие 6 (шесть) месяцев – 183 (сто восемьдесят три) календарных дня. По результатам каждого периода рассчитывается скоринговый балл, который принимает значение от 0 до 100, и позволяет дать сравнительную оценку проведенного Кибериспытания. Эта оценка может быть использована для сравнения с другими завершенными Кибериспытаниями.
Режим постоянного Кибериспытания проходит согласно актуальным УП, которые утверждены экспертным советом.

4.10 Приостановка

Решение о приостановке Кибериспытания может принять Заказчик, Площадка, Сертификационная организация или Экспертный совет.
Кибериспытание считается приостановленным, если:

- Заказчик обратился к Площадке или Сертификационной организации с заявкой на приостановку Кибериспытания;

- Площадка по техническим причинам не может проводить Кибериспытание;
- Экспертный совет решил приостановить Кибериспытание.

Период приостановки не учитывается при расчете срока Активного периода проведения Кибериспытания. Если приостановка Кибериспытания является предметом спора между Заказчиком и Площадкой, итоговое решение о приостановке принимает Экспертный совет в срок не более 5 (пяти) рабочих дней с момента получения обращения.

Если в период первичного проведения (6 календарных месяцев или 183 дня), Кибериспытание приостанавливались по инициативе Заказчика более 3 (трёх) раз, Площадка вправе потребовать компенсации в размере не более 1% от совокупной стоимости вознаграждения, согласованного в договоре.

При проведении Кибериспытания в режиме КИ-экспресс, приостановка не предусмотрена. Любая приостановка принимается остановкой – завершением Кибериспытания.

4.11 Остановка

Заказчик имеет право остановить Кибериспытание, однако должен уведомить Площадку и Сертификационную организацию в срок не менее чем за 30 (тридцать) рабочих дней до даты планируемой остановки.
Заказчик несет финансовые обязательства по выплате вознаграждения Исследователям в течение всего срока до даты прекращения Кибериспытания, указанной в уведомлении.

5. Формирование реестра недопустимых событий

Для прохождения Кибериспытания Заказчик должен определить для себя самостоятельно или при помощи Экспертного совета/АО «Кибериспытание» Недопустимые события, которые в случае своей реализации могут привести к нарушению функционирования инфраструктуры, продукта и технологии.

При формировании реестра недопустимых событий должны привлекаться как работники из руководящего состава Заказчика, так и руководители подразделений, отвечающих за критические процессы.

Этапы формирования реестра недопустимых событий:

1. Проводится анализ процессов Заказчика для выявления критических процессов.
2. Определяются недопустимые события для Заказчика.
3. Определяются сценарии реализации Недопустимого события.
4. Данные фиксируются в реестре Недопустимых событий.

6. Действия при реализации НС

Реализация Недопустимого события на Кибериспытании фиксируется, когда Исследователь предоставляет необходимую Информацию, подтверждающую достижение критерия реализации этого НС, определенного в УП.

6.1 Действия исследователя

В случае достижения Исследователем критерия реализации НС, он\она должен в течение 60 (шестидесяти) минут уведомить об этом Площадку, а также передать ей соответствующие сведения о достижении НС либо критерия НС.
Также в течение 3 (трёх) часов с момента достижения критерия НС, Исследователь должен предоставить отчет, содержащий:

- информацию о достижении НС из реестра;
- перечень сведений, уже переданных Площадке;
- перечень всех дополнительных действий и событий, необходимых для достижения НС, либо критерия НС. Примеры таких событий: компрометация узлов и компонентов инфраструктуры Заказчика, компрометация учетных записей пользователей, время реализации НС и время компрометации других компонентов, предшествующих реализации НС.

6.2 Действия площадки

После получения информации о достижении критерия НС от Исследователя, Площадка в течении 60 (шестидесяти) минут информирует об этом Заказчика.
После получения отчета от Исследователя и его проверки, Площадка в течение 1 (одного) рабочего дня передает Заказчику всю необходимую документацию:

- отчет о достижении Недопустимого события;
- полученные от Исследователей сведения, необходимые для достижения НС;
- иные документы на усмотрение Площадки.

При проведении Кибериспытания в формате Кибериспытание-экспресс, Площадка информирует о достижении критерия НС Сертификационную организацию и/или ее аккредитованных посредников при наличии таковых.

6.3 Действия заказчика

После получения информации от Площадки Заказчик обязан в течение 3 (трёх) рабочих дней совершить одно из действий:

- согласиться с информацией, поступившей от Площадки, и признать наступление критериев НС;
- оспорить информацию, предоставив мотивированный ответ с описанием критериев, по которым Заказчик не считает НС наступившим.

В случае, когда Заказчик признает наступление критериев НС и готов выплатить вознаграждение в порядке, установленном настоящей Методикой и правилами Площадки, факт наступления критерия НС считается подтвержденным и участие Экспертного совета не требуется.

6.4 Действия экспертного совета

При возникновении спора между Заказчиком и Площадкой (в том числе представляющей интересы Исследователя), касающегося сведений из отчета о достижении критериев НС, Площадка в течение 1 (одного) дня после получения ответа от Заказчика предоставляет в Экспертный совет следующие документы:

- отчет о достижении Недопустимого события;
- полученные от Исследователей сведения, необходимые для достижения НС;
- иные сведения на усмотрение Площадки;
- ответ Заказчика.

Экспертный совет анализирует результаты и выносит решение о фактической реализации НС в течение 5 (пяти) рабочих дней с момента поступления заявки о разрешении спора по наступлению НС.

