Правила взаимодействия: Тестирование на проникновение и оценка безопасности

Специалист по информационной безопасности

2025-12-21

Обзор

Данный документ определяет правила взаимодействия (Rules of Engagement) для проведения тестирования на проникновение и оценки безопасности информационных систем. Документ устанавливает рамки сотрудничества между заказчиком и командой тестирования, обеспечивая безопасность, законность и эффективность процесса.

Цели документа

> **Основная задача** — обеспечить контролируемое и авторизованное тестирование с минимальными рисками для производственных систем

Правила взаимодействия гарантируют: - **Безопасность** производственных систем - **Соблюдение** законодательных требований - **Прозрачную коммуникацию** между всеми сторонами - **Контролируемое** и авторизованное тестирование

.

Контактная информация

Организация-заказчик

Роль	Контактные данные
Основной контакт	
Должность	_____
Мобильный телефон	_____
Электронная почта	_____
Резервный контакт	
Должность	_____
Мобильный телефон	_____
Электронная почта	_____

Команда тестирования

Роль	Контактные данные

Роль	Контактные данные
Руководитель команды	
Мобильный телефон	_____
Электронная почта	_____
Резервный контакт	
Мобильный телефон	_____
Электронная почта	_____
Экстренный контакт 24/7	
Мобильный телефон	_____
Электронная почта	_____

.

Область тестирования

Включенные в тестирование активы

Сетевая инфраструктура: - Домены: _____ - Поддомены: _____ - IP-диапазоны: _____ - Облачные ресурсы: _____

Приложения и сервисы: - Веб-приложения: _____ - API-интерфейсы: _____ - Внутренние системы: _____

Исключенные из тестирования активы

⚠ **Критически важные ограничения:**

- Системы, не принадлежащие организации
- Сторонние сервисы без письменного разрешения
- Производственные базы данных (если не разрешено явно)
- Социальная инженерия (если не одобрена)
- Системы критической инфраструктуры

.

Правила проведения тестирования

Разрешенные виды деятельности

Авторизованные методы тестирования:

- Сканирование уязвимостей
- Ручное тестирование на проникновение
- Тестирование веб-приложений
- Тестирование API-интерфейсов

- Анализ конфигурации облачных сервисов
- Тестирование сетевой безопасности
- Проверка политик паролей

Запрещенные виды деятельности

× **Строго запрещенные действия:**

- Атаки типа “отказ в обслуживании” (DoS/DDoS)
- Физическое проникновение
- Социальная инженерия без явного разрешения
- Брутфорс-атаки без ограничения скорости
- Действия, способные привести к повреждению данных
- Несанкционированный доступ к персональным данным

.

Ограничения по нагрузке

Технические ограничения для производственных систем

⚡ **Критически важные лимиты нагрузки:**

Параметр	Ограничение	Примечание
Максимальные запросы в секунду	_____	Для предотвращения перегрузки
Одновременные соединения	_____	Лимит параллельных подключений
Размер payload	_____	Максимальный размер данных
Timeout соединений	_____	Время ожидания ответа

Временные ограничения

🕐 **Расписание интенсивного тестирования:**

- **Массовые сканирования**: Только в нерабочее время
- **Fuzzing-тестирование**: _____ (указать временные окна)
- **Нагрузочное тестирование**: Только с предварительным уведомлением
- **Автоматизированные сканеры**: Ограничение скорости в рабочие часы

Мониторинг нагрузки

📊 **Контроль воздействия на системы:** - Мониторинг CPU и памяти целевых систем - Отслеживание времени отклика приложений - Контроль пропускной способности сети - Немедленная остановка при превышении лимитов

.

Юридические основания

Правовая база проведения тестирования

⚖️ **Юридическое обоснование:**

> Все действия по тестированию на проникновение выполняются исключительно на основании письменного разрешения уполномоченного представителя организации-заказчика

Документальные основания: - Подписанный договор на оказание услуг - Настоящие Правила взаимодействия - Техническое задание с описанием области тестирования - Дополнительные соглашения (при необходимости)

Ограничение ответственности

🛡️ **Освобождение от ответственности:**

Команда тестирования освобождается от ответственности за: - Временную недоступность систем в результате авторизованного тестирования - Обнаружение уязвимостей, существовавших до начала тестирования - Действия, выполненные строго в рамках согласованной области тестирования - Косвенные убытки, связанные с выявлением проблем безопасности

Соблюдение законодательства

📋 **Нормативное соответствие:** - Соблюдение требований законодательства о персональных данных - Выполнение отраслевых стандартов безопасности - Соответствие международным практикам пентестирования - Документирование всех действий для аудита

.

