**Техническое задание**

**на оказание услуг**  **по подготовке и сертификации**  **на соответствие требованиям стандартОВ   
PCI DSS и PCI PIN Security**

**Москва**

**2024**

Перечень принятых сокращений

|  |  |  |
| --- | --- | --- |
| AOC | – | Attestation on Compliance (Заключение о соответствии требованиям стандарта PCI DSS) |
| ASV | – | Approved Scanning Vendor (Поставщик услуг сканирований, аккредитованный Советом стандартов безопасности (PCI SSC) |
| IP | – | Internet Protocol (Межсетевой протокол) |
| ISSAFF | – | Information System Security Assessment Framework (Система оценки безопасности информационной системы) |
| OSSTMM | – | Open Source Security Testing Methodology Manual (Руководство по методологии тестирования безопасности с открытым исходным кодом) |
| OWASP |  | Open Web Application Security Project (Открытый проект обеспечения безопасности веб-приложений) |
| PCI | – | Payment Card Industry (Индустрия платежных карт) |
| PCI DSS | – | Payment Card Industry Data Security Standard (Стандарт безопасности данных индустрии платежных карт) |
| PCI PIN Security |  | Payment Card Industry Personal Identification Numbers (PINs) Security Standard (Стандарт безопасности данных индустрии платежных карт для безопасного управления, обработки и передачи персональных идентификационных номеров (ПИН-кодов) и связанных с ними криптографических ключей) |
| QPA |  | Qualified PIN Assessors (Аудитор безопасности ПИН-кодов, аккредитованный Советом стандартов безопасности (PCI SSC)) |
| QSA | – | Qualified Security Assessor (Аудитор безопасности, аккредитованный Советом стандартов безопасности (PCI SSC)) |
| ROC | – | Report on Compliance (Отчет о соответствии требованиям стандарта PCI DSS) |
| ИС | – | Информационная система |
| ТЗ | – | Техническое задание |

# Общие сведения

## Настоящее Техническое задание (ТЗ) определяет требования к оказанию услуг по подготовке и сертификации на соответствие требованиям стандартов PCI DSS и PCI PIN Security.

# Цели и задачи оказания Услуг

## Цель оказания Услуг:

* + 1. Целью оказания Услуг является обеспечение выполнения требований стандартов Payment Card Industry Data Security Standard версия 4.0.1 (далее - PCI DSS) и Payment Card Industry Personal Identification Numbers Security Standard версия 3.1 (далее – PCI PIN Security) в Информационной системе (ИС) Заказчика.

## Задачи оказания услуг:

**PCI DSS**

* + 1. Предварительный аудит на соответствие требованиям стандарта PCI DSS v4.0.1.
    2. Приведение нормативной базы документов в соответствие требованиям стандарта PCI DSS v4.0.1.
    3. Внешнее тестирование на проникновение.
    4. Внутреннее тестирование на проникновение.
    5. Сертификационный аудит по стандарту PCI DSS v4.0.1.
    6. Внешнее ASV-сканирование уязвимостей.
    7. Внутреннее сканирование уязвимостей.
    8. Тестирование в отношении механизмов сегментации;
    9. Консультационная поддержка по реализации требований стандарта PCI DSS v4.0.1.

**PCI PIN Security**

* + 1. Предварительный аудит на соответствие требованиям стандарта PCI PIN Security v3.1.
    2. Приведение нормативной базы документов в соответствие требованиям стандарта PCI PIN Security v3.1.
    3. Сертификационный аудит по стандарту PCI PIN Security v3.1.
    4. Консультационная поддержка по реализации требований стандарта PCI PIN Security v3.1.

# Характеристика объекта обследования

## Объектом обследования является Информационная система ООО «Сервионика», расположенная по адресам:

* Москва, ул. Профсоюзная, д.76;
* Москва, ул. Воронцовская, д. 43, стр. 1.

## Сканированию уязвимостей и тестированию на проникновение подлежат IP-адреса, предоставленные Заказчиком в соответствии с п. 4.1.1 настоящего ТЗ.

# Требования к оказанию Услуг

## Требования к условиям оказания Услуг:

* + 1. Не позднее, чем за 5 (пять) рабочих дней до даты начала оказания Услуг по сканированиям и тестам на проникновение Заказчик должен письменно (по электронной почте) сообщить Исполнителю:
* Перечень IP-адресов, доступных из внешней сети Интернет, подлежащих внешнему сканированию уязвимостей (ASV сканированию) и тестированию на проникновение;
* Перечень IP-адресов внутренней сети Заказчика, подпадающих под требования PCI DSS, подлежащих внутреннему сканированию уязвимостей и тестированию на проникновение;
* Желаемые даты и время оказания Услуг;
* Контактное лицо со стороны Заказчика.
  + 1. Дата и время проведения каждого сканирования и тестирования на проникновение представители Заказчика и Исполнителя согласовывают письменно (по электронной почте).
    2. При оказании Услуг на объекте, Заказчик должен предоставить представителям Исполнителя рабочие места для выполнения предусмотренных договором обязательств.
    3. Заказчик должен обеспечить возможность для оказания предусмотренных договором услуг представителям Исполнителя в соответствии с согласованным Сторонами режимом конфиденциальности.
    4. Заказчик должен содействовать оказанию Услуг через полномочных сотрудников из подразделений Заказчика.
    5. Услуги оказываются в соответствии с Приложением №1 к настоящему Техническому заданию, после перечисления авансового платежа, в течение срока, указанного в Приложении №1 к настоящему Техническому заданию.
    6. В случае не предоставления Заказчиком необходимой для оказания Услуг информации сроки оказания Услуг могут сдвигаться по договоренности Сторон.