Экспертный совет имеет право запросить у Площадки дополнительную информацию о наступлении НС и событиях, связанных с ним. В результате, Экспертный совет принимает решение о признании или непризнании наступления НС.

6.5 Дальнейшие действия участников

При подтверждении критерия наступления НС Кибериспытание по НС приостанавливаются Заказчиком или Сертификационной организацией на время, необходимое Заказчику, чтобы устранить уязвимости, приведшие к наступлению НС либо критерия НС, и произвести выплаты Исследователю. При непризнаниии Экспертным советом Критерия наступления НС подтвержденным, Кибериспытание может быть продолжено в соответствии с утвержденными ранее УП.

После подтверждения Критерия наступления НС, Площадка информирует об этом все заинтересованные стороны, указанные в УП в разделе «Уведомления в случае реализации НС».

В дальнейшем, подтвержденный Критерий НС может быть повторно вынесен на Кибериспытание. Если Заказчик не изменял Реестр НС и Условия проведения Кибериспытания, никаких дополнительных действий не требуется.

В случае существенных изменений условий проведения Кибериспытания по НС, Заказчик по нему готовит УП и согласует с Экспертным советом.

При проведении Кибериспытания в формате Кибериспытание-экспресс, после достижения критерия НС кибериспытание считается завершенным, возобновление кибериспытания по заданному НС не проводится.

7. Учет значимых действий исследователей

Методика обязывает Исследователей вести учет всех своих действий, которые могут или могли повлечь Значимые события, и Значимых событий, в рамках участия в Кибериспытании на Платформе Площадки.
Это необходимо, чтобы защитить интересы как Заказчика, так и Исследователя. Информация о таких действиях и Значимых событиях является конфиденциальной и Площадка не в праве разглашать имеющуюся у нее информацию Заказчику без письменного разрешения Исследователя, являющегося владельцем данной информации.

Информация об указанных действиях и Значимых событиях используется для разрешения спорных ситуаций, а также в период подведения итогов Кибериспытания Экспертным советом.

Если Заказчик подозревает хакерскую атаку, он вправе запросить информацию о действиях и Значимых событиях Исследователей у Сертфиикационной организации только для того, чтобы выяснить, является ли возможная атака частью активности Исследователей. На основании имеющихся данных, полученных от Площадки, можно ответить «Является» или «Не является», не раскрывая дополнительную информацию.

7.1 Значимые события

Исследователю необходимо сохранять сведения о наступлении любого Значимого события. Таковым считается любое событие, которое может повлиять на деятельность Заказчика или результат Кибериспытания. Данная Методика определяет следующие значимые события:

- получение доступа к недоступным ранее учетным записям (УЗ);
- получение доступа к ранее недоступным узлам сети;
- повышение привилегий в операционной системе;

- активное противодействие средств защиты, либо обход средства защиты;
- действия, которые повлекли за собой нарушение работы сервиса или хоста;
- подтвержденное Заказчиком наступление Недопустимого события или Критериев НС после подтверждения Экспертного совета.

Заказчик имеет право определить дополнительные Значимые события в УП, в разделе 13.7 «Расширенный список значимых событий».

При проведении Кибериспытания в формате Кибериспытание-экспресс, учет Значимых событий может отсутствовать либо проводиться в упрощенном виде. В этом случае, информация о порядке учета Значимых событий публикуется на сайте Площадки и/или Сертификационной организации.

7.2 Перечень сведений, обязательных для сохранения

В рамках сохранения и возможности дальнейшего уведомления, Исследователь должен быть готов сохранить и при необходимости предоставить Площадке определенные сведения, которые необходимы для подготовки заключения экспертным советов или определяются скоринговой моделью.

- IP-адрес, с которого происходит эксплуатация уязвимости;
- утилита, эксплоит, номер эксплоита, применяемый для эксплуатации уязвимости;
- приблизительное время эксплуатации/получения данных (с точностью до 30 минут);
- подтверждение факта эксплуатации, позволяющие его однозначно определить.

При передаче третьему лицу эти данные должны быть маскированы.
Исследователи должны сохранять сведения о своих действиях для передачи третьему лицу в случаях, перечисленных ниже:

- достижение НС;
- компрометация учетной записи пользователя системы Заказчика;
- компрометация компонента инфраструктуры, продукта или технологии Заказчика;
- сканирование внутренних систем Заказчика с использованием скомпрометированных компонент инфраструктуры, продукта или технологии, и/или скомпрометированных УЗ;
- нарушение работоспособности одного из компонентов инфраструктуры, продукта или технологии Заказчика.

В случае достижения одного из вышеперечисленных пунктов Исследователи обязаны сохранить и передать эту информацию Площадке не позднее 60 минут после достижения одного из этих событий.
Для скомпрометированных учетных записей пользователя/системы Исследователи должны сохранять:

- пароль, маскированный с читаемым первым и последним символом;
- логин;
- домен, маскированный;
- роль, маскированная;
- краткое описание получения доступа к данным.

Для скомпрометированных компонент Исследователи должны сохранять, например, следующие данные:

- скриншот вызова команд ifconfig, whoami, uname;
- имя сервиса/службы/хоста;
- скриншот, позволяющий определить привилегии в учетной записи, с которой осуществлена компрометация системы;
- маскированные персональные данные;
- краткое описание эксплуатации.

В случае нарушения работоспособности системы Исследователи должны сохранять:

- имя сервиса/службы/хоста/файла, IP-адрес или любой другой идентификатор, позволяющий определить компонент системы;
- скриншот, подтверждающий нарушение работоспособности системы;
- маскированные персональные данные;
- краткое описание эксплуатации, повлекшей нарушение работоспособности системы.