Матрица критичности уязвимостей

Классификация по уровням риска

Стандартизированная система оценки:

Уровень	Описание	Примеры уязвимостей	Время устранения

Уровень	Описание	Примеры уязвимостей	Время устранения
P0 - Критический	Немедленная угроза безопасности	RCE, SQL Injection, Authentication Bypass	24-48 часов
P1 - Высокий	Серьезное нарушение безопасности	XSS, LFI, Privilege Escalation	1-2 недели
P2 - Средний	Умеренный риск	Security Misconfiguration, CSRF	1 месяц
P3 - Низкий	Минимальный риск	Information Disclosure, Weak Ciphers	3 месяца
P4 - Информационный	Рекомендации по улучшению	Best Practices, Hardening	По возможности

Критерии оценки

📈 **Факторы определения критичности:** - **Воздействие**: Потенциальный ущерб от эксплуатации - **Вероятность**: Легкость эксплуатации уязвимости - **Область действия**: Количество затронутых систем - **Доступность**: Требования к доступу для эксплуатации

Процедура эскалации

⚡ **Экстренное реагирование на критические находки:** 1. **P0-P1**: Немедленное уведомление по телефону + email 2. **P2**: Уведомление в течение рабочего дня 3. **P3-P4**: Включение в регулярные отчеты

.

Список используемых инструментов

Авторизованные инструменты тестирования

Основной инструментарий:

Категория	Инструмент	Назначение	Версия
Сканеры уязвимостей	Nessus	Автоматизированное сканирование	_____
	OpenVAS	Сканирование сети и приложений	_____
	Qualys VMDR	Облачное	_____

Категория	Инструмент	Назначение	Версия
		сканирование	
Веб-тестирование	Burp Suite Professional	Тестирование веб-приложений	_____
	OWASP ZAP	Анализ безопасности веб-приложений	_____
	Nikto	Сканирование веб-серверов	_____
Сетевое тестирование	Nmap	Сканирование портов и сервисов	_____
	Masscan	Высокоскоростное сканирование	_____
Эксплуатация	Metasploit Framework	Тестирование эксплойтов	_____
	Cobalt Strike	Симуляция атак (при согласовании)	_____

Дополнительные инструменты

🛠 **Специализированное ПО (по согласованию):** - **Социальная инженерия**: SET, Gophish (только при явном разрешении) - **Беспроводные сети**: Aircrack-ng, Kismet - **Мобильные приложения**: MobSF, Frida - **Облачная безопасность**: ScoutSuite, Prowler

Ограничения на инструменты

⚠ **Запрещенные или ограниченные инструменты:** - Инструменты для DDoS-атак - Неавторизованные сканеры с агрессивными настройками - Инструменты для взлома паролей без ограничений скорости - Любое ПО, не согласованное с заказчиком

.

Идентификация команды тестирования

Белые списки для защитных систем

🔍 **Критически важно для предотвращения блокировки санкционированного тестирования:**

Параметр идентификации	Значение	Назначение
IP-адреса источников	_____	Статические IP для добавления в

Параметр идентификации	Значение	Назначение
		белые списки WAF/IPS
Диапазоны подсетей	_____	Дополнительные сетевые сегменты команды
User-Agent строки	_____	Специфические идентификаторы для веб-сканеров
SSH ключи	_____	Публичные ключи для авторизованного доступа

Специальные идентификаторы

🏷️ **Маркеры для логирования и мониторинга:**

- **Префикс тестовых запросов**: _____
- **Специальные заголовки HTTP**: _____
- **Идентификаторы сессий**: _____
- **Маркеры в payload**: _____

Координация с Blue Team

Взаимодействие с командой защиты: - Предварительное уведомление о начале тестирования - Список контактов SOC (Security Operations Center) - Процедура подтверждения легитимности активности - Протокол экстренной остановки тестирования

.

Определение опасных тестов

Классификация рискованных операций

⚠ **Тесты высокого риска, требующие особого внимания:**

Категория теста	Описание	Окно выполнения	Дополнительные меры
Брутфорс-атаки	Подбор паролей, PIN-кодов	Только нерабочее время	Ограничение скорости, мониторинг блокировок
Fuzzing приложений	Отправка некорректных	_____	Контроль стабильности системы

Категория теста	Описание	Окно выполнения	Дополнительные меры
	данных		
Эксплуатация уязвимостей	Выполнение proof-of-concept	По согласованию	Немедленное уведомление при успехе
Тестирование DoS	Проверка устойчивости к нагрузке	Только в тестовой среде	Предварительное согласование

Окна обслуживания для критических тестов

🕐 **Специальные временные интервалы:**

- **Основное окно рискованных тестов**: _____
- **Резервное окно**: _____
- **Экстренное окно (по согласованию)**: _____
- **Запрещенные периоды**: _____

Тестирование на стороне клиента

Защита конечных пользователей:

- **Фишинг-симуляции**: Только с письменного согласия HR
- **Тестирование браузеров**: Изолированные тестовые машины
- **Социальная инженерия**: Строго ограниченная область
- **Защита персональных данных**: Избегание доступа к личной информации

.

