

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ «Анализ защищенности»

1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГ

- 1.1. В рамках оказания Услуги проводится анализ защищенности инфраструктуры Заказчика, состоящей из следующих компонентов:
- сервисы, принадлежащие Заказчику, доступные из сети Интернет;
 - веб-приложения, включенные в границы оказания Услуг.
- 1.2. В рамках оказания Услуг выполняется внутреннее и внешнее тестирование на проникновение информационных объектов и их компонентов (далее – Система или Системы), которые указываются в спецификации (Приложение № 13.А. к Договору, далее – Спецификация).
- 1.3. Услуга предоставляется Исполнителем в сотрудничестве с ООО «Безопасная информационная среда» (ООО «БИЗон», далее – «Партнер»). Заказчик является конечным потребителем оказываемой Услуги.

2. УСЛОВИЯ И ПОРЯДОК ОКАЗАНИЯ УСЛУГ

- 2.1. Услуги оказываются по методике Партнера в соответствии со следующими международными стандартами и практиками:
- Penetration Testing Execution Standard (PTES);
 - NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment;
 - Open Source Security Testing Methodology Manual (OSSTMM);
 - Information Systems Security Assessment Framework (ISSAF);
 - Web Application Security Consortium (WASC) Threat Classification;
 - Open Web Application Security Project (OWASP) Testing Guide;
 - Payment Card Industry Data Security Standard (PCI DSS);
 - Стандарты Center for Internet Security (CIS);
 - Common Vulnerability Scoring System (CVSS).
- 2.2. Специалисты Партнера оказывают Услуг в соответствии со следующими этапами:
- 2.2.1. **Поиск новых сервисов на внешнем периметре:**
- диапазоны IP-адресов;
 - доменные имена второго и третьего уровня;
 - сетевые публичные сервисы и системы;
 - почтовые серверы;
 - DNS-серверы;
 - сбор сведений о сотрудниках Заказчика и другой дополнительной информации, представляющей интерес для потенциального злоумышленника.
- 2.2.2. **Автоматизированное сканирование внешнего периметра Заказчика:**
- определение типов используемых устройств;
 - определение используемых операционных систем;
 - сканирование портов и обнаружение связанных сервисов;
 - идентификация уязвимостей сетевых служб и приложений;
 - анализ полученных результатов сканирования;
 - выявление ложных срабатываний автоматизированных систем сканирования;
 - тестирование обнаруженных уязвимостей на возможность их эксплуатации в инфраструктуре Заказчика.
- 2.2.3. **Мониторинг и экспертная оценка уязвимостей в используемых Заказчиком сервисах, в которых произошли изменения:**
- идентификация уязвимостей в публичных сервисах и системах;
 - эксплуатация обнаруженных уязвимостей для определения критичности;
 - экспертная оценка возможной эксплуатации и критичности уязвимостей.
- 2.2.4. **Автоматизированное сканирование веб-приложений:**
- применение инструментов автоматизированного анализа;
 - обнаружение ошибок исполнения;
 - анализ защищенности канала передачи данных;
 - тестирование механизма аутентификации;
 - тестирование механизма разграничения доступа (авторизации);
 - тестирование валидации пользовательских данных;

- поиск возможных векторов атак на клиентов приложения.

2.3. План оказания Услуг.

Услуги оказываются в соответствии со следующими планами:

Табл. 1. План оказания Услуг по внешнему тестированию на проникновение

№	Вид услуг	Перечень услуг	Необходимые ресурсы на стороне Заказчика
1	Сбор и анализ текущей документации об объекте тестирования	Анализ архитектуры Системы, уточнение типа злоумышленника, описание точек входа в Систему, изучение особенностей конфигурации, разработка векторов атаки. Сбор подробных сведений о структуре компании Партнера и информационных сервисах Партнера из открытых источников.	Документация и детальное описание компонентов Системы, первичные сведения о целевой системе: IP-адрес, домен и др.
2	Проведение внешнего тестирования на проникновение	Поиск векторов компрометации сервисов и систем; попытки получить несанкционированный доступ к критической информации для внешнего тестирования.	Список IP-адресов для внешнего тестирования. Доступ во внутренний сегмент сети
3	Подготовка отчета	Подготовка и согласование итогового отчета по результатам оказанных услуг в соответствии с формой, описанной в методике Исполнителя.	Участие уполномоченных согласующих Партнера и Исполнителя
4	Гарантийная поддержка: проверка факта устранения обнаруженных уязвимостей	Специалисты Исполнителя производят проверку исправления ранее обнаруженных уязвимостей. По результатам оказанных Услуг информация о статусе каждой из уязвимостей фиксируется в итоговом отчете.	Отчёт Партнера об устранении уязвимостей, обнаруженных Исполнителем.