В случае достижения НС Исследователи должны сохранять:

- имя сервиса/службы/хоста, IP-адрес или любой другой идентификатор, позволяющий определить компонент системы;
- скриншот, подтверждающий достижение НС;
- перечень необходимых доказательств согласно условиям, описанным в программе «Кибериспытания».
- краткое описание эксплуатации с указанием цепочки предыдущих событий.

7.3 Сроки регистрации значимых событий

Методика определяет максимальный срок регистрации Значимого события равный 24 часам с момента реализации Значимого события.

7.4 Санкции в случае нарушения правил учета

При систематическом (два и более раз) нарушении Исследователем правил по учету значимых событий, к нему будут применены санкционные меры — от понижения рейтинга, если предусмотрено Платформой Площакди, до закрытия возможности участия в Кибериспытании.

Дополнительно, если Исследователь реализовал НС, но на Платформе Площадки отсутствуют зарегистрированные Значимые события, то Исследователь получает 50% от суммы вознаграждения за реализацию НС.

8. Мониторинг

Площадка несет ответственность за непрерывный мониторинг хода Кибериспытания по следующим параметрам:

	Параметр	**Действия**	**Комментарий**
1.	Соответствие количества активных Исследователей на Кибериспытании требованиям УП.	1. Если количество активных Исследователей на Кибериспытании за последние 2 недели было ниже минимального порога, определенного в УП, Площадка в течение 1 рабочего дня уведомляет об этом Заказчика и Сертификационную организацию. 2. В момент, когда количество активных Исследователей Кибериспытания возвращается на требуемый уровень, Площадка в течение 1 (одного) рабочего дня уведомляет Заказчика и Сертификационную организацию.	Для расчета активных Исследователей см. П 10.2 «Порядок подсчета активных исследователей».

2.	Активные спорные ситуации между Заказчиком и Исследователями.	В случае возникновения спорной ситуации между Заказчиком и Исследователями, Площадка в течение 1 (одного) рабочего дня уведомляет Сертификационную организацию.	
3.	Приостановка Кибериспытания.	В случае приостановки Кибериспытания по решению Заказчика/Площадки/Экспертного совета, Площадка в течение 1 (одного) рабочего дня уведомляет всех участников Кибериспытания (Заказчика, Сертификационную организацию, Исследователей).	

9. Ограничения

Кибериспытание максимально приближено к реальной ситуации, которая может возникнуть в инфраструктуре, продукте или технологии Заказчика. Это предполагает, что Кибериспытание не имеет ограничений по действиям Исследователей. Однако, Заказчик в праве определить список ограничений в УП. Этот список будет рассмотрен Экспертным советом в рамках рассмотрения заявки. Экспертный совет может согласовать или не согласовать отдельные ограничения или список целиком.

Заказчик имеет право активно противодействовать Исследователям любым способом, которым он может противодействовать злоумышленникам, с учетом согласованных в УП ограничений.

Заказчик не имеет права ограничивать Исследователю доступ к своей инфраструктуре, кроме как в рамках регулярных процедур по защите инфраструктуры.

9.1 Ограничения для исследователей

- DdoS атаки допустимы только при наличии в перечне НС события, связанного с доступностью инфраструктуры Заказчика.
- Запрещается реализовывать НС, если возможно ограничиться сбором доказательств, подтверждающих наличие возможности у Исследователя реализовать это НС.
- Запрещается реализовывать НС, если собраны доказательства, подтверждающие, что у Исследователя есть возможность реализовать это НС.
- Исследователь не должен выходить за рамки, обозначенные в УП, не может атаковать инфраструктуру партнеров Заказчика с целью реализовать НС в инфраструктуре Заказчика. Партнеры Заказчика всегда являются «out of scope».
- Исследователь не вправе загружать на свои системы персональные данные, конфиденциальную информацию Заказчика без предварительного разрешения (например условий программы

Кибериспытания опубликованных на Платформе Площадки). Если есть предварительное разрешение, сохранять на стороне Исследователя, можно только ограниченную часть данных в маскированном формате и слепок этих данных (например, хеш-сумму от одной записи в базе данных заказчика, дополнительно скриншот маскированных данных, хеш сумму файла, содержащего конфиденциальные данные дополнительно маскированный скриншот конфиденциальных данных).

9.2 Ограничения для заказчика

- В случае простоя одного или более сервисов, влияющих на наступление НС, срок испытания для данного НС увеличивается на общее количество дней простоя.
- Информацию от Площадки по Исследователям разрешено использовать только для определения этичности/неэтичности Исследователей.
- Запрещено любое воздействие на Исследователей кроме их блокировки и иного противодействия в инфраструктуре Заказчика при обнаружении подозрительной активности.
- Заказчик гарантирует и может подтвердить при возникновении такой необходимости, что обозначенные в УП сетевые узлы и части инфраструктуры находятся у него на законных основаниях и под управлением Заказчика.

9.3 Запрещенные действия

В ходе проведения Кибериспытания запрещены действия, влекущие за собой или подразумевающие:

- нарушение КоАП РФ и УК РФ;
- атаку на сторонние системы, не имеющие отношения к тестируемому Заказчику;
- физическое воздействие либо угрозу физического воздействия на сотрудников Заказчика и их близких;
- шантаж, подкуп сотрудников Заказчика и их близких;
- атаку на личные устройства сотрудников Заказчика;

- кражу и порчу имущества Заказчика;
- вывод из строя систем тестируемого Заказчика, включая удаление и повреждение баз данных, шифрование данных.