## Общие требования.

* + 1. В ходе оказания Услуг должны использоваться требования и рекомендации стандартов PCI DSS и PCI PIN Security:
* Стандарт PCI DSS Requirements and Testing Procedures версии 4.0.1;
* Стандарт PCI PIN Security Requirements and Testing Procedures версии 3.1;
* Guidance for PCI DSS Scoping and Network Segmentation;
* PCI DSS Risk Assessment Guidelines;
* PCI DSS Tokenization Guidelines;
* PCI DSS Virtualization Guidelines;
* PCI SSS Cloud Computing Guidelines.
* PCI DSS Wireless Guidelines;
* PCI DSS Penetration Testing Guidance;
* PCI DSS ASV Program Guide;
* Best Practices for Maintaining PCI DSS Compliance.
  + 1. В ходе обследования на месте должен быть проведен сбор, систематизация и анализ исходных данных, необходимых для получения исходной информации по обследуемым объектам Заказчика. Обследование может производиться как очным, так и заочным образом.
    2. Содержание опросных листов для интервьюирования сотрудников, необходимых для сбора исходных данных, а также методы сбора информации, должны быть согласованы с Заказчиком.
    3. Перечень исходных данных, а также содержание опросных листов может уточняться и дополняться во время оказания Услуг.

# Требования к составу Услуг

## **PCI DSS**

## Предварительный аудит на соответствие требованиям стандарта PCI DSS v4.0.1.

* + 1. Целью предварительного аудита по стандарту Payment Card Industry Data Security Standard v4.0.1 является, оценка текущего уровня соответствия ИС Заказчика, а также разработка рекомендаций по приведению в соответствие PCI DSS v4.0.1.
    2. Сбор сведений, необходимых в рамках предварительного аудита соответствия PCI DSS должен выполняться специалистами Исполнителя удалённо путем интервьюирования работников Заказчика и обследования ИС, так и с помощью анкетирования и запроса документов.
    3. Оценка соответствия требованиям стандарта PCI DSS должна производиться на основании внутренней методики проведения оценки соответствия по стандарту PCI DSS.
    4. Методика проведения оценки соответствия требованиям стандарта PCI DSS Исполнителя должна быть разработана на основе PCI DSS Requirements and Testing Procedures версии 4.0.1.
    5. По итогам анализа собранной информации в ходе предварительного аудита должна быть разработаны рекомендации по приведению Заказчика в соответствие стандарту PCI DSS v4.0.1.
    6. Разрабатываемые рекомендации по приведению в соответствие стандарту PCI DSS v4.0.1 должны включать:
* Сужение области сертификации PCI DSS;
* Изменение/дополнение/внедрение организационно-распорядительной документации;
* Изменение настроек и конфигураций технических, программных и программно-аппаратных комплексов защиты информации;
* Внедрение средств защиты информации, требуемых для соответствия PCI DSS;
* Иные мероприятия, выполнение которых необходимо для приведения в соответствие.
  + 1. Результатом услуги являются Рекомендации по приведению в соответствие стандарту PCI DSS v4.0.1.

## Приведение нормативной базы документов в соответствие требованиям стандарта PCI DSS v4.0.1.

* + 1. Целью услуги является модификация имеющихся документов Заказчика и разработка недостающих документов, требуемых для соответствия стандарту PCI DSS v4.0.1.
    2. Приведение нормативной базы документов в соответствие требованиям стандарта PCI DSS должно включать доработку имеющихся документов и предоставление шаблонов новых документов:
* Организационно-распорядительных документов (концепции, политики, процедуры, порядки, инструкции), регламентирующие процессы ИБ при обработке, передаче и хранении данных платежных карт;
* Стандартов безопасной настройки ресурсов, участвующих в обработке данных платежных карт;
* Актуализация действующей политики ИБ в рамках области применения стандарта PCI DSS v4.0.1.
  + 1. В случае наличия у Заказчика документированной политики или процедуры Исполнитель должен предложить доработать имеющийся документ, включив в него требуемые стандартом PCI DSS v4.0.1 политики и/или процедуры.
    2. В случае отсутствия у Заказчика документа, в который было бы целесообразно включить требуемые стандартом PCI DSS v4.0.1 политики и/или процедуры, Исполнитель должен предоставить Заказчику шаблон типового документа.
    3. При разработке шаблонов проектов внутренних нормативных документов Заказчика должны учитываться существующие у Заказчика процессы и устоявшиеся практики с целью внесения минимально необходимых изменений в существующие процессы Заказчика.
    4. Сбор необходимых сведений может выполняться специалистами Исполнителя удалённо путем интервьюирования работников Заказчика и обследования ИС, так и с помощью анкетирования и запроса документов.
    5. Результатом Услуги являются доработанные имеющиеся документы Заказчика либо шаблоны новых документов, в случае отсутствия необходимых документов у Заказчика:
* Организационно-распорядительные документы (концепции, политики, процедуры, порядки, инструкции), регламентирующие процессы ИБ;
* Стандарты безопасной настройки ресурсов, участвующих в обработке данных платежных карт;
* Актуализированные действующие политики ИБ в рамках области применения стандарта PCI DSS v4.0.1.

