Дата: «13» 03 2026г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
ПРОВЕДЕНИЕ СЕРТИФИКАЦИОННОГО АУДИТА

Наименование:
Проведение сертификационного аудита для соответствия требованиям стандарта PCI DSS для АО «Milliy Banklararo Protsessing Markazi»

Заказчик: АО «Национальный Межбанковский Процессинговый Центр» (НМПЦ)
Контактное лицо: Тоиров А. (Главный специалист отдела по закупкам, +998781132407 / 7733, tender@nmpc.uz)

Согласовано:
Председатель правления
Бахадиров У. Х.

Директор департамента ИБ
Гафуров А. А.

Разработал:
Ведущий специалист отдела анализа уровня обеспечения информационной безопасности, расследований и оценки ущерба от событий и инцидентов информационной безопасности
Зубайдуллаев Ж. Ш.

Техническое задание

на проект

**Проведение сертификационного аудита
для соответствия требованиям стандарта PCI DSS для АО «Milliy Banklararo Protsessing Markazi»»,**

Ташкент – 2026 г.

1. ТРЕБОВАНИЯ К УСЛУГАМ

1.1. Полное наименование предмета работ

Проведение сертификационного аудита соответствия требованиям стандарта PCI DSS 4.0.1, а также консультация на подготовку к последующему соответствию требованиям стандарта PCI DSS 4.0.1 для АО «Milliy Banklararo Protsessing Markazi», (далее – Работы).

1.2. Границы проведения работ

Работы проводятся не более чем на 2-х площадках Заказчика, расположенных в г. Ташкент, Республика Узбекистан.

Внешний тест на проникновение выполняется Исполнителем не более 1-го (одного) раза.

Внутренний тест на проникновение выполняется Исполнителем не более 1-го (одного) раза.

Внешнее сканирование уязвимостей (ASV-сканирование) выполняется Исполнителем как минимум ежеквартально в течение 1 года с даты проведения первого из ASV-сканирования для не более чем 5 IP-адресов.

Расширение границ работ закрепляется дополнительным соглашением сторон к Договору, подписываемым Сторонами и скрепляемым печатями Сторон.

Услуги могут быть проведены как на площадке Заказчика, так и удаленно.

1.3. Состав работ

Для приведения Заказчика в соответствие требованиям Стандарта PCI DSS - Исполнитель обеспечивает выполнение следующих работ:

a) Предварительный аудит и консультирование на этапе приведения в соответствие, включая:

- Предварительный аудит на площадке Заказчика, в том числе на соответствие требованиям версии 4.0.1 Стандарта PCI DSS;
- Консультирование по выбору возможных средств защиты и способам снижения затрат;
- Разработку детального плана приведения в соответствие;
- Оказание годовой консультационной поддержки по вопросам выполнения требований Стандарта;

b) Разработку пакета необходимой нормативной документации;

c) Проведение внешних сканирований уязвимостей (ASV-сканирования);

d) Проведение внешнего тестирования на проникновение;

e) Проведение внутреннего тестирования на проникновение;

f) Тестирование механизмов сегментации

g) Проведение итогового сертификационного аудита.

2. Требования к Исполнителю

1. Исполнитель должен иметь действующий статус Qualified Security Assessor (QSA) в регионе CEMEA. Подтверждается письмом Участника с приведением скрина нахождения участника в актуальном списке сертифицированных аудиторов Payment Card Industry Security Standards Council (PCI SSC):

https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors/

2. При оказании услуг по ASV-сканированию должно использоваться ASV-сертифицированное решение, включенное в перечень «Approved Scanning Vendors» для выполнения требований стандартов PCI DSS:

https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

3. Исполнитель должен иметь действующий статус Software Security Framework Assessors. Подтверждается письмом Участника с приведением скрина нахождения участника в актуальном списке сертифицированных аудиторов Software Security Framework Assessors:

https://www.pcisecuritystandards.org/assessors_and_solutions/software_security_framework_assessors/

4. Исполнитель должен иметь не менее 3-х завершенных проектов по оценке соответствия требованиям стандарта PCI DSS за последние 2 (два) года (результаты приняты МПС и выданы сертификаты соответствия). Подтверждается копиями Актов оказания услуг или УПД, счет-фактуры, отзывами, благодарностями от Заказчиков (допускается сокрытие конфиденциальной информации, но из представленных документов должны определяться: дата договора, предмет оказания услуг, наименование заказчика, подписи сторон).

Опыт завершенных проектов по оценке соответствия требованиям стандарта PCI DSS (результаты приняты МПС и выданы сертификаты соответствия), проведенных на территории Республики Узбекистан, будет преимуществом.