10. Изменение условий проведения по инициативе заказчика

10.1 Предварительное согласование изменений

1. Если в ходе Кибериспытания Заказчик хочет внести изменения в условия его проведения, он должен обратиться к Сертификационной организации для оценки значимости вносимых изменений и их влияния на дальнейший ход Кибериспытания. Для этого Заказчик в свободной форме предоставляет всю необходимую информации, касающуюся изменения.
2. Сертификационная организация передает Площадке полученную информацию.
3. Площадка от лица Исследователей в срок до 5 (пяти) рабочих дней определяет значимость вносимых изменений и их влияние на ход Кибериспытания.
4. Если Площадка и Сертификационная организация признает изменения незначительными, Площадка уведомляет в течение 1 (одного) рабочего дня с момента принятия такого решения.
5. На основе этого уведомления Сертификационная организация может внести запрошенные им изменения в УП.
6. Если Площадка и Сертификационная организация признает изменения значительными, Заказчик не может внести их, пока не согласует с Экспертным советом. Для этого Заказчик обращается в Сертификационную организацию и Экспертный совет, предоставляет актуальное УП и информацию о планируемых изменениях. Экспертный совет согласует изменения в срок до 5 (пяти) рабочих дней. Возможные результаты согласования см. 10.3 Действия Экспертного совета.

При проведении Кибериспытания в формате Кибериспытание-экспресс изменение условий не предусмотрено.

10.2 Обнаружение изменений исследователем

1. Исследователь обязан уведомить Площадку, если считает, что Заказчик в ходе Кибериспытания внес значимые изменения в условия его проведения. Вместе с уведомлением Исследователь предоставляет необходимые подтверждения этого изменения и обоснование его значимости.
2. Площадка в течение 1 (одного) рабочего дня должна уведомить Заказчика и потребовать отменить все внесенные изменения.
3. Если Заказчик согласен с правомерностью запроса Площадки, Заказчик должен отменить внесенные изменения в течение 72 часов.
4. Если Заказчик не согласен с оценкой значимости внесенных изменений, он в течение 72 часов предоставляет Площадке письменный мотивированный отказ от отмены изменений.
5. На основе полученной от Заказчика информации, Площадка в течение 1 (одного) рабочего дня обращается в Экспертный совет для разрешения конфликта. Площадка предоставляет Экспертному совету:
    - УП;
    - информацию от Исследователя(ей);
    - информацию от Заказчика.

10.3 Действия экспертного совета

Экспертный совет рассматривает запрос Заказчика на внесение изменений в условия проведения Кибериспытания в соответствии с п. 10.1. или информацию об уже внесенных Заказчиком изменениях в соответствии с п 10.2. В обоих случаях Экспертный совет должен дать ответ на запрос в срок до 5 (пяти) рабочих дней с момента получения запроса. Существует 3 возможных исхода:

1. Изменение условий Кибериспытания признается правомерным и не имеющим существенного влияния. Заказчик имеет право применить

изменения.

Если изменения уже были внесены, Заказчик не отменяет ранее внесенные им изменения. Период с момента внесения изменений до момента принятия положительного решения Экспертного совета по изменению идет в учет активного периода Кибериспытания.

2. Изменение условий Кибериспытания признается неправомерным и имеющим существенное влияние, Заказчик не имеет права применить изменения.

   Если изменения уже были внесены, Заказчик должен отменить все внесенные изменения в срок до 72 часов. Период с момента внесения изменений до отмены изменений не идет в учет активного периода Кибериспытания.

3. Ознакомившись с доводами Заказчика, Экспертный совет предлагает альтернативный вариант изменений.

   Если изменения уже были внесены, Заказчик должен отменить все внесенные изменения в срок до 72 часов, период с момента внесения изменений до отмены изменений не идет в учет Активного периода Кибериспытания. Заказчик имеет право внести альтернативные изменения, предложенные ЭС.

Если Заказчик не согласен с решением ЭС, Кибериспытание приостанавливается для поиска оптимального решения с целью возобновить Кибериспытание.

11. Оценка состоятельности Кибериспытания

Оценка эффективности проведения Кибериспытания строится на основе анализа реальных действий Исследователей при достижении Критериев НС, которые в свою очередь подсчитываются на основе зарегистрированных на Платформе Площадки Значимых событий (см. раздел 7).

Методика определяет минимальные требования к объему проведенных действий, необходимых для успешной оценки защищенности.

11.1 Первичное проведение Кибериспытания

Для оценки эффективности хода Кибериспытания до момента получения Сертификата о его успешном прохождении, первые 6 месяцев (3 месяца для КИ-экспресс) его проведения разбиваются на 3 этапа. По окончанию каждого из них предпринимается ряд возможных действий в зависимости от хода проведения Кибериспытания. В случае приостановки Кибериспытания, время текущего этапа также приостанавливается.

11.1.1. Этап 1 - «Привлечение»

Данный этап проходит в течение первых 2 месяцев (в течение первого месяца для КИ-экспресс) с даты запуска Кибериспытания. По его окончанию оценивается количество привлеченных на Кибериспытание Исследователей (активность исследователей не оценивается). Для этого Площадка предоставляет информацию о количестве зарегистрированных на Кибериспытание Исследователей.