## Внешнее тестирование на проникновение.

* + 1. Целью оказания Услуги является реализация требования 11.4 стандарта PCI DSS.
    2. Тестирование на проникновение проводится на основе внутренней методики Исполнителя, которая основана на методиках и рекомендациях OWASP, ISSAFF, OSSTMM и включает:
* Сбор предварительной информации;
* Составление карты сети, определение используемых сервисов, устройств и операционных систем;
* Выявление уязвимостей;
* Моделирование атаки.
  + 1. Предварительная информация должна собираться с использованием источников информации, доступных злоумышленнику.
    2. Для выявления уязвимостей проводится инструментальный анализ защищенности – сканирование сети.
    3. Все собранные сведения анализируются для составления векторов атаки. При разработке векторов моделируемой атаки Исполнитель должен определить все возможные пути проникновения в ИС Заказчика.
    4. Для моделирования атаки Исполнитель должен использовать общедоступное программное обеспечение.
    5. Тестирование на проникновение должно проводиться в соответствии с требованиями стандарта PCI DSS. В частности, тестирование на проникновение должно быть проведено на сетевом уровне и уровне приложений.
    6. Тест на проникновение должен охватывать компоненты, поддерживающие взаимодействие на сетевом уровне, а также учитывать следующие уязвимости:
* Инъекции (в том числе SQL-инъекции);
* Переполнение буфера;
* Небезопасное криптографическое хранилище;
* Небезопасная передача данных;
* Некорректная обработка ошибок;
* Все уязвимости, имеющие «Высокую» степень риска, найденные в процессе обнаружения уязвимостей;
* Межсайтовый скриптинг (XSS);
* Ошибки в контроле доступа, такие как небезопасные прямые ссылки на объект, невозможность ограничения доступа по URL и обход директорий;
* Подделка межсайтовых запросов (CSRF).
  + 1. Моделирование атак, приводящих к отказу в обслуживании системы, не проводится.
    2. Результатом оказания Услуги является Отчет о результатах внешнего тестирования на проникновение.

## Внутреннее тестирование на проникновение

* + 1. Целью оказания Услуги является реализация требования 11.4 стандарта PCI DSS.
    2. Внутреннее тестирование на проникновение проводится для адресного пространства, подпадающего под требования PCI DSS.
    3. Тестирование на проникновение проводится на основе внутренней методики Исполнителя, которая основана на методиках и рекомендациях OWASP, ISSAFF, OSSTMM и включает:
* Сбор предварительной информации;
* Составление карты сети, определение используемых сервисов, устройств и операционных систем;
* Выявление уязвимостей;
* Моделирование атаки.
  + 1. Предварительная информация должна собираться с использованием источников информации, доступных злоумышленнику.
    2. Для выявления уязвимостей проводится инструментальный анализ защищенности – сканирование сети.
    3. Все собранные сведения анализируются для составления векторов атаки. При разработке векторов моделируемой атаки Исполнитель должен определить все возможные пути проникновения в ИС Заказчика.
    4. Для моделирования атаки Исполнитель должен использовать общедоступное программное обеспечение.
    5. Тестирование на проникновение должно проводиться в соответствии с требованиями стандарта PCI DSS. В частности, тестирование на проникновение должно быть проведено на сетевом уровне и уровне приложений.
    6. Тест на проникновение должен охватывать компоненты, поддерживающие взаимодействие на сетевом уровне, а также учитывать следующие уязвимости:
* Инъекции (в том числе SQL-инъекции);
* Переполнение буфера;
* Небезопасное криптографическое хранилище;
* Небезопасная передача данных;
* Некорректная обработка ошибок;
* Все уязвимости, имеющие «Высокую» степень риска, найденные в процессе обнаружения уязвимостей;
* Межсайтовый скриптинг (XSS);
* Ошибки в контроле доступа, такие как небезопасные прямые ссылки на объект, невозможность ограничения доступа по URL и обход директорий;
* Подделка межсайтовых запросов (CSRF).
  + 1. Моделирование атак, приводящих к отказу в обслуживании системы, не проводится.
    2. Результатом услуги является Отчет о результатах внутреннего тестирования на проникновение.

