

Заказ № _____ от « _____ » _____ 20__ г.
к Договору № __ от « __ » _____ 20__ г.
оказания услуги республиканской платформы «Аттестация системы
защиты информации»
(ТЕХНИЧЕСКАЯ ЧАСТЬ)

Информация для определения объема работ при тестировании веб-ресурсов Клиента на проникновение (Пентест):

1	Перечень проверяемых доменов или IP-адресов включающие поддомены и URL	Доменное имя (IP-адрес)	URL (поддомены)
		<i>Пример:</i> 1) example.com 2) 12.13.14.1	<i>Пример:</i> 1) https://example.com/site 2) one.example.com
2	Список тестируемых мобильных приложений с указанием его названия либо используемого им IP-адреса и платформы (iOS, Android)	<i>Пример:</i> 1) application1 (Android, iOS) 2) application2 (iOS) 3) 12.13.14.1	
3	Управление ИТ и ИБ централизовано?	<i>Пример: Да</i>	
4	Укажите цели анализа защищенности		
4.1	Выявление всех возможных уязвимостей вне зависимости от степени их критичности	<i>Пример: Да</i>	
4.2	Выявление наиболее критических уязвимостей и способов их эксплуатации (тест на проникновение)	<i>Пример: Да</i>	
5	Укажите состав работ по анализу защищенности		
5.1	Проведение внешнего анализа защищенности (из сети Интернет)	<i>Пример: Да</i>	
5.2	Проведение внутреннего анализа защищенности (из сети организации)	<i>Пример: Да</i>	
5.3	Тестирование веб-ресурсов ¹	<i>Пример: Да</i>	
5.4	Тестирование мобильных приложений ²	<i>Пример: Нет</i>	
6	Укажите методы анализа защищенности которые необходимо использовались		
6.1	Анализ защищенности методом «черного ящика» (без предоставления реквизитов доступа к системам/сервисам)	<i>Пример: Не использовать</i>	
6.2	Анализ защищенности методом «серого ящика» (с предоставлением санкционированного доступа к системам/сервисам)	<i>Пример: Использовать</i>	
6.3	Методы социальной инженерии	<i>Пример: Использовать/Не использовать</i>	
7	Желаемое время и дата начала работ	<i>Пример: Дата 01.01.2024, Время начала 9:00</i>	
8	Желаемое время и дата окончания работ	<i>Пример: Дата 01.01.2024, Время окончания 15:00</i>	

¹ Тестирование веб-ресурсов проводится в соответствии с OWASP Testing Guide с фокусом на уязвимости списка OWASP Top 10 Application Security Risks;

² Тестирование мобильных приложений производится в соответствии с Mobile Security Testing Guide (MSTG) с фокусом на уязвимости из списка OWASP Mobile Top 10.

9	Адрес электронной почты для получения отчета по результатам проведения работ в рамках оказываемой услуги	<i>Пример: security@email.com</i>
10	Сотрудник Клиента ответственный за информационную безопасность и доступность ИС при проведении тестирования (ФИО, контактный телефон, адрес электронной почты)	