Для каждого НС Методика устанавливает минимальное количество Исследователей, зарегистрированных для участия в Кибериспытании. Минимальное число является суммарным значением, по всем Площадкам, у которых запущенно Кибериспытание по конкретному НС.

В случае, если по итогу этапа количество зарегистрированных на Кибериспытание Исследователей меньше минимально установленного значения, Площадкам дается еще семь календарных дней для привлечения дополнительных Исследователей. Если после этих дополнительных дней

количество зарегистрированных Исследователей все еще ниже требуемого минимального числа, Кибериспытание приостанавливается, выносится вопрос по пересмотру суммы вознаграждения или изменения иных требований в условиях проведения Кибериспытания.

При проведении Кибериспытания в формате Кибериспытание-экспресс изменение условий или вознаграждения не предусмотрено.

11.1.2. Этап 2 - «Первые результаты»

Данный этап проходит в течение последующих 2 месяцев (в течение второго месяца для КИ-экспресс) проведения Кибериспытания. На данном этапе оценивается активность Исследователей и количество зарегистрированных Значимых событий. Предполагается, что в ходе данного этапа должно быть зафиксировано достаточно Значимых событий для того, чтобы считать Кибериспытания успешно проходящими.

Для каждого НС Методика устанавливает минимальное количество Значимых событий, зарегистрированных на Площадке. Данное минимальное число является суммарным значением, по всем Площадкам, где запущенно Кибериспытание по конкретному НС. В случае, если в ходе данного этапа было зарегистрировано целевое значение Значимых событий, Кибериспытание продолжается без изменений.

В случае, если по итогам данного этапа, количество зарегистрированных Значимых событий меньше минимально требуемого значения, Методика требует изменения суммы вознаграждения, согласно таблице ниже.

Доля зарегистрированных Значимых событий от целевого значения, в %	**Изменение величины вознаграждения к текущему значению**
80% и более	+10%
50-80%	+20%
20-50%	+30%
20% и менее	+50%

Таблица 1. Изменение вознаграждения в зависимости от числа зарегистрированных Значимых событий.

При проведении Кибериспытания в формате Кибериспытание-экспресс изменение условий или вознаграждения не предусмотрено.

11.1.3. Этап 3 - «Активная фаза»

Данный этап проходит в течение заключительных 2 месяцев (в течение третьего месяца для КИ-экспресс) Кибериспытания. На данном этапе оценивается активность Исследователей – предполагается, что количество Значимых событий должно быть не менее оценки целевого значения на предыдущем этапе.

Дополнительно к этому, если по результатам подсчета Значимых событий на предыдущем этапе менялась сумма вознаграждения, вводится промежуточная дата подсчета Значимых событий, в дату завершения первого месяца этапа 3. В эту дату проверяется эффект изменения вознаграждения. Если в результате подсчета количество зарегистрированных событий за месяц работ на этапе 3 равен половине минимального значения, услуги по Кибериспытанию продолжаются без изменений.

В случае, если количество Значимых событий не достигает половины оценки целевого значения на предыдущем этапе, на последующем этапе производится выяснение причин. Для этого проводится детальная верификация действий Исследователей на протяжении Кибериспытания. Для этого в срок начиная с 5-го по 6-й месяц (начиная с третьего месяца для КИ-экспресс) проведения Кибериспытания Исследователи должны зарегистрировать свои Значимые события, которые не привели к результату в упрощённой форме. Для этого на Платформе Площадки вносятся следующие данные:

- что делал Исследователь (попытка получения доступа, рассылка, атака);
- когда делал (дата и время);
- что получилось в результате (краткое описание).

Все вышеобозначенные действия для успешного проведения Кибериспытания Площадка должна проводить самостоятельно, при необходимости привлекая Заказчика или Экспертный совет.

При проведении Кибериспытания в формате Кибериспытание-экспресс, требования к активности исследователей могут отличаться от приведенных выше и могут определяться индивидуально Сертификационной организацией. Изменения величины вознаграждения не предусматривается.

11.2 Постоянный режим

Для постоянного режима проведения Кибериспытания Методикой не определяется необходимое минимальное количество зарегистрированных Значимых событий.

Обязательно рекомендуется вести их учет для оценки полноты исследуемых векторов атак и киберугроз.

12. Требования к вознаграждению

12.1 Определение начальной суммы вознаграждения Исследователям

Сумма вознаграждение Исследователям является ключевым фактором успешного проведения Кибериспытания, ее правильное определение позволяет привлечь достаточное количество квалифицированных исследователей для объективной оценки защищенности. Сумма вознаграждения и логика ее формирования рассматривается и согласовывается экспертным советом. В случае, если экспертный совет не видит возможным получение необходимого результата Кибериспытания за обозначенное в УП вознаграждение, он выносит вопрос изменения начальной суммы вознаграждения Исследователям.

При проведении Кибериспытания в формате Кибериспытание-экспресс, первоначальная величина вознаграждения определяется условиями акции, опубликованной на сайте Кибериспытания и пересмотру не подлежит.