## Сертификационный аудит по стандарту PCI DSS

* + 1. Целью услуги является прохождение сертификационной проверки соответствия стандартам PCI DSS и демонстрация соответствия различным заказчикам услуг ООО «Сервионика»: международным платежным системам, организациям финансового сектора, торгово-сервисным предприятиям и иным организациям (в случае успешного прохождения сертификационной проверки)
    2. При определении области оценки Заказчик и Исполнитель должны уточнить границы проведения оценки по PCI DSS, а также перечень объектов и информационных систем, подлежащих дальнейшему обследованию и оценке по PCI DSS, также должен быть уточнен объем оказываемых Услуг.
    3. Перед оказанием Услуг Исполнитель должен предоставить и согласовать с Заказчиком план-график оказания Услуг, включая список документов, необходимых для анализа, а также перечень должностных лиц, с которыми предполагается провести собеседование и способ его проведения.
    4. Процедура оценки соответствия должна быть выполнена на основании методики Исполнителя, разработанной на основе документа «PCI DSS v4.0 Report on Compliance Template».
    5. Оценка соответствия требованиям стандарта PCI DSS должна включать в оценку:
* Оценку на организационном уровне;
* Технологическую оценку;
* Оценку на физическом уровне.
  + 1. При оценке на организационном уровне должна быть выполнена проверка наличия и анализ имеющейся организационно-распорядительной документации (ОРД), и степень ее соответствия требованиям стандарта PCI DSS. Услуги оказываются на стороне Исполнителя. Заказчик должен предоставить Исполнителю ОРД и другую информацию на основе списка необходимых исходных данных для анализа.
    2. При технологической оценке получение информации должно быть выполнено на территории Заказчика путем наблюдений и проверок выполнения требований стандарта, интервьюирования ответственных сотрудников Заказчика, а также запросом и изучением дополнительных документов. Тематика опроса и дата интервьюирования должна быть предварительно согласована с Заказчиком.
    3. В ходе технологической оценки должен быть выполнен анализ технических, программных и аппаратно-программных комплексов защиты информации, включая:
* Физической защиты помещений;
* Программно-аппаратных средств защиты каналов передачи данных;
* Программно-аппаратных комплексов защиты сетевого уровня;
* Программных средств защиты на прикладном уровне;
* Программных средств защиты информации на серверах и рабочих станциях.
  + 1. При оказании услуг по сертификационному аудиту должно быть учтено планирование и выполнение анализа защищенности и моделирования действий нарушителя с учетом результатов уже проведенных мероприятий. Проверке должны быть подвергнуты отчеты предыдущих проверок соответствия и оценка принятых решений по устранению выявленных недостатков в защите.
    2. Результаты Услуги:
* Заключение о соответствии требованиям стандарта PCI DSS (Attestation of Compliance);
* Отчет о соответствии требованиям стандарта PCI DSS (Report on Compliance);
* Сертификат соответствия PCI DSS (в случае успешного прохождения аудита).
  + 1. В случае выявления несоответствий требованиям стандарта дополнительно разрабатываются рекомендации по приведению Информационной системы в соответствие требованиям стандарта PCI DSS.
    2. В случае успешного прохождения сертификационной проверки соответствия стандарту PCI DSS Исполнитель выдает Заказчику сертификат соответствия PCI DSS.
    3. Исполнитель может передать в международные платежные системы согласованные с Заказчиком отчетные документы, а именно Заключение о соответствии требованиям стандарта PCI DSS (Attestation of Compliance).

## Внешнее ASV-сканирование уязвимостей

* + 1. Целью Услуги является выполнение требования 11.3 стандарта PCI DSS – внешнее сканирование сети Заказчика (ASV-сканирование).
    2. Услуга включает:
* Проведение не более 4 (четырех) сканирований для не более 25 IP-адресов в течение года;
* Определение используемых сервисов, устройств и операционных систем;
* Выявление уязвимостей для каждого IP-адреса;
* Анализ выявленных уязвимостей;
* Оценка статуса соответствия;
* Диспутный процесс.
  + 1. Статус соответствия системы Заказчика должен рассматриваться ASV-специалистом Исполнителя в соответствии со стандартом PCI DSS (ASV Program Guide).
    2. В случае если Заказчик не согласен с корректностью определения CVSS оценки, наличием данной уязвимости в своей системе, а также, если используются компенсирующие меры, Заказчик может оспорить выявленные в процессе работы Исполнителем уязвимости в диспутной форме.
    3. Диспутная форма запрашивается Заказчиком у Исполнителя и заполняется Заказчиком.
    4. Диспутная форма должна содержать письменное объяснение, доказательства и способ их получения.
    5. Исполнитель должен консультировать Заказчика по заполнению диспутной формы.
    6. Заполненная диспутная форма должна быть рассмотрена ASV-специалистом Исполнителя, который принимает решение о ее утверждении.
    7. Адреса, имеющие статус не соответствия, могут быть пересканированы в согласованные Заказчиком и Исполнителем сроки.
    8. Результатом Услуги является Отчет о результатах внешнего сканирования уязвимостей.

