

**Техническое задание на оказание услуг по
проведению теста на проникновение и анализу уязвимостей информационной безопасности
объектов информационной инфраструктуры
АО БАНК «СНГБ»**

Срок предоставления ТКП	13.08.2021
Адрес направления ТКП	obit@sngb.ru
Контакты	+7 (3462) 39-88-88 доб. 2181

1. Общие сведения

Целью предлагаемой услуги является выявление существующих уязвимых мест объектов информационной инфраструктуры АО БАНК «СНГБ» (далее - Системы) и получение объективной и независимой оценки ее текущего уровня защищенности. Идентификация уязвимостей и рисков, которые с ними связаны, является важнейшим элементом обеспечения информационной безопасности и может послужить основой для формирования адекватной и всеобъемлющей программы мероприятий по повышению уровня защищенности Системы, что в свою очередь ведет к снижению соответствующих операционных, финансовых и репутационных рисков.

Для достижения указанной цели Исполнитель обеспечивает анализ защищенности Системы путем проведения внешнего тестирования на проникновение. Предлагаемые услуги включают в себя решение следующих задач:

- выявление недостатков в применяемых Заказчиком мерах информационной безопасности, и оценка возможности их использования нарушителем;
- практическая демонстрация возможности использования уязвимостей (на примере наиболее критических);
- получение на основе объективных свидетельств комплексной оценки текущего уровня защищенности Системы;
- выработка рекомендаций по устранению;
- проверка корректности устранения уязвимостей, выявленных в ходе проведенных работ в АО БАНК «СНГБ».

Общее число IP адресов на которых опубликованы объекты информационной инфраструктуры Заказчика: 51;

2. Дополнительные условия:

- 1) Исполнитель не имеет права привлекать внешних исполнителей.
- 2) Обязательное наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации №79.
- 3) Опыт работы с банками не менее 3 (трех) лет, просим участников подтвердить рекомендательными письмами, желательно по направлению Pentest.
- 4) Условия по оплате, с указанием отдельно стоимости НДС: 100% оплата поэтапная по факту выполнения работ каждого этапа. Стоимость командировочных расходов указывается отдельной позицией. Необходимо предоставить стоимость по каждому этапу с указанием объема и формы предоставления услуги.
- 5) Обязательное указание в ТКП сроков и стоимости по каждому этапу работ.

- 6) Отсутствие Исполнителя в санкционном списке: <https://sanctionssearch.ofac.treas.gov/>.
- 7) Срок исполнения обязательств по работам, указанным в п.4-5: не позднее 10.09.2021г.
Срок исполнения обязательств по работам, указанным в п.6: не позднее 20.10.2021г.
- 8) По окончании каждого этапа работ Исполнитель предоставляет отчет с результатами проделанной работы.
- 9) Исполнитель не имеет права привлекать внешних исполнителей.
- 10) Исполнитель должен иметь возможность работать в системе электронного документа «Диадок» или совместимой с ней.

3. Методика проведения работ

Работы проводятся методом черного ящика на в качестве основы используются стандарты:

- NIST SP800-115 «Technical Guide to Information Security Testing and Assessment»
- OWASP Foundation «OWASP Testing Guide»
- Penetration Testing Guidance (PCI Data Security Standard)

Все операции выполняются специалистами Исполнителя, находящимися в тех же условиях, что и потенциальный нарушитель. В рамках выполнения работ рассматриваются следующие типы нарушителя:

- Высококвалифицированный внешний нарушитель, действующий со стороны сети Интернет, который не имеет привилегий в Системе и реализует атаки, направленные на получение доступа к одному или несколькими узлам ЛВС Заказчика с развитием атаки на внутренние компоненты Системы.

При проведении тестирования на проникновение специалисты Исполнителя не располагают какими-либо предварительными данными об информационных системах Заказчика и используемой инфраструктуре. Анализ защищенности направлен на выявление недостатков, для использования которых существуют методики и инструментальные средства, доступные в свободной продаже, в открытых источниках и в специализированных источниках ограниченного доступа.