12.2 Определение рекомендованной суммы вознаграждения

Для определения максимально точной оценки киберзащищенности определены требования к начальной сумме вознаграждения исследователям, которая определяется по следующей формуле:

$S_{(Вознаграждения)}=S_{(Значимых\ событий)}*S_{(Bug\ \ Bounty)}*K_{(Кибериспытание)}*K_{(Текущий\ уровень\ ИБ)}$;

где:

$S_{(Значимых\ событий)}$ - среднее количество значимых событий в цепочке до достижения недопустимого события, определенных в сценариях реализации НС;

$S_{(Bug\ \ Bounty)}$ – средняя стоимость вознаграждения за критическую уязвимость на программах Bug Bounty, проводимых Заказчиком или другими компаниями, имеющими соизмеримый уровень зрелости ИБ;

$K_{(Кибериспытание)}$ – коэффициент Кибериспытания, предполагающий получение вознаграждения только при реализации НС, а не отдельных уязвимостей.;

$K_{(Текущий\ уровень\ ИБ)}$ – коэффициент текущего уровня ИБ организации, рассчитанный на основе предоставленной Анкеты заказчика (расчет коэффициента, так же доступен в

Анкете). Показатели информационной безопасности для оценки отбираются в соответствии с отраслевой принадлежностью Заказчика. Коэффициент текущего уровня ИБ организации определяется по значению R согласно анкете.

Пример расчета суммы вознаграждения (цифры даны условно):

$S_{(Значимых\ событий)}$ = 5 (количество значимых событий в цепочке для достижения НС)

$S_{(Bug\ \ Bounty)}$ = 800 тыс. руб.

$K_{(Кибериспытание)}$ = 2,5

$K_{(Текущий\ уровень\ ИБ)}$ = 3

$S_{(Вознаграждения)}$= 5 * 800 000 * 2,5 * 3 = 30 млн руб.

При проведении Кибериспытания в формате Кибериспытание-экспресс, приведенные выше расчеты не применимы. Величина вознаграждения устанавливается Сертификационной организацией. Вознаграждение в ходе КИ-эксперсс не изменяется.

12.3 Порядок пересмотра суммы вознаграждения

Во время первичного размещения на Кибериспытании (первые 6 месяцев) пересмотр суммы вознаграждения зависит от активности Исследователей, участвующих в Кибериспытании. Порядок пересмотра суммы вознаграждения приведен в п.12.2 настоящей Методики.

Если первичное Кибериспытание признано успешным на основе дополнительной информации, предоставленной Исследователями о действиях, не приведших к успеху (см. п.11.1.3. Этап 3), что в свою очередь означает не достижение минимального порога зарегистрированных Значимых событий, то происходит пересмотр вознаграждения для постоянного режима Кибериспытания согласно таблице 1 из раздела 11.1.

При проведении Кибериспытания в формате Кибериспытание-экспресс первоначальная величина вознаграждения не изменяется.

12.3 Внешние факторы, влияющие на сумму вознаграждения

Методика предусматривает и учитывает внешние факторы, которые могут увеличивать требования к минимальной сумме начального вознаграждения исследователям. Так, например, страховые компании, предлагающие киберстрахование на основе полученного Сертификата о Кибериспытании могут привязать минимальную сумму вознаграждения исследователям к сумме страхового покрытия.

12.4 Вознаграждение исследователям при сборе неуспешных значимых событий

Согласно разделу 11.1 «Первичное проведение Кибериспытания» (Этап 3 – «Активная фаза»), если количество значимых событий не достигло требуемого Методикой количества, Исследователи должны внести информацию об неуспешных значимых действиях, которые они осуществляли в рамках проводимого Кибериспытания. Для поощрения исследователей, из бюджета выделенного на вознаграждения за НС, выделяется сумма равная 10% от первичной суммы вознаграждения за НС, которая выплачивается в следующей пропорции ТОП5 участников, предоставившим наиболее полные и достоверные данные по своим попыткам реализации НС, проверенные и выбранные Экспертным советом:

- Первое место: 5%;
- Второе место: 2,5%;
- Третье место: 1,25%;
- Четвертое место: 0,75%;
- Пятое место: 0,5%.

13. Требования к условиям проведения

Раздел регламентирует подход к составлению Условий проведения (далее – УП) для проведения Кибериспытания. Соответствие УП требованиям этого раздела является обязательным условием для согласования его Экспертным советом и старта Кибериспытания.

13.1 Информация о заказчике

Данный раздел УП должен содержать общую информацию о Заказчике услуг (форма собственности, наименование, ИНН,, ОГРН, место регистрации), позволяющую произвести его однозначную идентификацию.

13.2 Место проведения

Заказчик имеет возможность выбрать один из двух вариантов проведения Кибериспытания:

1. организованная Площадка из списка аккредитованных Площадок cyberfy.ru;
2. собственная инфраструктура.

В рамках УП Заказчик может указать как конкретную Площадку, на которой он намерен провести Кибериспытание, так и выбрать один из двух приведенных выше вариантов без указания конкретной Площадки.
Настоящая Методика не запрещает проводить Кибериспытания у более чем одной Площадки одновременно, в том числе для различных перечней Недопустимых событий.

При проведении Кибериспытания в формате Кибериспытание-экспресс, проведение Кибериспытания на собственной инфраструктуре Заказчика невозможно, Площадка проведения определяется Сертификационной организацией либо аккредитованным посредником.

13.3 Недопустимые события

Раздел УП описывает список Недопустимых событий, подготовленный для запуска Кибериспытания и содержит следующую информацию:

13.3.1 Название

Название НС, кратко описывающее его суть.

Пример:

Кража денежных средств со счета Заказчика.

13.3.2 Детальное описание

Подробное описание значимой для эффективного проведения Кибериспытания информации, включая бизнес контекст, значимые метрики и т.д.

Пример:

В компании XYZ существуют процессы, связанные с движением денег: оплата услуг контрагентов, покупки лицензий, выдача заработной платы и многие другие. Исследователю необходимо разобраться, как работают бизнес-процессы, какие системы в них участвуют, и попробовать перевести деньги на любой подконтрольный себе счет.