## Внутреннее сканирование уязвимостей

* + 1. Целью Услуги является выполнение требования 11.3 стандарта PCI DSS в части выполнения внутреннего сканирования информационных ресурсов Заказчика.
    2. Услуга включает:
* Сканирование перечня IP-адресов, определенных согласно п.4.1.1 настоящего ТЗ;
* Определение используемых сервисов, устройств и операционных систем;
* Выявление уязвимостей для каждого IP-адреса;
* Анализ выявленных уязвимостей;
* Оценка статуса соответствия;
* Диспутный процесс.
  + 1. Статус соответствия системы Заказчика должен рассматриваться ASV-специалистом Исполнителя в соответствии со стандартом PCI DSS (ASV Program Guide).
    2. В случае если Заказчик не согласен с корректностью определения CVSS оценки, наличием данной уязвимости в своей системе, а также, если используются компенсирующие меры, Заказчик может оспорить выявленные в процессе работы Исполнителем уязвимости в диспутной форме.
    3. Диспутная форма запрашивается Заказчиком у Исполнителя и заполняется Заказчиком.
    4. Диспутная форма должна содержать письменное объяснение, доказательства и способ их получения.
    5. Исполнитель должен консультировать Заказчика по заполнению диспутной формы.
    6. Заполненная диспутная форма должна быть рассмотрена ASV-специалистом Исполнителя, который принимает решение о ее утверждении.
    7. Адреса, имеющие статус не соответствия, могут быть пересканированы в согласованные Заказчиком и Исполнителем сроки.
    8. Результатом является Отчет о результатах внутреннего сканирования уязвимостей.

## Тестирование в отношении механизмов сегментации

* + 1. Тестирование механизмов сегментации сети проводится в соответствии с требованиями п.11.4.6 PCI DSS через 6 месяцев после проведения внутреннего тестирования на проникновение.
    2. Результатом Услуги является Отчет по результатам проверки в отношении механизмов сегментации. Отчет должен содержать сведения о предпринятых тестах механизмов сегментации, обеспечивающих эффективную изоляцию среды обработки данных платёжных карт от других сегментов Компании, и результатах проведения тестов.

## Консультационная поддержка по реализации требований PCI DSS

* + 1. Целью Услуги является оказание консультационной помощи Заказчику в выполнении требований стандарта PCI DSS.
    2. Специалисты Исполнителя должны оказывать консультационную поддержку, включая:
* консультации и пояснения требований стандарта PCI DSS, а также детальные рекомендации по их выполнению применительно к частным информационным системам, бизнес-процессам, процессам управления и обеспечения информационной безопасности;
* консультации в случае изменения требований стандарта PCI DSS;
* консультации по влиянию на область сертификации и соответствию требованиям PCI DSS проводимых изменений в ИТ - инфраструктуре и бизнес-процессах Заказчика;
* консультации по возможным изменениям структуры ИС или адаптации процессов с учетом требований PCI DSS;
* консультации по снижению влияния проводимых изменений в бизнес-процессах и ИТ-инфраструктуре на расширение области аудита;
* консультации по осуществлению сегментации вычислительной сети и размещению ней в ИС Заказчика;
* консультации по выбору, внедрению и анализу эффективности компенсирующих мер, консультирование по их модификации в случае необходимости.
  + 1. Исполнитель должен оказывать консультационную поддержку по запросам Заказчика, которые должны быть предоставлены в письменном виде по электронной почте или телефонной связи.
    2. Исполнитель должен оказывать консультационную поддержку по настоящему Техническому заданию в рабочее время, в будние дни, с 10.00 до 18.00 по московскому времени.
    3. Консультации оказываются в объеме не более 40 часов работы специалистов Исполнителя.

## **PCI PIN Security**

## Предварительный аудит на соответствие требованиям стандарта PCI PIN Security v3.1.

* + 1. Целью предварительного аудита по стандарту Payment Card Industry Personal Identification Numbers (PINs) Security Standard v3.1 является, оценка текущего уровня соответствия ИС Заказчика, а также разработка рекомендаций по приведению в соответствие PCI PIN Security v3.1.
    2. Сбор сведений, необходимых в рамках предварительного аудита соответствия PCI PIN Security должен выполняться специалистами Исполнителя удалённо путем интервьюирования работников Заказчика и обследования ИС, так и с помощью анкетирования и запроса документов.
    3. Оценка соответствия требованиям стандарта PCI PIN Security должна производиться на основании внутренней методики проведения оценки соответствия по стандарту PCI PIN Security.
    4. Методика проведения оценки соответствия требованиям стандарта PCI PIN Security Исполнителя должна быть разработана на основе PCI PIN Security Requirements and Testing Procedures версии 3.1.
    5. По итогам анализа собранной информации в ходе предварительного аудита должна быть разработаны рекомендации по приведению Заказчика в соответствие стандарту PCI PIN Security v3.1.
    6. Разрабатываемые рекомендации по приведению в соответствие стандарту PCI PIN Security v3.1 должны включать:
* Сужение области сертификации PCI PIN Security;
* Изменение/дополнение/внедрение организационно-распорядительной документации;
* Изменение настроек и конфигураций технических, программных и программно-аппаратных комплексов защиты информации;
* Внедрение средств защиты информации, требуемых для соответствия PCI PIN Security;
* Иные мероприятия, выполнение которых необходимо для приведения в соответствие.
  + 1. Результатом услуги являются Рекомендации по приведению в соответствие стандарту PCI PIN Security v3.1.