Табл. 2. План оказания Услуг по внутреннему тестированию на проникновение

№	Вид услуг	Перечень услуг	Необходимые ресурсы на стороне Заказчика
1	Сбор и анализ текущей документации об объекте тестирования	Активный и пассивный сбор данных о Внутренней инфраструктуре (используемые технологии, архитектура и оборудование сети), а также первичная идентификация уязвимостей в сетевых службах и приложениях.	Доступ во внутренний сегмент сети
2	Проведение внутреннего тестирования на проникновение	Поиск возможности получения НСД к конфиденциальным данным и защищенным сегментам сети при наличии требуемого сетевого доступа, но в отсутствие достаточных привилегий в операционной системе, сервисах и приложениях. Эксплуатация обнаруженных уязвимостей и проверка наиболее вероятных векторов атаки, позволяющих получить НСД к конфиденциальным данным, защищенным сегментам сети или даже полный контроль над IT-инфраструктурой.	Необходимые привилегии во Внутренней инфраструктуре в соответствии с выбранной моделью злоумышленника
3	Подготовка отчета	Подготовка и согласование итогового отчета по результатам оказанных услуг в соответствии с формой, описанной в методике Исполнителя.	Участие уполномоченных согласующих Партнера и Исполнителя
4	Гарантийная поддержка: проверка факта устранения обнаруженных уязвимостей	Специалисты Исполнителя производят проверку исправления ранее обнаруженных уязвимостей. По результатам оказанных Услуг информация о статусе каждой из уязвимостей фиксируется в итоговом отчете.	Отчёт Партнера об устранении уязвимостей, обнаруженных Исполнителем.

2.3.1. Внутреннее тестирование на проникновение.

Тестирование на проникновение проводится с целью выявления уязвимостей Внутренней инфраструктуры Заказчика, а также получения объективной оценки ее текущего уровня защищенности. Достижение этих целей снижает вероятность наступления инцидента, вызванного действиями потенциального злоумышленника. Внутреннее тестирование на проникновение имитирует действия злоумышленника в соответствии с одной из моделей, приведенных ниже. Предполагается, что злоумышленник является высококвалифицированным специалистом, обладающим навыками, сопоставимыми с навыками Партнера.

Возможные модели злоумышленника (выбирается одно из значений)

Цель: получение финансовой или другой личной выгоды, а также нанесение любого вреда Заказчику или его клиентам.

Уровень квалификации: высококвалифицированный специалист, обладающий навыками, сравнимыми с навыками Партнера.

Привилегии:

- привилегии во внутренней сети отсутствуют;
- пользовательская учетная запись в домене;
- учетная запись типового АРМ.

Доступ к инфраструктуре:

- доступ в гостевой сегмент сети;
- доступ в пользовательский сегмент сети;
- доступ в выделенный сегмент сети.

В ходе оказания услуг Партнер имитирует процесс анализа Внутренней инфраструктуры потенциальным злоумышленником в соответствии с вышеописанной моделью. При этом действия, ведущие к возможности нанесения вреда Заказчику или его клиентам, Партнер выполняет исключительно по согласованию с Заказчиком.

2.3.2. **Внешнее тестирование на проникновение.**

В рамках внешнего тестирования на проникновение Партнер имитирует действия злоумышленника в соответствии с одной из моделей, приведенных в Таблице 3. Предполагается, что злоумышленник является высококвалифицированным специалистом, обладающим навыками, сопоставимыми с навыками Партнера. На основании данных, полученных от Заказчика, тестирование на проникновение проводится в соответствии с моделью злоумышленника А для Черного ящика, В для Серого ящика и С для Белого ящика.

Табл.3. Модель злоумышленника

Модель	Привилегии	Описание
A	Нет	Злоумышленник не имеет учетных данных в Системе, действуя из Интернета, не обладает базовыми знаниями о Системе Партнера, имеет опыт и навыки в использовании уязвимостей.
B	Учетные данные пользователя	Злоумышленник имеет минимальные привилегии в Системе, действуя из Интернета, имеет минимальные знания о Системе Партнера.
C	Права администратора	Злоумышленник обладает правами администратора во внешних службах Партнера.