Техническая методология

Стандарты и классификации

📊 **Используемые международные стандарты:**

Стандарт	Версия	Применение
CVSS	v3.1/4.0	Оценка критичности уязвимостей
OWASP Top 10	2021	Веб-приложения
NIST Cybersecurity Framework	v1.1	Общая методология
OSSTMM	v3	Методология тестирования
PTES	v1.0	Стандарт пентестирования

Модель тестирования

🔍 **Уровень доступа к информации:**

- ☐ **Черный ящик** - Без предварительных знаний о системе
- ☐ **Серый ящик** - С частичным доступом к документации/архитектуре
- ☐ **Белый ящик** - С полным доступом к коду и архитектуре

Выбранная модель: _____

Оценка по CVSS

📈 **Критерии оценки уязвимостей:**

- **Базовые метрики**: Вектор атаки, сложность, привилегии, взаимодействие с пользователем
- **Временные метрики**: Доступность эксплойта, уровень исправления
- **Экологические метрики**: Влияние на конкретную среду заказчика
- **Пороговые значения**: P0 (9.0-10.0), P1 (7.0-8.9), P2 (4.0-6.9), P3 (0.1-3.9)

.

Дополнительные юридические аспекты

Трансграничная передача данных

🌍 **Международное соответствие:**

> При работе с международными командами тестирования обеспечивается соблюдение требований GDPR, CCPA и других применимых норм защиты данных

Юрисдикционные требования: - **Страна базирования команды**: _____ - **Применимое законодательство**: _____ - **Механизмы передачи данных**: Standard Contractual Clauses (SCC) / Adequacy Decision - **Локализация данных**: _____

Соответствие международным стандартам

📋 **Нормативное соответствие:**

Стандарт/Регулирование	Статус соответствия	Примечания
GDPR (EU)	_____	Защита персональных данных
ISO 27001	_____	Система менеджмента

Стандарт/Регулирование	Статус соответствия	Примечания
		ИБ
SOC 2 Type II	_____	Контроли безопасности
PCI DSS	_____	Платежные системы

Право на аудит

🔍 **Контроль процессов обработки данных:**

Заказчик имеет право: - Проверить процедуры удаления данных после завершения проекта - Запросить подтверждение уничтожения конфиденциальной информации - Провести аудит мер безопасности команды тестирования - Получить сертификаты соответствия применимым стандартам

.

Процесс реагирования на критические ситуации

Алгоритм экстренного реагирования

Пошаговая процедура для критических инцидентов:

1. ОБНАРУЖЕНИЕ КРИТИЧЕСКОЙ СИТУАЦИИ
↓
2. НЕМЕДЛЕННАЯ ОСТАНОВКА ТЕСТИРОВАНИЯ
↓
3. УВЕДОМЛЕНИЕ ЗАКАЗЧИКА (в течение 15 минут)
↓
4. ОЦЕНКА ВОЗДЕЙСТВИЯ И УЩЕРБА
↓
5. ПРИНЯТИЕ РЕШЕНИЯ О ПРОДОЛЖЕНИИ
↓
6. ДОКУМЕНТИРОВАНИЕ ИНЦИДЕНТА
↓
7. АНАЛИЗ ПРИЧИН И КОРРЕКТИРУЮЩИЕ МЕРЫ

Матрица эскалации

Контакты по уровням критичности:

Уровень	Время реагирования	Способ связи	Ответственный
P0 - Критический	15 минут	Телефон + SMS + Email	_____
P1 - Высокий	1 час	Телефон + Email	_____

Уровень	Время реагирования	Способ связи	Ответственный
P2 - Средний	4 часа	Email + Slack/Teams	_____
P3 - Низкий	24 часа	Email	_____

Критерии остановки тестирования

Автоматические триггеры прекращения работ:

- Недоступность критических сервисов более 5 минут
- Обнаружение активной эксплуатации уязвимостей третьими лицами
- Превышение согласованных лимитов нагрузки
- Запрос на остановку от любого уполномоченного представителя

.

