Техническое задание

Проведение сертификационного аудита соответствия требованиям стандарта PCI DSS 4.0.1

## Состав Услуг

* 1. Предварительный аудит
     1. Сбор организационной и технической информации

Целью оказания услуг на данном этапе является оценка внесенных изменений в организационные процессы и технические системы, отвечающие за обеспечение информационной безопасности, за период времени, прошедший с момента проведения предыдущего сертификационного аудита.

На данном этапе оказываются следующие услуги:

* актуализация свидетельств соответствия;
* проверка внедрения и поддержания требуемых организационных мероприятий и технических систем;
* оценка соответствия внесенных изменений и существующих процессов требованиям стандарта;
* разработка Плана мероприятий с рекомендациями по устранению несоответствий.

Результатом оказания услуг является План мероприятий с рекомендациями по устранению несоответствий в случае их выявления.

* + 1. Оценка соответствия требованиям Стандарта

Целью данного этапа является определение текущего уровня соответствия требованиям Стандарта PCI DSS 4.0.1.

На данном этапе, на основе полученной ранее информации, выполняется анализ соответствия инфраструктуры Заказчика требованиям Стандарта PCI DSS 4.0.1, для чего оказываются следующие услуги:

* анализ структуры сети и сегментации;
* анализ конфигураций активного сетевого оборудования и существующих правил разграничения доступа;
* анализ используемых сетевых протоколов с точки зрения безопасности;
* анализ принятых в информационной системе политик безопасности;
* анализ процессов обработки данных платежных карт;
* и другие необходимые услуги.
  + 1. Разработка рекомендаций по приведению в соответствие требованиям Стандарта

При разработке рекомендаций по устранению выявленных несоответствий требованиям Стандарта PCI DSS учитываются следующие направления:

* уменьшение границ применимости требований Стандарта PCI DSS;
* изменение конфигураций существующих средств защиты;
* доработка существующей и разработка дополнительной документации в области обеспечения информационной безопасности;
* внедрение и настройка дополнительных средств защиты информации (как общедоступных, так и коммерческих решений);

Результатом оказания услуг на данном этапе является План реализации организационных и технических мероприятий, выполнение которых позволит обеспечить выполнение всех требований Стандарта PCI DSS 4.0.1.

* 1. Тестирование на проникновение

Предлагаемые услуги по моделированию действий потенциального злоумышленника разделяются на два типа:

* Внешнее тестирование на проникновение. Осуществляется из сети Интернет и представляет собой выявление и анализ технических уязвимостей информационной системы внешнего периметра корпоративной компьютерной сети Заказчика.
* Внутреннее тестирование на проникновение. Осуществляется с мобильной рабочей станции Исполнителя, включенной в ЛВС Заказчика, и представляет собой выявление и анализ технических уязвимостей внутренних информационных систем.

Состав и ход оказания услуг на каждом этапе тестирования на проникновение определяются внутренними методиками Исполнителя, поддерживаемыми в актуальном состоянии путем их регулярного пересмотра и анализа с учетом постоянно накапливаемого опыта оказания услуг и текущих изменений в области информационной безопасности. Глубина и уровень исследования каждой из проверяемых систем определяется Исполнителем экспертно, исходя из достигаемых в ходе оказания услуг результатов, и с учётом доступного времени для дальнейшего оказания услуг.

Также в ходе тестирования на проникновение Исполнителем используются общепринятые мировые практики оказания подобных услуг, включая следующие методики:

* Open Source Security Testing Methodology Manual («OSSTMM») v3;
* OWASP Web Security Testing Guide v4.2;
* OWASP API Security 2023;
* OWASP Mobile Application Security Testing Guide v2.1.0;
* Web Application Security Consortium (WASC) Threat Classification v2;
* Payment Card Industry Data Security Standard Guidance: Penetration Testing Guidance v4.

Услуги на каждом из этапов предварительно согласуются с ответственными представителями Заказчика. В случае высокой вероятности нарушения функционирования целевых систем или в случае успешного доступа к конфиденциальной информации Заказчика Исполнитель прекращает дальнейшее оказания услуг до получения от Заказчика формального разрешения на продолжение.

