**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Комплексное тестирование на проникновение корпоративной информационной системы lms.cpcpipe.ru**

Оглавление

[1.0 ОБЩИЕ ПОЛОЖЕНИЯ 3](#_Toc87548324)

[2.0 ОБЩИЕ ТРЕБОВАНИЯ. 3](#_Toc87548325)

[3.0 ТРЕБОВАНИЯ К ОКАЗЫВАЕМЫМ УСЛУГАМ. 3](#_Toc87548326)

[4.0 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ. 4](#_Toc87548327)

[5.0 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ РАБОТ 5](#_Toc87548328)

[6.0 ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ 5](#_Toc87548329)

[7.0 ТЕХНИЧЕСКОЕ ПРЕДЛОЖЕНИЕ 5](#_Toc87548330)

[8.0 КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ 6](#_Toc87548331)

## ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Настоящее Техническое Задание выдано в соответствии с Меморандумом № Out-M-CPCR-9671-2021 ОТ 27.10.2021.
	2. Место предоставления услуг:

 г.Москва, ул.Павловская, дом 7, строение 1.

* 1. Цель предоставления услуг.

 Комплексное тестирование на проникновение направлено на выявление уязвимых мест Информационной Системы (ИС) lms.cpcpipe.ru и получение объективной, актуальной и независимой оценки уровня её защищенности с целью рассмотрения возможности дальнейшего опубликования в интернет.

* 1. Задачи проекта.
	+ Выявление уязвимостей и недостатков при использовании Заказчиком мерах информационной безопасности и оценка возможности их использования нарушителем;
	+ практическая демонстрация возможности использования уязвимостей;
	+ получение на основе объективных свидетельств комплексной оценки текущего уровня защищенности Системы;
	+ выработка рекомендаций по устранению выявленных недостатков для повышения уровня защищенности Системы.
	1. Объекты исследования в Системе

 Информационная система lms.cpcpipe.ru и компоненты.

* 1. Тип и длительность работ

 Сервис расположен во внутреннем периметре сети. Проводится внутреннее тестирование с физическим присутствием на объекте тестирования, согласно п.1.2.

## ОБЩИЕ ТРЕБОВАНИЯ.

* 1. Даты выполнения работ должны быть согласованы между Заказчиком и Исполнителей, при этом общая длительность работ не должна превышать 25 рабочих дней.
	2. Для проведения внутреннего тестирования Исполнителю будет предоставлен доступ к соответствующему сегменту ЛВС. Все работы должны выполняться на площадке Заказчика.
	3. Работы проводятся при наличии соглашения о конфиденциальности между Исполнителем и Заказчиком работ.
	4. Исполнитель должен предпринимать все разумные меры предосторожности, чтобы при оказании услуг не нарушать нормальную работу Информационной Системы Заказчика.

## ТРЕБОВАНИЯ К ОКАЗЫВАЕМЫМ УСЛУГАМ.

* 1. Целью тестирования на проникновение является получение привилегий в критических компонентах системы. Поиск, ручная верификация и эксплуатация уязвимостей должны осуществляться в объемах, необходимых для обнаружения наиболее серьезных уязвимостей и для выявления хотя бы одного вектора атаки с целью получения доступа к таким компонентам.
	2. В рамках тестирования на Исполнитель должен осуществить:
	+ перехват и анализ сетевого трафика (проводится по согласованию с Заказчиком, при целесообразности проведения работы в рамках имеющейся инфраструктуры);
	+ инструментальное сканирование узлов, доступных из текущего сегмента ЛВС;
	+ идентификацию уязвимостей инструментальными и ручными методами (в том числе для внутренних веб-приложений);
	+ подбор паролей (по согласованию с Заказчиком);
	+ эксплуатацию наиболее критических уязвимостей с целью выхода за границы текущего сегмента сети и дальнейшего развития атаки вплоть до получения доступа к целевым компонентам.
	1. В рамках внутреннего тестирования на проникновение должны использоваться методы и средства, позволяющие идентифицировать следующие классы уязвимостей:
	+ ошибки в настройке системы виртуализации;
	+ ошибки доступа к базам данных;
	+ использование открытых или недостаточно защищенных протоколов передачи данных;
	+ программные уязвимости сетевых служб и приложений, в доступных внутреннему нарушителю компонентах системы;
	+ ошибки в реализации механизмов аутентификации пользователей;
	+ ошибки в реализации механизмов авторизации и разграничения доступа;
	+ уязвимости веб-приложений (в том числе внедрение операторов SQL, выполнение команд операционной системы и т.п.);
	+ раскрытие конфиденциальной информации, хранение важных данных в незащищенном или недостаточно защищенном виде;
	+ ошибки в настройке операционных систем, веб-серверов, систем управления базами данных и других компонентов инфраструктуры;
	+ недостатки парольной политики.