2.4. **Объем Услуг.**

2.4.1. Внешнее тестирование на проникновение включает следующие этапы:

1. Сбор информации об объекте исследования:

- диапазоны IP-адресов;
- имена доменов и поддоменов;
- сетевые публичные сервисы и системы;
- почтовые сервера;
- DNS-сервера;
- средства защиты, используемые Заказчиком;
- информация о сотрудниках и другая дополнительная информация, представляющая интерес для потенциального злоумышленника.

2. Тестирование на проникновение и попытки компрометации публичных сервисов Заказчика:

- поиск уязвимостей в публичных сервисах и системах;
- эксплуатация обнаруженных уязвимостей и закрепление в скомпрометированных сервисах и системах;
- развитие атаки на внутреннюю сеть и попытками доступа к конфиденциальной информации.
- применение инструментов автоматизированного анализа защищенности

3. Подготовка итогового отчета:

- общая информация;
- экспертная оценка текущего уровня защищенности;
- перечень обнаруженных уязвимостей;
- общие рекомендации по повышению уровня защищенности;
- сценарий компрометации;
- подробная информация о найденных уязвимостях, включая подробное описание, уровень опасности, место обнаружения, пример эксплуатации и рекомендации по устранению.

2.4.2. Внутреннее тестирование на проникновение включает следующие этапы:

1. Сбор данных об объекте исследования:

- диапазоны IP-адресов;

- имена доменов и поддоменов;
 - сетевые протоколы, используемые в локальной сети;
 - сетевое оборудование;
 - почтовые сервера;
 - DNS-сервера;
 - компоненты сети;
 - средства защиты;
 - внешние системы, отраженные во внутренней сети;
 - типы и версии ОС;
 - типы и версии ПО;
 - типы и виды устройств.
2. **Тестирование на проникновение:**
- проверка возможности преодоления сетевого периметра;
 - поиск способов получения НСД к операционным системам, приложениям и службам (СУБД, веб-приложения и др.).
3. **Эксплуатация обнаруженных уязвимостей:**
- анализ уязвимостей рабочих станций пользователей, компонентов Внутренней инфраструктуры, сетевого оборудования и сетевых средств защиты;
 - моделирование атак на уровне приложений, сетевых сервисов и ОС с использованием специализированных средств, а также сведений об уязвимостях и ошибках конфигурации;
 - эскалация привилегий пользователя – проверка возможности получения прав администратора;
 - проверка возможности несанкционированного повышения привилегий в IT-сервисах авторизованными пользователями и получения доступа к закрытой информации;
 - проверка возможности компрометации публичных сервисов с целью получения доступа к конфиденциальной информации или информации ограниченного пользования;
 - проверка возможности получения доступа к контроллеру домена.
4. **Подготовка отчета:**
- общая информация;
 - экспертная оценка текущего уровня защищенности;
 - сценарий компрометации;
 - перечень обнаруженных уязвимостей;
 - общие рекомендации по повышению уровня защищенности;
 - подробная информация о найденных уязвимостях, включая подробное описание, уровень опасности, место обнаружения, пример эксплуатации и рекомендации по устранению.

2.5. **Ограничение ответственности при оказании Услуг.**

Партнер берет на себя обязательства предпринимать все разумные меры предосторожности, чтобы при оказании Услуг не нарушать нормальную работу компонентов сети Заказчика.

Партнер гарантирует соблюдение условий конфиденциальности исходных данных и/или сведений, относящихся к деятельности Заказчика, ставших известными специалистам Партнера в ходе оказания Услуг.

При обнаружении уязвимостей, которые могут повлиять на целостность/доступность/конфиденциальность систем Заказчика Партнер проводит предварительное согласование перед их эксплуатацией на целевой системе.

В случае возникновения внештатных ситуаций, а также при случае воздействия на доступность или производительность целевых систем, специалисты Партнера оповещают об этом Заказчика.

Соглашаясь с оказанием Услуг, Заказчик принимает на себя риск возможного наступления негативных последствий проверки. Учитывая, что часть проверок полностью имитирует атаки злоумышленников, Заказчик берет на себя урегулирование проблем, связанных с претензиями операторов связи или любых иных организаций и физических лиц к Партнеру.

Заказчик понимает, что в ходе проведения проверки может быть снижена доступность сервисов и приложений, и берет на себя урегулирование связанных с этим возможных проблем, а также обязуется не предъявлять претензий к Партнеру по данному факту. Заказчик не возражает против привлечения Партнером специалистов, квалификация которых позволяет им оказывать указанные виды Услуг.