Для поиска и эксплуатации уязвимостей корпоративных веб-приложений используется комбинация инструментальных методов анализа и ручного исследования компонентов Системы экспертами. Для каждого из этапов специалисты Заказчика должны обеспечить доступность всех исследуемых компонентов Системы, а также выделить сотрудника, ответственного за взаимодействие со специалистами Исполнителя. Обязательным условием является согласование Исполнителем временных рамок при проведении работ с Заказчиком. Работы по тестированию на проникновение осуществляются в период времени, согласованный с Заказчиком. Все действия Исполнителя, которые могут привести к нарушению функционирования Системы или другим негативным последствиям для Заказчика, согласовываются с представителем Заказчика. После завершения работ все средства проведения тестирования, применявшиеся в рамках работ, удаляются из Системы Заказчика.

При отсутствии успеха в преодолении защиты соответствующий этап завершается после исчерпания специалистами Исполнителя всех потенциально применимых в рамках данного этапа методов проведения атаки. В любом случае Заказчику предоставляется полная информация о действиях, выполнявшихся в ходе анализа защищенности, применявшихся методах атаки, выявленных недостатках и причинах, результатах использования наиболее серьезных недостатков и объективные свидетельства, подтверждающие как наличие недостатков, так и результаты их использования специалистами Исполнителя.

4. Тестирование на проникновение (Черный ящик)

4.1. **Внешнее тестирование на проникновение** Анализ защищенности сетевого периметра включает в себя проверки, направленные на поиск и эксплуатацию уязвимостей на сетевом и прикладном уровнях. Работы осуществляются в следующем порядке:

- 4.1.1. **Получение предварительной информации о сетевом периметре** на основе источников информации, доступных потенциальному нарушителю (поисковые системы, новости, конференции и т.п.). На этом этапе составляется перечень идентифицированных сетей и доменных имен, принадлежащих Заказчику. Заказчик добавляет или исключает из списка, предоставленного Исполнителем, тестируемые сети и сетевые объекты.
- 4.1.2. **Сканирование узлов сетевого периметра**, определение типов устройств, операционных систем, приложений по реакции на внешнее воздействие. Составляется перечень идентифицированных сервисов на узлах, вошедших в границы проведения работ. В случае наличия значительного количества узлов и сервисов в границах проведения работ в итоговом отчете указываются только общие данные о типах и количестве обнаруженных сервисов, при этом полная информация (результаты сканирования) может быть предоставлена Заказчику по запросу.
- 4.1.3. **Идентификация уязвимостей сетевых служб**. Осуществляется анализ данных, полученных в результате сканирования узлов сетевого периметра. Выявляются факты использования сетевых служб на сетевом периметре, доступ к которым со стороны внешнего нарушителя может привести к компрометации систем, перехвату чувствительных данных, реализации атак на отказ в обслуживании и других угроз.
- 4.1.4. **Анализ защищенности сервисов сетевой инфраструктуры (DNS, электронной почты и т.д.)**. Устанавливается наличие или отсутствие уязвимостей инфраструктурных служб и приложений (при использовании соответствующих служб).
- 4.1.5. **Инструментальное обследование** с использованием системы контроля защищенности и инструментальных средств. Выявляются уязвимости сетевых служб и узлов, которые могут быть найдены автоматизированными методами, в границах проведения работ.
- 4.1.6. **Анализ первичных результатов, ручная верификация уязвимостей**. Подтверждается наличие уязвимостей, выявленных в ходе инструментального сканирования, исключаются уязвимости, являющиеся результатом ложного срабатывания автоматизированных средств анализа защищенности (в случае возможности и целесообразности подобной верификации).
- 4.1.7. **Анализ защищенности внешних корпоративных веб-приложений** методом черного ящика, то есть со стороны нарушителя, не обладающего никакими сведениями и логическим доступом к корпоративным веб-приложениям. Цель анализа защищенности веб-приложений – выявление уязвимостей, которые могут быть использованы для преодоления сетевого периметра и дальнейшего развития атаки во внутреннюю сеть. Анализ защищенности веб-приложений осуществляется в объемах, необходимых для обнаружения наиболее серьезных уязвимостей и для выявления хотя бы одного вектора атаки, позволяющего получить доступ к критичным ресурсам.
- 4.1.8. **Эксплуатация наиболее критичных уязвимостей**, с целью преодоления сетевого периметра. Устанавливается возможность или невозможность преодоления специалистами Исполнителя сетевого периметра. В случае успешной атаки специалисты