13.3.3 Критерий достижения НС

Критерии наступления Недопустимого события, позволяющие однозначно определить ситуацию, когда исследователь достиг результата.

Методика рекомендует определять такой критерий через бизнес-метрики и показатели, на основе самого Недопустимого события, но с порогом негативного влияния на компанию Заказчика существенно ниже уровня, когда событие становится недопустимым. Это позволит не раскрывать какую-либо дополнительную информацию технического характера и провести испытания в условиях максимально приближенных к реальным.

Примеры (все данные приведены условно):

	Недопустимое событие	Критерий наступления НС
1	Кража денежных средств со счета компании в размере 500 млн. руб.	Исследователь должен перевести до 2499 рублей со счета Заказчика на любой подконтрольный себе счет. Транзакция должна быть инициирована Исследователем и пройти через банк. Перевод денег сотруднику Заказчика не считается реализацией Недопустимого события.
2	Кража персональных данных клиентов Заказчика в объеме более 100 тыс. записей.	Исследователь должен предоставить не менее 100 записей персональных данных клиентов Заказчика.
3	Остановка дистанционного обслуживания клиентов Заказчика за счет блокирования работы мобильного приложения Заказчика на срок более трех рабочих дней.	Исследователь должен внести новый элемент (детальная спецификация) в продуктовый каталог мобильного приложения Заказчика.

При проведении Кибериспытания в формате Кибериспытание-экспресс, допустимо использование ограниченного перечня Недопустимых событий, информация о котором публикуется на сайте Кибериспытания.

13.3.4 Вознаграждение

Вознаграждение и детальное описание правил и условий, в соответствии с которыми Заказчик будет производить выплаты Исследователям в случае достижения условий НС. Правила выплат не должны противоречить правилам выбранной Площадки.

Кроме того, УП должно содержать правила пересмотра величины вознаграждения в ходе Кибериспытания, не противоречащие п.13 настоящей Методики. В УП должны быть подробно описаны правила изменения величины вознаграждения, порядок изменения и все необходимые условия, приводящие к нему.

13.3.5 Ограничения

Ограничения действий Исследователей при проведении Кибериспытания регламентируются п.9 данной Методики, однако Заказчик может определить дополнительные ограничения, но в пределах возможности проведения Кибериспытания Исследователями.

12.3.6 Срок запуска

Срок запуска Кибериспытания по каждому Недопустимому событию. Кибериспытания по разным НС могут запускаться одновременно или по отдельности.

13.4 Требования к исследователям

Раздел УП описывает список обязательных и дополнительных требований к Исследователям, которые может устанавливать Заказчик.

13.4.1 Авторизация

Методика определяет следующие варианты авторизации Исследователей:

1. все, зарегистрированные на Платформе Площадки;
2. зарегистрированные только по приглашениям;
3. зарегистрированные и прошедшие верификацию через Госуслуги;
4. зарегистрированные юридические лица.

13.4.2 Другие требования

Заказчик имеет право указать дополнительные требования к Исследователям. Важно учитывать, что это усложняет привлечение Исследователей в необходимом числе.

Такими требованиями могут быть:

1. ограничение по возрасту;
2. наличие специализированных сертификатов;
3. участие сотрудников Заказчика;
4. И т.п.

При проведении «Кибериспытания» в формате Кибериспытание-экспресс, требования к исследователям определяются Сертификационной организацией.

13.5 Требования к экспертному совету

Заказчик имеет право уточнить требования к Экспертам, которые проводят экспертизу Кибериспытания, на предмет порядка разрешения конфликта интересов, но не может явно ограничивать или указывать конкретных Экспертов.

При проведении Кибериспытания в формате Кибериспытание-экспресс, оценку проводит единственный член экспертного совета, выбранный Сертификационной организацией либо самим Экспертным советом.

13.6 Уведомление

Раздел УП определяет список адресатов, параметры и порядок их уведомления согласно разделам 6 и 8.

13.7 Расширенный список значимых событий

Для анализа активности Исследователей, Методика в разделе 7.1 определяет список Значимых событий. Однако Заказчик вправе определить дополнительный список Значимых для него событий в данной разделе УП.

13.8 Вознаграждение за значимые события

Заказчик имеет право установить сумму вознаграждения за значимые для него Недопустимые события, указав их в УП.

13.9 Дополнительные разделы

УП может включать в себя неограниченное количество дополнительных разделов, способствующих эффективному проведению Кибериспытания. Содержание этих разделов не должно противоречить настоящей Методике.

14. Требования к площадке

14.1 Виды площадок

Настоящая Методика позволяет проводить Кибериспытание как на Организованной площадке, так и с использованием платформ Заказчика.

Организованные площадки проходят аккредитацию в Сертификационной организации и имеют право предоставлять услуги по проведению Кибериспытания третьим лицам.

Заказчики, выбравшие вариант проведения Кибериспытания на собственной платформе, не имеют права предоставлять услуги по проведению Кибериспытания с применением настоящей Методики третьим лицам (кроме дочерних компаний) и должны соответствовать требованиям, предъявляемым к Площадке Методикой.

14.2 Требования безопасности

Площадка проведения Кибериспытания должна соответствовать следующим требованиям безопасности:

1. иметь активное Кибериспытание, либо программу поиска уязвимостей (bug bounty) для собственной Платформы Площадки.
2. обеспечивать конфиденциальность передаваемой и хранящейся на ней информации.