## Приведение нормативной базы документов в соответствие требованиям стандарта PCI PIN Security v3.1.

* + 1. Целью услуги является модификация имеющихся документов Заказчика и разработка недостающих документов, требуемых для соответствия стандарту PCI PIN Security v3.1.
    2. Приведение нормативной базы документов в соответствие требованиям стандарта PCI PIN Security должно включать доработку имеющихся документов и предоставление шаблонов новых документов:
* Организационно-распорядительных документов (концепции, политики, процедуры, порядки, инструкции), регламентирующие процессы ИБ при обработке, передаче и хранении данных платежных карт;
* Стандартов безопасной настройки ресурсов, участвующих в обработке данных платежных карт;
* Актуализация действующей политики ИБ в рамках области применения стандарта PCI PIN Security v3.1.
  + 1. В случае наличия у Заказчика документированной политики или процедуры Исполнитель должен предложить доработать имеющийся документ, включив в него требуемые стандартом PCI PIN Security v3.1 политики и/или процедуры.
    2. В случае отсутствия у Заказчика документа, в который было бы целесообразно включить требуемые стандартом PCI PIN Security v3.1 политики и/или процедуры, Исполнитель должен предоставить Заказчику шаблон типового документа.
    3. При разработке шаблонов проектов внутренних нормативных документов Заказчика должны учитываться существующие у Заказчика процессы и устоявшиеся практики с целью внесения минимально необходимых изменений в существующие процессы Заказчика.
    4. Сбор необходимых сведений может выполняться специалистами Исполнителя удалённо путем интервьюирования работников Заказчика и обследования ИС, так и с помощью анкетирования и запроса документов.
    5. Результатом Услуги являются доработанные имеющиеся документы Заказчика либо шаблоны новых документов, в случае отсутствия необходимых документов у Заказчика:
* Организационно-распорядительные документы (концепции, политики, процедуры, порядки, инструкции), регламентирующие процессы ИБ;
* Стандарты безопасной настройки ресурсов, участвующих в обработке данных платежных карт;
* Актуализированные действующие политики ИБ в рамках области применения стандарта PCI PIN Security v3.1.

## Сертификационный аудит по стандарту PCI DSS

* + 1. Целью услуги является прохождение сертификационной проверки соответствия стандартам PCI PIN Security и демонстрация соответствия различным заказчикам услуг ООО «Сервионика»: международным платежным системам, организациям финансового сектора, торгово-сервисным предприятиям и иным организациям (в случае успешного прохождения сертификационной проверки).
    2. При определении области оценки Заказчик и Исполнитель должны уточнить границы проведения оценки по PCI DSS, а также перечень объектов и информационных систем, подлежащих дальнейшему обследованию и оценке по PCI DSS, также должен быть уточнен объем оказываемых Услуг.
    3. Перед оказанием Услуг Исполнитель должен предоставить и согласовать с Заказчиком план-график оказания Услуг, включая список документов, необходимых для анализа, а также перечень должностных лиц, с которыми предполагается провести собеседование и способ его проведения.
    4. Процедура оценки соответствия должна быть выполнена на основании методики Исполнителя, разработанной на основе документа «PCI PIN Security v3.1 Report on Compliance Template».
    5. Оценка соответствия требованиям стандарта PCI DSS должна включать в оценку:
* Оценку на организационном уровне;
* Технологическую оценку;
* Оценку на физическом уровне.
  + 1. При оценке на организационном уровне должна быть выполнена проверка наличия и анализ имеющейся организационно-распорядительной документации (ОРД), и степень ее соответствия требованиям стандарта PCI PIN Security. Услуги оказываются на стороне Исполнителя. Заказчик должен предоставить Исполнителю ОРД и другую информацию на основе списка необходимых исходных данных для анализа.
    2. При технологической оценке получение информации должно быть выполнено на территории Заказчика путем наблюдений и проверок выполнения требований стандарта, интервьюирования ответственных сотрудников Заказчика, а также запросом и изучением дополнительных документов. Тематика опроса и дата интервьюирования должна быть предварительно согласована с Заказчиком.
    3. В ходе технологической оценки должен быть выполнен анализ технических, программных и аппаратно-программных комплексов защиты информации, включая:
* Физической защиты помещений;
* Программно-аппаратных средств защиты каналов передачи данных;
* Программно-аппаратных комплексов защиты сетевого уровня;
* Программных средств защиты на прикладном уровне;
* Программных средств защиты информации на серверах и рабочих станциях.
  + 1. При оказании услуг по сертификационному аудиту должно быть учтено планирование и выполнение анализа защищенности и моделирования действий нарушителя с учетом результатов уже проведенных мероприятий. Проверке должны быть подвергнуты отчеты предыдущих проверок соответствия и оценка принятых решений по устранению выявленных недостатков в защите.
    2. Результаты Услуги:
* Заключение о соответствии требованиям стандарта PCI PIN Security (Attestation of Compliance);
* Отчет о соответствии требованиям стандарта PCI PIN Security (Report on Compliance);
* Сертификат соответствия PCI PIN Security (в случае успешного прохождения аудита).
  + 1. В случае выявления несоответствий требованиям стандарта дополнительно разрабатываются рекомендации по приведению Информационной системы в соответствие требованиям стандарта PCI PIN Security.
    2. В случае успешного прохождения сертификационной проверки соответствия стандарту PCI DSS Исполнитель выдает Заказчику сертификат соответствия PCI PIN Security.
    3. Исполнитель может передать в международные платежные системы согласованные с Заказчиком отчетные документы, а именно Заключение о соответствии требованиям стандарта PCI PIN Security (Attestation of Compliance).