Данный этап заканчивается получением доступа с максимальными привилегиями в Системе и получения доступа к целевым ресурсам.

## ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ.

* 1. Вся отчетная документация предоставляется по форме Исполнителя.
	2. По результатам всех этапов Исполнителем должен быть подготовлен «Отчет о результатах комплексного тестирования», содержащий:
	+ общие сведения о проведенном тестировании на проникновение;
	+ средства и методы тестирования;
	+ результаты проведенных проверок;
	+ оценку состояния защищенности информационной системы Заказчика как с точки зрения потенциальных векторов проникновения, так и с точки зрения используемых механизмов защиты;
	+ перечень и описание существующих угроз;
	+ графическое отображение всех выявленных векторов атак с оценкой сложности их реализации;
	+ выводы по анализу уязвимостей в веб-приложении и методам их нейтрализации;
	+ описание хода работ, выявленных уязвимостей, ранжирование их по степени потенциальной опасности, вероятности их использования, описание последствий реализации выявленных уязвимостей;
	+ перечень скомпрометированных в рамках работ компонентов Системы;
	+ рекомендации по устранению выявленных уязвимостей, в том числе рекомендации по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения;
	+ результаты эксплуатации нескольких критически опасных уязвимостей, включая информацию о полученном уровне привилегий в Системе на различных этапах тестирования;
	+ рекомендации по опубликованию ИС и методам защиты, с учетом имеющихся у Заказчика программно-аппаратных комплексов.

## ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ РАБОТ

* 1. В приемке и контроле работ участвуют Заказчик и Исполнитель.
	2. Приемка работ включает в себя анализ и согласование отчетной документации.
	3. Контроль и приемка разработанной документации осуществляются на основании данного технического задания, при этом проводится проверка полноты документации и соответствия техническому заданию.
	4. Максимальный срок со дня получения документации Заказчиком для отправки Исполнителю уведомления о её согласовании либо мотивированного отказа составляет 15 дней.
	5. В случае мотивированного отказа составляется акт с перечнем необходимых доработок.
	6. В составлении перечня замечаний и доработок со стороны Заказчика должны принимать участие квалифицированные специалисты, имеющие опыт и знания в вопросах информационной безопасности.
	7. В случае получения мотивированного отказа Исполнитель в течение не более 15 рабочих дней со дня получения мотивированного отказа производит устранение замечаний и передает Заказчику скорректированную в соответствии с замечаниями документацию совместно с отчетом об устранении замечаний для утверждения работ Заказчиком.
	8. Факт выполнения работ оформляется актом сдачи-приемки работ.

## ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ

* 1. Исполнитель должен иметь:
	+ подтвержденный опыт работы в области оказания услуг информационной безопасности не менее пяти лет;
	+ Опыт реализации проектов, касающихся поиска уязвимостей в виртуальной инфраструктуре, программном коде, веб-приложениях;
	+ Наличие представительства в г. Москва или Московской области;
	+ Иметь все необходимые действующие лицензии на оказание предлагаемых услуг;
	1. Преимуществом Исполнителя будет считаться наличие следующих сертификатов:
	+ OSCP (Offensive Security Certified Professional);
	+ OSCE (Offensive Security Certified Expert);
	+ GPEN(GIAC Penetration Tester).

## ТЕХНИЧЕСКОЕ ПРЕДЛОЖЕНИЕ

* 1. Техническое предложение должно включать в себя:
	+ Копии сертификатов OSCP, OS СЕ, GPEN (при наличии);
	+ Согласие компании выполнять работы по контракту согласно данному ТЗ;
	+ Согласие подписать договор по форме стандартного договора КТК (рассматривается как плюс);
	+ Иная информация в соответствии с условиями данного Технического задания.

## КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ

* 1. Предоставляемое Исполнителем коммерческое предложение должно содержать следующую информацию:
	+ Стоимость работ по техническому заданию;
	+ Срок работ по каждому из этапов;
	+ Условия оплаты (предпочтение отдается пост оплате);
	+ Дополнительные коммерческие преимущества, которые могут быть предоставлены Заказчику.
	1. СРОК ДЕЙСТВИЯ ПРЕДЛОЖЕНИЯ ИСПОЛНИТЕЛЯ ДОЛЖЕН СОСТАВЛЯТЬ НЕ МЕНЕЕ 3 МЕСЯЦЕВ.