В ходе оказания услуг Исполнитель не проводит распределенные атаки на отказ в обслуживании (DDoS).

* + 1. Сведения о моделях злоумышленника

В рамках оказания услуг по тестированию на проникновение предлагается смоделировать действия потенциальных злоумышленников, соответствующих следующим моделям:

* **«Интернет-хакер»** (модель «Черный ящик» внешнего тестирования) – злоумышленник, действующий из сети Интернет, не имеющий логических прав на внешних ресурсах Заказчика и осуществляющий атаки, направленные на получение доступа к внешним ресурсам, обрабатываемым данным и на получение доступа к узлам внутренней сети Заказчика;
* **«Посетитель»** (модель «Черный ящик» внутреннего тестирования) – злоумышленник, имеющий возможность подключения неконтролируемой рабочей станции к ЛВС Заказчика (например, внешний консультант), не имеющий логических прав в корпоративной информационной системе Заказчика и не обладающий подробными сведениями о структуре корпоративной сети и используемых средствах защиты.

Основными целями потенциальных злоумышленников являются:

* Получение доступа в корпоративную информационную систему Заказчика;
* Получение логического доступа к различным ресурсам корпоративной информационной системы Заказчика;
* Получение доступа к конфиденциальной информации, обрабатываемой в корпоративной информационной системе Заказчика;
* Определение возможности нарушения работоспособности систем Заказчика путем нарушения целостности обрабатываемых данных или нарушения доступности функционирующих сервисов.
  + 1. Внешнее тестирование на проникновение

Моделирование действий потенциального злоумышленника представляет собой проведение активного внешнего тестирования на проникновение.

Услуги на данном этапе оказываются путем выявления уязвимостей «ручным» методом и с использованием специализированного ПО и включают в себя:

* Определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
* Идентификация уязвимостей серверов, сетевого оборудования и сетевых средств защиты. Идентификация уязвимостей производится для всех хостов, входящих в границы оказания услуг и доступных (или ставших доступными в ходе оказания услуг) из сети Интернет (в том числе, сервисы HTTP и DNS, VPN-сервисы, web-приложения, сервис электронной почты, системные и прикладные сервисы). Производится выявление как уязвимостей, связанных с некорректной реализацией, так и уязвимостей, связанных с некорректной конфигурацией сетевых сервисов, ОС, приложений, сетевых устройств и средств защиты;
* Экспертный анализ (проникновение). Представляет собой моделирование атак, с использованием специализированных средств и сведений об известных уязвимостях, в отношении целевых систем. Услуги на данном этапе при необходимости могут итеративно повторяться с целью воздействия на связанные информационные системы, вошедшие в границы оказания услуг.
  + 1. Внутреннее тестирование на проникновение

Услуги на данном этапе заключаются в моделировании действий потенциального злоумышленника, имеющего возможность несанкционированного подключения к внутренней локальной сети Заказчика.

В состав услуг входит:

* Сбор сведений о ЛВС Заказчика изнутри сети;
* Определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
* Моделирование атак на сетевом уровне (ARP Spoofing, LLMNR и NBT-NS Poisoning и другие);
* Идентификация уязвимостей рабочих станций пользователей, компонентов информационных систем, сетевого оборудования и сетевых средств защиты;
* Моделирование атак на уровне приложений, сетевых сервисов и ОС, с использованием специализированных средств и сведений об известных уязвимостях в отношении выявленных систем;
* Выявление и оценка программных уязвимостей и ошибок конфигурации ресурсов локальной сети;
* Проверка прав доступа к различным информационным ресурсам с привилегиями, полученными на различных этапах тестирования.
  + 1. Тестирование механизмов сегментации

Услуги по тестированию механизмов сегментации заключаются в проверке эффективности использованных мер сегментации сети (отделении границ сертификации от остальной сети).

Тестирование механизмов сегментации выполняется два раза в течение одного календарного года с даты подписания договора. Первое тестирование проводится одновременно с этапом внутреннего тестирования на проникновение, второе – через 6 месяцев после первого тестирования по запросу Заказчика.