Исполнителя реализуют обход технических средств защиты, получают доступ к ресурсам внутренней сети, с последующим развитием атаки в разных направлениях до получения доступа конфиденциальной информации.

4.1.9. Выявление возможных мер противодействия со стороны специалистов Заказчика, а также реакции систем обнаружения и предотвращения вторжений. Собирается информация о зафиксированных инцидентах, реакции систем обнаружения и предотвращения вторжений, а также реакции персонала на действия Исполнителя.

4.2. В рамках анализа защищенности сетевого периметра используются методы и средства, позволяющие идентифицировать следующие классы уязвимостей:

- ошибки в настройке телекоммуникационного оборудования сетевого периметра;
- ошибки межсетевого экранирования;
- ошибки в организации удаленного доступа;
- программные уязвимости сетевых служб и приложений, в доступных внешнему нарушителю компонентах Системы;
- ошибки в реализации механизмов аутентификации пользователей веб-приложений;
- ошибки в реализации механизмов авторизации и разграничения доступа веб-приложений;
- отсутствие или недостаточность механизмов противодействия атакам на пользователей веб-приложений (межсайтовое выполнение сценариев, подделка запросов и т.п.);
- уязвимости, приводящие к нарушению логики функционирования веб-приложений (внедрение операторов SQL, выполнение команд операционной системы и т.п.);
- раскрытие конфиденциальной информации, в том числе – раскрытие информации об особенностях реализации функций приложений, используемых программных компонентах и прочей информации, облегчающей нарушителю организацию атаки;
- ошибки в реализации доступных пользователю функций веб-приложений;
- ошибки в настройке операционной системы, веб-сервера, системы управления контентом и прочих компонентов веб-приложений.

Для поиска и эксплуатации уязвимостей используется комбинация инструментальных методов анализа и ручного исследования компонентов Системы экспертами.

5. Проверка корректности устранения выявленных уязвимостей

Данная услуга подразумевает проверку корректности устранения уязвимостей, обнаруженных по результатам внешнего и внутреннего тестирований на проникновение. Специалисты Исполнителя оценивают степень эффективности предпринятых Заказчиком мер по устранению уязвимостей. Проверка проводится для векторов атаки, выявленных в результате соответствующих этапов анализа защищенности.

Исполнитель подготавливает экспертное заключение по результатам перепроверки выявленных уязвимостей и несоответствий.

6. Результат оказания услуг

По результатам проекта Заказчик получает объективную и независимую оценку защищенности Системы, которая позволяет определить, насколько эффективны на практике применяемые меры защиты информации.

По окончании комплексного тестирования на проникновение Заказчику предоставляется отчетные документы, которые содержат:

- общие сведения о проведенном тестировании на проникновение;
- результаты проведенных проверок и перепроверок;
- выводы (как развернутые технические, так и более краткие для руководства), в которых дается оценка состояния защищенности информационной системы Заказчика;
- выводы по анализу уязвимостей в веб-приложениях и методах 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 компонент 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 и т.п.;
- результаты эксплуатации нескольких критичных уязвимостей, включая информацию о полученном уровне привилегий в Системе на различных этапах тестирования.