Обработка доказательств и очистка

Протокол работы с доказательствами

🔒 Evidence Handling - строгие требования безопасности:

Этап	Требования	Ответственный
Сбор	Шифрование, хеширование, временные метки	Тестировщик
Хранение	Изолированное хранилище, контроль доступа	Руководитель проекта
Передача	Защищенные каналы, подтверждение получения	Обе стороны
Уничтожение	Безвозвратное удаление, сертификат уничтожения	Команда тестирования

План очистки после тестирования

Post-test Cleanup - обязательные процедуры:

Удаление созданных объектов: - [ ] Тестовые учетные записи пользователей - [ ] Загруженные файлы и скрипты - [ ] Временные конфигурации - [ ] Тестовые базы данных и таблицы

Восстановление исходного состояния: - [ ] Откат изменений конфигурации - [ ] Удаление тестовых сертификатов - [ ] Очистка логов тестирования (по согласованию) - [ ] Восстановление резервных копий (при необходимости)

Сертификация уничтожения данных

Документальное подтверждение:

По завершении проекта команда тестирования предоставляет: - Сертификат безвозвратного удаления всех данных заказчика - Отчет о выполненных процедурах очистки - Подтверждение соблюдения стандартов уничтожения данных (DoD 5220.22-M или аналогичных)

.

График тестирования

Временные рамки

Параметр	Значение
Дата начала	_____
Дата окончания	_____
Рабочее окно	_____
Часовой пояс	_____
Ежедневный брифинг	_____

Коммуникационный протокол

Регулярные обновления: - Ежедневные статус-отчеты - Еженедельные сводки прогресса - Экстренные уведомления при критических находках

.

Обработка инцидентов

Процедура реагирования на инциденты

В случае нестабильности системы во время тестирования:

1. **Немедленная остановка** тестирования командой
2. **Уведомление** организации-заказчика
3. **Принятие решения** экстренным контактом о продолжении
4. **Документирование** инцидента

Критерии остановки тестирования

🔍 **Условия для прекращения работ:** - Обнаружение критических уязвимостей - Нестабильность производственных систем - Превышение согласованных рамок тестирования - Запрос от заказчика

.

Обработка данных и конфиденциальность

Принципы работы с данными

> **Конфиденциальность** — приоритет номер один при обработке любой информации

Обязательства команды тестирования: - Чувствительные данные не сохраняются без необходимости - Все собранные данные шифруются - Данные удаляются после передачи отчета - Избегание доступа к персональным данным

Соглашение о неразглашении

Все участники тестирования обязуются: - Сохранять конфиденциальность полученной информации - Не разглашать результаты третьим лицам - Использовать данные исключительно для целей тестирования

.

Требования к отчетности

Структура отчетов

Промежуточные отчеты: - Ежедневные или еженедельные обновления - Статус выполнения задач - Предварительные находки

Финальная отчетность: - **Технический отчет** — детальное описание уязвимостей - **Управленческий отчет** — рекомендации для руководства - **Исполнительное резюме** — краткий обзор для топ-менеджмента

Формат представления результатов

📊 **Стандартизированная структура:** - Классификация уязвимостей по критичности - Рекомендации по устранению - Временные рамки для исправления - Метрики безопасности

.

Принятие рисков

Подтверждение организации-заказчика

Организация-заказчик подтверждает понимание того, что:

- Тестирование может выявить критические уязвимости
- Некоторые тесты могут вызвать временное снижение производительности
- Все действия авторизованы и согласованы

- Результаты будут использованы для улучшения безопасности

.

Чек-лист готовности к тестированию

Подготовительные мероприятия

- ☐ Определена область тестирования
- ☐ Назначены ответственные контакты
- ☐ Согласован график работ
- ☐ Подписаны все необходимые документы
- ☐ Настроены каналы коммуникации
- ☐ Подготовлена тестовая среда (при необходимости)
- ☐ Проведен инструктаж команды тестирования

Контрольные точки во время тестирования

- ☐ Ежедневные статус-встречи
- ☐ Мониторинг производственных систем
- ☐ Документирование всех действий
- ☐ Соблюдение временных рамок
- ☐ Регулярная связь с заказчиком

.

Подписи и утверждения

Представитель организации-заказчика

Поле	Значение
Имя и должность	_____
Подпись	_____
Дата	_____

Руководитель команды тестирования

Поле	Значение
Имя и должность	_____
Подпись	_____
Дата	_____

.

Контактная форма для экстренных ситуаций

Информация для быстрого реагирования

Параметр	Контактные данные

Параметр	Контактные данные
Основной контакт заказчика	_____
Резервный контакт заказчика	_____
Руководитель тестирования	_____
Экстренная линия 24/7	_____

Процедура экстренного контакта

1. **Первичный контакт** — основной представитель заказчика
2. **При недоступности** — резервный контакт
3. **Критические ситуации** — экстренная линия 24/7
4. **Документирование** всех обращений

.

Данный документ является юридически обязывающим соглашением между сторонами и должен быть подписан всеми участниками процесса тестирования на проникновение.