**Техническое задание на оказание услуг по проведению теста на проникновение в корпоративную информационную систему АО БАНК «СНГБ»**

**Срок предоставления ТКП: 15.07.2020г.**

**1. Общие сведения**

Целью предлагаемой услуги является выявление существующих уязвимых мест 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 основной 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, оценки осведомленности пользователей Системы в вопросах информационной безопасности. 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);
- оценку текущего уровня осведомленности пользователей Заказчика в вопросах обеспечения информационной безопасности;
- получение на основе объективных свидетельств комплексной оценки текущего уровня защищенности Системы;
- выработка рекомендаций по устранению;
- проверка корректности устранения уязвимостей, выявленных входе проведенных работ в АО БАНК «СНГБ» на всех этапах.

**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 10.09.2020г.
   Срок исполнения обязательств по работам, указанным в п.6: не позднее 20.10.2020г.
8) По окончании каждого этапа работ Исполнитель предоставляет отчет с результатами проделанной работы.

## 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.

Оценка осведомленности пользователей Системы в вопросах информационной безопасности производится с помощью телефонного обзвона и рассылки фокус-группе электронного сообщения с содержанием, побуждающим пользователя ознакомиться с вложенным в сообщение электронным документом (сценарий 1) и/или перейти по указанной в письме гиперссылке с предоставление учетных данных (сценарий 2). При открытии документа производится автоматическая попытка эксплуатации одной из распространенных уязвимостей в программном обеспечении, предназначенном для обработки подобного типа вложений. Эксплуатация уязвимости не приводит к уничтожению, блокированию, модификации или копированию информации, обрабатываемой на рабочем месте пользователя, или к нарушению функционирования рабочего места пользователя. Фиксирование фактов открытия документов и перехода по ссылкам осуществляется в том числе с помощью полученных уникальных DNS-запросов.

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.

Параметры фокус группы с помощью телефонного обзвона – не более 20 номеров.

Параметры фокус группы с помощью рассылки электронного сообщения – не более 200 электронных адресов.

## 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:

4.2. ***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.

4.3. ***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.

4.4. ***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.

4.5. ***Анализ защищенности сервисов сетевой инфраструктуры (DNS, электронной почты и т.д.).*** Устанавливается наличие или отсутствие уязвимостей инфраструктурных служб и приложений (при использовании соответствующих служб).

4.6. ***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.

4.7. ***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).

4.8. ***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.

4.9. ***Эксплуатация наиболее критичных уязвимостей***, с целью преодоления сетевого периметра. Устанавливается возможность или невозможность преодоления специалистами Исполнителя сетевого периметра. В случае успешной атаки специалисты Исполнителя получают доступ к ресурсам внутренней сети.

4.10. ***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.

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. Оценка осведомленности сотрудников в вопросах ИБ

В ходе данного этапа оценивается эффективность предпринимаемых Заказчиком мер по повышению осведомленности сотрудников в вопросах информационной безопасности. Для оценки проводится ряд тестов, эмулирующих распространенные сетевые атаки с использованием методов социальной инженерии.

***5.1. Атаки с использованием методов социальной инженерии используют комбинацию двух факторов:***

- наличие на рабочем месте пользователя локально эксплуатируемой уязвимости в одном или нескольких популярных приложениях (браузеры, Microsoft Office, Adobe Flash и т.п.);
- свойственное пользователям отсутствие разумной осторожности при обращении с электронными сообщениями.

***5.2. Для взаимодействия с тестируемыми сотрудниками используются следующие каналы:***

- корпоративные адреса электронной почты;
- телефонные звонки.

***Тестирование производится в следующем порядке:***

- сбор информации о сотрудниках Заказчика в общедоступных источниках, в том числе - получение списка адресов электронной почты и иных контактных данных сотрудников, сведений об их интересах и т.п.;
- формирование и согласование с Заказчиком перечня проводимых проверок и перечня тестируемых пользователей (фокус-группы);
- разработка специального программного обеспечения для проведения тестов и его адаптация под особенности системы обеспечения информационной безопасности Заказчика.
- проведение тестов и обработка их результатов.

Тестирование производится с помощью рассылки фокус-группе электронного сообщения с содержанием, побуждающим пользователя ознакомиться с вложенным в сообщение электронным документом или перейти по указанной в письме гиперссылке.

При открытии документа производится автоматическая попытка эксплуатации одной из распространенных уязвимостей в программном обеспечении, предназначенном для обработки подобного типа вложений. Результатом эксплуатации становится сбор и передача Исполнителю сведений, позволяющих идентифицировать пользователя и использованную уязвимость. Эксплуатация уязвимости не приводит к уничтожению, блокированию, модификации или копированию информации, обрабатываемой на рабочем месте пользователя, или к нарушению функционирования рабочего места пользователя.

Отдельно фиксируются попытки пользователей фокус-группы вступить в общение с отправителем сообщения, их реакция на получение сообщения и иные обстоятельства, существенные для оценки осведомленности.

В случае проверок с использованием телефонных звонков, подобные проверки проводятся в отношении согласованного перечня сотрудников (фокус-группы), либо в отношении сотрудников, вступивших в общение с Исполнителем в рамках других проверок.

Результатом оценки осведомленности является первичная информация о результатах тестов и статистическая оценка количества сотрудников, в отношении которых может быть проведена успешная атака с использованием методов социальной инженерии.

**6. Проверка корректности устранения 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.

**7. 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 документы, которые содержат:

- общие сведения о проведенном тестировании на проникновение;
- результаты проведенных проверок;
- 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.

По окончании оценки осведомленности пользователей Системы в вопросах информационной безопасности Заказчику предоставляется документ с результатами оценки осведомленности пользователей в вопросах информационной безопасности, который содержит:

- оценку эффективности программы повышения осведомленности;
- статистику по каждому из типов атаки и действиям пользователей.