14.3 Функциональные требования

Площадка должна соответствовать следующим функциональным требованиям:

1. Обеспечивать возможность управления доступом Исследователей к Кибериспытанию согласно п.14.4.1.
2. Обеспечить возможность единоразовой регистрации исследователя на Кибериспытании с указанием даты регистрации.

3. Обеспечить возможность категоризации исследователей по группам (Новичок, Специалист, Эксперт) по заранее согласованному с Сертификационной организацией правилу.
4. Обеспечивать возможность учета Значимых действий Исследователей согласно п. 7. Со следующими атрибутами:
    a. Исследователь;
    b. Дата значимого события (не разрешается вносить события позднее чем 24 часа от текущего момента);
    c. Тип значимого события согласно п.7.1;
    d. Свободное поле, с детальной информацией о действиях исследователя.
5. Обеспечивать возможность мониторинга Кибериспытания согласно п.8.
6. Иметь возможность публикации в сети Интернет информации о проводимых Кибериспытаниях и программах Bug Bounty в рамках собственной инфраструктуры.
7. Иметь возможность для сбора и анализа данных о количестве Исследователей и их активностях в рамках отдельных временных периодов, согласно требованиям, определенным к формату отчета Площадки.

14.4 Дополнительные требования для организованных площадок

1. Доказанный успешный опыт проведения Bug Bounty не менее двух лет.
2. Обеспечение круглосуточной поддержки и возможности реагирования на отчеты Исследователей и обращения Заказчика.

15. Требования к конфиденциальности

В вопросах защиты конфиденциальной информации отношения Заказчика, Исследователя, Площадки и Сертификационной организации регламентируются подписываемыми ими коммерческими документами и (или) некоммерческими соглашениями.

15.1 Требования к площадке

Площадка не имеет права разглашать сведения об Исследователях, их действиях, а также о ходе проведения Кибериспытания Заказчику, кроме как в случаях, предусмотренных законодательством РФ и настоящей Методикой.

15.2 Требования к исследователям

Исследователь не имеет права разглашать сведения о Заказчике, его инфраструктуре, уязвимостях, а также о ходе проведения Кибериспытания Заказчику, кроме как в случаях, предусмотренных законодательством РФ и настоящей Методикой, а также для целей проведения Кибериспытания.

15.3 Требования к экспертному совету и сертификационной организации

Экспертный совет не имеет права разглашать информацию об участниках, ходе проведения Кибериспытания, его результатах, а также свойствах инфраструктуры, продукта или технологии Заказчика, кроме как в случаях, предусмотренных законодательством РФ и настоящей Методикой.

16. Требования к отчету площадки по результатам

Отчет Площадки — это документ, подготовленный Площадкой, детально и подробно описывающий ход проведения Кибериспытания Исследователями. Он нужен для того, чтобы все заинтересованные стороны могли оценить ход проведения Кибериспытания и его результат.

Перечень пунктов, которые должны быть раскрыты в Отчете Площадки:

1. дата начала периода проведения Кибериспытания;
2. дата готовности Отчета Площадки;
3. количество дней Активного периода;
4. информация по реализованных НС в период проведения (если имелись);
5. среднее недельное количество активных Исследователей на Кибериспытании за весь учетный период с даты подачи последнего Отчета Площадки;
6. информацию обо всех Значимых событиях, зарегистрированных Исследователями на Платформе Площадки;
7. перечень всех спорных ситуаций, возникших между Исследователями и Площадкой в учетный период;
8. информацию о количестве и характере обращений Заказчика к Площадке;
9. информацию о внесенных в условия Кибериспытания дополнительных ограничений, отсутствующих в согласованном УП.

Экспертный совет должен оценить предоставленный Отчет Площадки на предмет полноты, возможных нарушений условий проведения Кибериспытания и соответствие настоящей Методике. На основе этой оценки ЭС согласовывает Отчет о Кибериспытании и выносит решение о соответствии или несоответствии УП проведенного Кибериспытания.

17. Режим Bug Bounty

Методика проведения Кибериспытания предполагает возможность произвести коммерческий обмен найденных Исследователем уязвимостей на денежное вознаграждение со стороны Заказчика.

При проведении «Кибериспытания» в формате Кибериспытание-экспресс, данный режим не применим.

17.1. Объект оценки

Могут быть обменяны уязвимости, которые определены Заказчиком в УП к проводимых Кибериспытаниях и зарегистрированные в качестве Значимых событий не позднее дня завершения Кибериспытания и начала подведения итогов.

17.2. Сроки

Обмен может быть осуществлен после завершения Кибериспытания, в момент, когда оно находится на оценке Экспертного совета. Для этого Исследователь должен уведомить Площадку о своем намерении.

17.3. Решение спорных ситуаций

В случае, если несколько Исследователей подали запрос на обмен по одной и той же уязвимости, то приоритет в обмене принадлежит Исследователю, который первым зарегистрировала уязвимость на Платформе (т.е. дата фиксации Значимого события этого Исследователя наступила первой). Если уязвимости были зарегистрированы в один день, то вознаграждение делится пропорционально между всеми Исследователями, зарегистрировавшими уязвимость.

17.4. Определение суммы вознаграждения

Сумма вознаграждения определяется Заказчиком по каждому типу уязвимости и указывается в УП на Кибериспытание в разделе 13.8 «Вознаграждение за значимые события».

18. Последствия действий иной силы

Если в ходе Кибериспытания обнаруживается активное и существенное воздействие злоумышленников, приведшее к реализации критерия НС, либо НС, Кибериспытание приостанавливается, выплаты не производятся.