## Консультационная поддержка по реализации требований PCI PIN Security

* + 1. Целью Услуги является оказание консультационной помощи Заказчику в выполнении требований стандарта PCI PIN Security.
    2. Специалисты Исполнителя должны оказывать консультационную поддержку, включая:
* консультации и пояснения требований стандарта PCI PIN Security, а также детальные рекомендации по их выполнению применительно к частным информационным системам, бизнес-процессам, процессам управления и обеспечения информационной безопасности;
* консультации в случае изменения требований стандарта PCI PIN Security;
* консультации по влиянию на область сертификации и соответствию требованиям PCI PIN Security проводимых изменений в ИТ - инфраструктуре и бизнес-процессах Заказчика;
* консультации по возможным изменениям структуры ИС или адаптации процессов с учетом требований PCI PIN Security;
* консультации по снижению влияния проводимых изменений в бизнес-процессах и ИТ-инфраструктуре на расширение области аудита;
* консультации по осуществлению сегментации вычислительной сети и размещению ней в ИС Заказчика;
* консультации по выбору, внедрению и анализу эффективности компенсирующих мер, консультирование по их модификации в случае необходимости.
  + 1. Исполнитель должен оказывать консультационную поддержку по запросам Заказчика, которые должны быть предоставлены в письменном виде по электронной почте или телефонной связи.
    2. Исполнитель должен оказывать консультационную поддержку по настоящему Техническому заданию в рабочее время, в будние дни, с 10.00 до 18.30 по московскому времени.
    3. Консультации оказываются в объеме не более 40 часов работы специалистов Исполнителя.

# Порядок контроля и приемки Услуг

## Оказание Услуг подтверждается Актом сдачи-приемки услуг и предоставлением соответствующей документации (отчетных материалов).

## Содержание отчетных материалов согласуется Исполнителем и Заказчиком на основе требований настоящего ТЗ.

## Сроки согласования отчетных материалов не входят в сроки их разработки, указанные в Календарном плане оказания услуг. Срок согласования отчетных материалов не должен превышать 15 (пятнадцать) календарных дней.

## Во время оказания каждой Услуги промежуточная документация может передаваться представителю Заказчику в рабочем порядке до завершения оказания Услуги.

## Настоящее ТЗ может быть уточнено или изменено в процессе оказания Услуг. Уточнения и (или) изменения ТЗ производятся по письменному согласованию Сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТЗ.

## Согласование и утверждение изменений (дополнений) к ТЗ производится теми же должностными лицами, что и согласование (утверждение) ТЗ.

# Требования к документированию

## Состав и содержание отчетной документации

## **PCI DSS**

* + 1. Рекомендации по приведению в соответствие стандарту PCI DSS v4.0.1.
    2. Доработанные имеющиеся документы Заказчика либо шаблоны новых документов:
* Организационно-распорядительные документы (концепции, политики, процедуры, порядки, инструкции), регламентирующие процессы ИБ.
* Стандарты безопасной настройки ресурсов, участвующих в обработке данных платежных карт.
* Актуализированные действующие политики ИБ в рамках области применения стандарта PCI DSS v4.0.1.
  + 1. Отчет о результатах внешнего тестирования на проникновение должен содержать:
* Описание доступной инфраструктуры;
* Перечень полученной информации из открытых источников;
* Описание выявленных уязвимостей;
* Рекомендации по устранению выявленных уязвимостей;
* Описание действий по эксплуатации выявленных уязвимостей и получению несанкционированного доступа;
* Рекомендации к противодействию возможной эксплуатации каждой из уязвимостей.
  + 1. Отчет о результатах внутреннего тестирования на проникновение должен содержать:
* Описание доступной инфраструктуры;
* Перечень полученной информации из открытых источников;
* Описание выявленных уязвимостей;
* Рекомендации по устранению выявленных уязвимостей;
* Описание действий по эксплуатации выявленных уязвимостей и получению несанкционированного доступа;
* Рекомендации к противодействию возможной эксплуатации каждой из уязвимостей.
  + 1. Заключение о соответствии требованиям стандарта PCI DSS (Attestation of Compliance – AOC) должно соответствовать форме PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers, приведенной по адресу https://www.pcisecuritystandards.org/document\_library/.
    2. Отчет о соответствии требованиям стандарта PCI DSS (Report on Compliance – ROC) должен соответствовать форме PCI DSS v4.0.1 Report on Compliance Template, приведенной по адресу https://www.pcisecuritystandards.org/document\_library/.
    3. Сертификат соответствия стандарту PCI DSS (в случае успешного прохождения аудита).
    4. Отчет о результатах внешнего ASV-сканирования уязвимостей:
* Аттестационный лист ASV сканирования, содержащий информацию о Заказчике и итоги сканирования;
* Описание уязвимостей, содержащее информацию о соответствии компонент сканирования и общую информации о выявленных уязвимостях;
* Детальное описание уязвимостей, содержащее детальное описание каждой выявленной уязвимости, включающее рекомендации по устранению.
  + 1. Отчет о результатах внутреннего сканирования уязвимостей должен содержать:
* Детальное описание уязвимостей, содержащее детальное описание каждой выявленной уязвимости, включающее рекомендации по устранению.
  + 1. Отчет по результатам проверки в отношении механизмов сегментации:
* Сведения о предпринятых тестах механизмов сегментации, обеспечивающих эффективную изоляцию среды обработки данных платёжных карт от других сегментов Компании;
* Результаты проведения тестов механизмов сегментации.