В состав услуг входит:

1. Сбор сведений о ЛВС Заказчика изнутри сети;
2. Идентификация сетевых сервисов и приложений по реакции на внешнее воздействие из-за пределов границ сертификации;
3. Выборочная проверка правил межсетевого экранирования на границе среды сертификации.

Результатом оказания услуг на данном этапе является отчет по результатам дополнительного внутреннего тестирования сегментации, содержащий информацию об оказываемых услугах, включая информацию обо всех выявленных недостатках и рекомендации по их устранению.

* 1. Внешнее сканирование уязвимостей (ASV-сканирование)

В ходе оказания Услуг в рамках данного Этапа Исполнитель использует ASV-сертифицированное решение, осуществляет поиск уязвимостей и небезопасных конфигураций сетевых служб, функционирующих на общедоступных сетевых узлах Заказчика.

Внешнее сканирование уязвимостей (ASV-сканирование) выполняется один раз в квартал в течение одного календарного года с даты подписания договора по запросу Заказчика для не более, чем **5** IP-адресов.

При оказании Услуг в соответствии с требованиями Стандарта (процедурами сканирования) используются профили, не включающие в себя опасные проверки, такие как атаки на «отказ в обслуживании», «перебор паролей», а выявляемые в ходе оказания Услуг уязвимости классифицируются по степени критичности.

В случае выявления уязвимостей или небезопасных конфигураций, Исполнитель передает Заказчику сведения необходимые для их устранения (на русском или английском языках), а также осуществляет повторные сканирования для подтверждения устранения выявленных уязвимостей (не более двух раз в квартал).

Результатом проведения сканирования являются:

* Attestation of Scan Compliance;
* Executive Summary;
* Vulnerability Details.
  1. Сертификационный аудит соответствия требованиям стандарта PCI DSS 4.0.1
     1. Определение области сертификации

На данном этапе аудиторской группой Исполнителя производится определение и согласование актуальной области аудита. Для этого, Исполнителем запрашивается имеющая информация о структуре информационных систем процессингового решения и процессах обеспечения информационной безопасности, а также определятся системные компоненты, каналы передачи данных и другие системы, включаемые в область аудита в соответствии с требованиями Стандарта.

Результатом данного этапа является перечень системных компонент, подлежащих аудиту.

* + 1. Сбор свидетельств соответствия

На данном этапе аудиторы Исполнителя проводят необходимое интервьюирование ответственных сотрудников Заказчика, проверяют параметры безопасности системных компонент, входящих в область аудита, и документируют свидетельства аудита необходимые для формирования итоговой отчетной документации.

Сбор всех необходимых сведений производится путем изучения нормативной документации, проведения интервью, анализа конфигурационных файлов, демонстрирования сотрудниками Заказчика выполняемых ими процедур по обеспечению информационной безопасности.

* + 1. Формирование отчетной документации

На данном этапе аудиторская группа Исполнителя на основе собранных свидетельств аудита проводит анализ выполнения требований Стандарта, которые определены в шести группах:

1. Построение и поддержание защищенной вычислительной сети;
2. Защита информации держателей платежных карт;
3. Реализация программы управления уязвимостями;
4. Реализация мер по строгому контролю доступа;
5. Регулярный мониторинг и тестирование вычислительных сетей;
6. Поддержание политики информационной безопасности.

и формирует необходимую отчётную документацию.

Результатом оказания услуг на данном этапе являются отчетные документы:

* SAQ-D, подписанный QSA-аудитором, или Report on Compliance;
* Attestation of Compliance;
* Сертификат соответствия PCI DSS 4.0.1.

Отчет по результатам сертификационного аудита разрабатывается в соответствии с регламентирующими документами консула PCI SSC по заполнению отчетов и должен содержать описание области оценки на соответствие требованиям Стандарта и оценочную часть, включая описание наблюдений по каждому из пунктов Стандарта.

Заключение о сертификационной проверке (Attestation of Compliance) разрабатывается в соответствии с формой, предоставленной консулом PCI SSC, на английском языке.