3. ПОРЯДОК РАСЧЕТОВ И ТАРИФИКАЦИЯ

3.1. Стоимость оказываемых Услуг согласовывается Сторонами в Заказах Услуг и Спецификации на основании Тарифов, размер которых установлен в Приложении № 7.А. к Договору. Стоимость Услуги указывается за Отчётный период.

3.2. Оплата Услуг осуществляется Заказчиком в порядке, установленном Разделом 4 Договора.

4. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГАМ

- 4.1. Заказчик проинформирован и согласен с тем, что в отношении описанных в Приложении Услуг не применяются условия SLA Услуг – Приложения 2.0 и т. д., которые описывают уровни предоставления Услуг по Договору, компенсации за несоблюдение доступности Услуг, порядок обработки запросов Заказчика, а также иные связанные с оказанием Услуг вопросы.
- 4.2. Перед началом оказания Услуг Заказчик обязуется передать Исполнителю оригинал (-ы) подписанного (-ных) Авторизационного (-ных) письма (писем). Авторизационные письма составляются по форме Приложения № 13.Б. к Договору.
- 4.3. Заказчик обязуется получить все необходимые согласия на обработку персональных данных физических лиц, позволяющие Исполнителю оказывать Услуги, а также обеспечить надлежащую и безопасную их обработку при передаче Исполнителю.
- 4.4. Заказчик как оператор персональных данных обязуется после получения согласий на обработку персональных данных до их передачи Партнеру направить ему поручение на обработку персональных данных, составленное по форме согласно Приложению № 13.В. к Договору, на электронную почту info@bi.zone.
- 4.5. В случае выявления недочетов в итоговом отчете Заказчик должен удалить из отчета персональные данные и направить Исполнителю письмо по электронной почте с замечаниями для их устранения Партнером.
- 4.6. Стороны пришли к соглашению, что в случае отказа Заказчика от оказания Услуги по подписанному Заказу и Спецификации Заказчик обязуется оплатить Исполнителю стоимость таких Услуг в следующем размере и порядке:
- 4.6.1. Если заявка на расторжение соответствующей Спецификации направлена Заказчиком в адрес Исполнителя не позже 3 (трех) календарных месяцев с момента подписания соответствующей Спецификации, то Заказчик оплачивает Исполнителю стоимость Услуги, указанной в соответствующей Спецификации, в размере 1/4 (одной четвертой) от годовой стоимости Услуги, указанной в данной Спецификации.
- 4.6.2. Если заявка на расторжение соответствующей Спецификации направлена Заказчиком в адрес Исполнителя позже 3 (трех) календарных месяцев с момента подписания соответствующей Спецификации, но не превышает 6 (шести) календарных месяцев с момента подписания такой Спецификации, то Заказчик оплачивает Исполнителю стоимость Услуги, указанной в соответствующей Спецификации, в размере 1/2 (одной второй) от годовой стоимости Услуги, указанной в данной Спецификации.
- 4.6.3. Если заявка на расторжение соответствующей Спецификации направлена Заказчиком в адрес Исполнителя позже 6 (шести) календарных месяцев с момента подписания соответствующей Спецификации, то Заказчик оплачивает Исполнителю полную годовую стоимость Услуги, указанную в данной Спецификации.
- 4.6.4. Если заявка на расторжение соответствующей Спецификации на разовые услуги направлена Заказчиком в адрес Исполнителя не позже 1 (Одной) календарной недели с момента подписания соответствующей Спецификации, то Заказчик оплачивает Исполнителю стоимость услуг пропорционально общему количеству дней срока оказания Услуг, указанной в соответствующей Спецификации на разовые услуги.
- 4.6.5. Если заявка на расторжение соответствующей Спецификации на разовые услуги направлена Заказчиком в адрес Исполнителя позже 1 (Одной) календарной недели с момента подписания соответствующей Спецификации, то Заказчик оплачивает Исполнителю полную стоимость разовой Услуги, указанную в данной Спецификации.
- 4.7. Вне зависимости от основания расторжения Спецификации Стороны обязуются в течение 15 (Пятнадцати) рабочих дней с даты ее расторжения произвести полный взаиморасчет по обязательствам с подписанием акта сверки.
- 4.8. При расторжении Спецификации по соглашению Сторон Стороны обязуются урегулировать все взаимные требования, в т. ч. имущественные, при заключении соответствующего соглашения.
- 4.9. В случае расторжения Спецификации или одностороннего отказа Заказчика от исполнения Договора Партнер возвращает Заказчику все полученные документы и (или) материалы в течение 5 (Пяти) рабочих дней с момента расторжения соответствующей Спецификации/Договора.