|  |
| --- |
|  |
|  |
|  |

|  |  |
| --- | --- |
|  |  |

**Задание на работы по тестированию ИТ-инфраструктуры АО РНПК на проникновение из сети Интернет**

Содержание

[Общие сведения 3](#_Toc173336379)

[1 Цели и задачи работ 3](#_Toc173336380)

[2 Методология проведения работ 3](#_Toc173336381)

[3 Требования к модели нарушителя 3](#_Toc173336382)

[4 Требования к составу и содержанию работ 4](#_Toc173336383)

[4.1 Внешний тест на проникновение 4](#_Toc173336384)

[5 Требования к условиям выполнения работ 5](#_Toc173336385)

[6 Требования к отчетной документации 6](#_Toc173336386)

[6.1 Внешний тест на проникновение 6](#_Toc173336387)

[7 Требования к Исполнителю 6](#_Toc173336388)

#  Общие сведения

Заказчиком работ является АО Российская Национальная Перестраховочная Компания (далее «Заказчик»).

Наименование работ: Тестирование ИТ-инфраструктуры АО РНПК на проникновение из сети Интернет.

Основание проведения работ: положение Банка России от 20 апреля 2021 г. № 757 - П.

# Цели и задачи работ

Целью проведения работ является выявление уязвимостей, влияющих на уровень защищенности, возможность эксплуатации этих уязвимостей, и выработка рекомендаций по их устранению и повышению уровня защищенности объекта тестирования.

Задачами, решаемыми в ходе проведения работ, являются:

* анализ защищенности объектов тестирования;
* выявление в объекте тестирования уязвимостей и проверка возможности их эксплуатации для осуществления несанкционированных действий, направленных на нарушение конфиденциальности, целостности и доступности обрабатываемой информации;
* разработка рекомендаций по устранению выявленных уязвимостей, повышению уровня защищенности объекта тестирования по результатам проведённых работ.

# Методология проведения работ

Работы по тестированию на проникновение должны проводиться в соответствии с требованиями стандартов Open Source Security Testing Methodology Manual (OSSTMM), Penetration Testing Execution Standard (PTES) и Common Vulnerability Scoring System (CVSS).

# Требования к модели нарушителя

Все действия должны выполняться специалистами Исполнителя, находящимися в тех же условиях, что и потенциальный нарушитель. В рамках выполнения работ следует рассматривать следующий тип нарушителя:

* Внешний нарушитель, действующий со стороны сети Интернет, не имеющий логических прав в ИТ-инфраструктуре Заказчика, не обладающий сведениями о ИТ-инфраструктуре Заказчика и не обладающий информацией о работниках Заказчика (внутренние адреса электронной почты, внутренние идентификаторы в ИТ-инфраструктуре Заказчика). Данная модель нарушителя применятся на этапе «Внешний тест на проникновение».

# Требования к составу и содержанию работ

«Тестирование на проникновение» необходимо выполнять в один этап (см. Табл. 2).

Табл. 2. Состав и содержание работ

| **№** | **Наименование этапа** | **Состав работ** | **Длительность, раб. дней** |
| --- | --- | --- | --- |
| 1 | Внешний тест на проникновение | * Сбор информации
* Определение портов и сервисов
* Выявление недостатков и уязвимостей
* Анализ полученных результатов и выработка рекомендаций
* Разработка отчетной документации
* Разработка и согласование сценариев учебных атак
* Проведение учебных атак
* Анализ полученных результатов и выработка рекомендаций
* Разработка отчетной документации
 | 20 |

Длительность выполнения работ не включает время согласования итоговой отчетной документации с Заказчиком.

## Внешний тест на проникновение

При проведении работ на данном этапе должны быть выполнены следующие действия:

* сбор публично доступной информации об исследуемых ресурсах (используемые почтовые адреса, доменные имена, IP-адреса и др.) из различных источников (поисковые системы, регистраторы доменов, DNS-серверы, официальный сайт и др.);
* инструментальное определение открытых портов, сетевых сервисов, версий прикладного программного обеспечения (далее – ПО) и операционных систем (далее – ОС);
* выявление недостатков и уязвимостей на ресурсах внешнего сетевого периметра ИТ-инфраструктуры Заказчика, эксплуатация которых может привести к компрометации системы или может быть использована для получения неавторизованного доступа к конфиденциальным данным;
* выявление недостатков и уязвимостей веб-приложений, доступных из сети Интернет, с учетом статистики и рекомендаций OWASP Top 10[[1]](#footnote-1)
* разработка векторов учебных атак на основе полученной информации при проведении работ на предыдущих этапах;
* попытки эксплуатации выявленных уязвимостей с целями:
* согласование векторов эксплуатации и проведение попыток эксплуатации с целью компрометации целевых систем;
* анализ полученной информации, оценка влияния выявленных уязвимостей на защищаемую информацию, категорирование уязвимостей;
* выработка мер по устранению выявленных уязвимостей и/или снижению их уровня риска.

В рамках данных работ исследованию подлежат 13 IP-адресов. Точный список адресов должен быть предоставлен Заказчиком после подписания договора и до начала проведения работ.

# Требования к условиям выполнения работ

До начала проведения работ Исполнитель получает точную информацию об объектах исследования:

* список IP-адресов целевых систем;
* список доменных имен целевых систем

Также до начала проведения работ Исполнитель согласует с Заказчиком следующие детали:

* модель (модели) злоумышленника, применяемые на данных работах;
* сценарии проведения учебных атак;
* временные интервалы проведения активных работ;
* порядок взаимодействия с контактным лицом Заказчика;
* порядок и частоту предоставления обратной связи о ходе работ контактному лицу Заказчика.

# Требования к отчетной документации

По результатам всех этапов должен быть разработан документ, содержащий в себе объективную и независимую оценку состояния защищенности исследуемых систем, обобщенное резюме по результатам проведенных работ, а также детальное описание результатов по каждому этапу с рекомендациями по устранению выявленных уязвимостей и повышению уровня защищенности исследуемых систем.

## Внешний тест на проникновение

Раздел по результатам внешнего тестирования на проникновение должен содержать:

* общие сведения о проведенном внешнем тестировании на проникновение;
* краткие выводы по анализу выявленных уязвимостей и методам их нейтрализации;
* результаты проведенных проверок;
* выявленные в ходе проведения работ уязвимости и недостатки;
* степень критичности выявленных уязвимостей и недостатков;
* фактические доказательства успешности/не успешности выполненных действий (снимки экранов, вывод используемого ПО, полученная информация);
* рекомендации по устранению выявленных уязвимостей и/или снижению риска их эксплуатации.

# Требования к Исполнителю

* Профильной деятельностью Исполнителя должно являться оказание услуг по оценке уровня защищенности и тестированию на проникновение. (Участник предоставляет договоры с актами, за последние 5 лет, минимум 3 договора).
* Исполнитель должен иметь лицензии ФСТЭК России на деятельность
по технической защите конфиденциальной информации.
1. <https://owasp.org/> - проект OWASP Top 10, официальный сайт [↑](#footnote-ref-1)