## **PCI PIN Security**

* + 1. Рекомендации по приведению в соответствие стандарту PCI PIN Security v3.1.
    2. Доработанные имеющиеся документы Заказчика либо шаблоны новых документов:
* Организационно-распорядительные документы (концепции, политики, процедуры, порядки, инструкции), регламентирующие процессы ИБ;
* Стандарты безопасной настройки ресурсов, участвующих в обработке данных платежных карт;
* Актуализированные действующие политики ИБ в рамках области применения стандарта PCI PIN Security v3.1.
  + 1. Заключение о соответствии требованиям стандарта PCI PIN Security (Attestation of Compliance – AOC) должно соответствовать форме PCI PIN Security v3.1 Attestation of Compliance for Onsite Assessments, приведенной по адресу https://www.pcisecuritystandards.org/document\_library/.
    2. Отчет о соответствии требованиям стандарта PCI PIN Security (Report on Compliance – ROC) должен соответствовать форме PCI PIN Security v3.1 Template for Report on Compliance, приведенной по адресу https://www.pcisecuritystandards.org/document\_library/.
    3. Сертификат соответствия стандарту PCI PIN Security (в случае успешного прохождения аудита).

## Требования к оформлению отчетной документации.

* + 1. Итоговые документы оформляются Исполнителем в соответствии с согласованным сторонами режимом конфиденциальности.
    2. Сертификаты соответствия выдаются при полном соответствии требованиям стандартов PCI DSS и PCI PIN Security.
    3. Все отчетные документы, перечисленные в п.7.1, за исключением Attestation of Compliance, Report on Compliance и Сертификатов соответствия стандартам PCI DSS и PCI PIN Security, должны быть выполнены на русском языке.
    4. Отчетные документы Attestation of Compliance, Report on Compliance должны быть выполнены на английском языке.
    5. Сертификаты соответствия стандартам PCI DSS и PCI PIN Security должны быть выполнены на русском и английском языке.
    6. Отчетные документы Attestation of Compliance и Сертификаты соответствия стандартам PCI DSS и PCI PIN Security должны быть предоставлены Заказчику в одном экземпляре в бумажном и электронном виде. Остальные отчетные документы должны быть предоставлены в электронном виде в формате pdf.
    7. Доработанные имеющиеся документы Заказчика либо шаблоны новых документов предоставляются на русском языке в электронном виде в формате Word:
* Организационно-распорядительные документы (концепции, политики, процедуры, порядки, инструкции), регламентирующие процессы ИБ;
* Стандарты безопасной настройки ресурсов, участвующих в обработке данных платежных карт;
* Актуализированные действующие политики ИБ в рамках области применения стандартов PCI DSS v4.0.1 и PCI PIN Security v3.1.

# Приложение №1

**к Техническому заданию**

## **Календарный план оказания Услуг**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ этапа** | **Оказываемые по этапу Услуги** | Отчетные документы | Срок исполнения |
| 1 | Предварительный аудит на соответствие требованиям стандартов PCI DSS и PCI PIN Security | Рекомендации по приведению в соответствие стандартам PCI DSS и PCI PIN Security | 30 (тридцать) календарных дней с даты получения аванса |
| 2 | Приведение нормативной базы документов в соответствие требованиям стандартов PCI DSS и PCI PIN Security | Организационно-распорядительные документы (концепции, политики, процедуры, порядки, инструкции), регламентирующие процессы ИБ  Стандарты безопасной настройки ресурсов, участвующих в обработке данных платежных карт  Актуализированные действующие политики ИБ в рамках области применения стандартов PCI DSS и PCI PIN Security | 30 (тридцать) календарных дней с даты окончания услуг по Этапу 1 |
| 3 | Внешнее тестирование на проникновение  Внутреннее тестирование на проникновение  Сертификационные аудиты по стандартам PCI DSS и PCI PIN Security  Консультационная поддержка по реализации требований PCI DSS и PCI PIN Security | Отчет о результатах внешнего тестирования на проникновение  Отчет о результатах внутреннего тестирования на проникновение  Заключения о соответствии требованиям стандартов PCI DSS и PCI PIN Security (Attestation of Compliance)  Отчеты о соответствии требованиям стандартов PCI DSS и PCI PIN Security (Report on Compliance)  Сертификаты соответствия стандартам PCI DSS и PCI PIN Security | 30 (тридцать) календарных дней с даты окончания услуг по Этапу 2 |
| 4 | Внешнее ASV-сканирование уязвимостей (не более 25 IP-адресов, не более 4-х сканирований в течение года)  Внутреннее сканирование уязвимостей (не более 4-х сканирований в течение года)  Тестирование в отношении механизмов сегментации | Отчет о результатах внешнего ASV-сканирования уязвимостей  Отчет о результатах внутреннего сканирования уязвимостей  Отчет по результатам проверки в отношении механизмов сегментации | 12 (двенадцать) месяцев с даты выполнения первичного сканирования |