5. Среди членов команды должны быть представлены специалисты, обладающие подтверждёнными компетенциями в области информационной безопасности:

- наличие в команде сертифицированных специалистов, обладающих статусом Qualified Security Assessor (QSA) – не менее 3 (Копии сертификатов специалистов);
- наличие в команде сертифицированных специалистов, обладающих статусом Certified Information Systems Security Professional (CISSP) или Certified Information Systems Auditor (CISA) или CISM – не менее 2 специалистов (Копии сертификатов специалистов);
- наличие в команде специалистов, обладающих статусом BSI ISO/IEC 27001 Lead Auditor – не менее 2 специалистов (Копии сертификатов специалистов);
- наличие в команде специалистов, обладающих статусом BSI ISO/IEC 27001 Lead Implementer – не менее 1 специалиста (Копия сертификата специалиста);
- наличие в команде сертифицированных специалистов, обладающих статусом CEH (Certified Ethical Hacker) – не менее 1 специалиста (Копия сертификата специалиста);
- наличие в команде сертифицированных специалистов, обладающих статусом OSCP (Offensive Security Certified Professional) – не менее 1 специалиста (Копия сертификата специалиста).

3. Этапы проведения работ

3.1. Предварительный аудит по требованиям Стандарта PCI DSS 4.0.1

3.1.1. Предварительное определение области применения Стандарта

Целью данного этапа является определение области применения Стандарта PCI DSS 4.0.1 применительно к создаваемой и имеющейся ИТ-инфраструктуре АО «Milliy Banklararo Protsessing Markazi» а также согласование объема выполняемых работ при проведении первичной оценки процессингового центра Заказчика.

Для определения области применения Стандарта PCI DSS Заказчик предоставляет документацию о разрабатываемой (существующей) архитектуре АО «Milliy Banklararo Protsessing Markazi», перечне систем участвующих в процессах обработки, хранения или передачи данных платежных карт, а также существующих процессах обеспечения информационной безопасности.

Результатом данного этапа является перечень обследуемых физических, программных и информационных ресурсов, функциональных подсистем, включаемых в границы проведения работ.

3.1.2. Сбор организационной и технической информации о процессинговом центре

Целью данного этапа является получение актуальной и достоверной информации об архитектуре создаваемого процессингового центра, потоках данных платежных карт, текущем уровне обеспечения информационной безопасности, планов по развитию и модернизации процессинга, а также другой информации, необходимой для оценки соответствия требованиям Стандарта PCI DSS и разработки Плана мероприятий с рекомендациями по подготовке к успешному сертификационному аудиту.

При выполнении данных работ производится сбор следующих сведений:

- об организационной структуре;
- о структуре комплекса используемых программно-технических средств;
- о топологии сети и применяемых методах сегментации (в т.ч. характеристики используемых каналов и точек подключения к сетям связи и сети Интернет, беспроводные точки доступа);
- о процедурах обеспечения безопасности в локальной сети;
- о механизмах защиты данных платежных карт;

- о процедурах управления уязвимостями;
- о реализации системы управления доступом;
- о процедурах мониторинга и контроля доступа (на уровне сети и приложений);
- о политике информационной безопасности.

Сбор всех необходимых сведений производится путем изучения предоставленной Заказчиком документации, проведения интервью с персоналом Заказчика, анализа конфигурационных файлов программных и программно-технических системных компонентов, демонстрирования сотрудниками Заказчика выполняемых ими процедур.

Также, по желанию Заказчика, на данном этапе может быть проведено однократное внутреннее сканирование уязвимостей, с выдачей рекомендаций по устранению выявленных уязвимостей.

3.1.3. Оценка соответствия требованиям Стандарта PCI DSS

Целью данного этапа является определение текущего уровня соответствия платежного шлюза Заказчика требованиям Стандарта PCI DSS.

На данном этапе, на основе полученной ранее информации - выполняется анализ соответствия инфраструктуры Заказчика требованиям Стандарта PCI DSS, для чего проводятся следующие работы:

- 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 работы.

Результатом работ на данном этапе является «Отчет об оценке соответствия создаваемой и существующей инфраструктуры Заказчика требованиям Стандарта PCI DSS». Данный отчет, включает в себя описание предлагаемой архитектуры платежного шлюза, перечень выявленных несоответствий требованиям Стандарта PCI DSS, описание текущей области применимости требований Стандарта PCI DSS (текущей области аудита) и входящих в неё системных компонент.

3.1.4. Разработка рекомендаций по приведению в соответствие требованиям Стандарта PCI DSS

На данном этапе работ осуществляется разработка возможных вариантов реализации требований Стандарта PCI DSS, путем построения комплекса организационных мероприятий и реализации необходимых технических решений, также, на данном этапе разрабатываются возможные варианты уменьшения области аудита (области сертификации) для снижения суммарных затрат на подготовку к успешной сертификации, за счет уменьшения числа внедряемых средств защиты и объема проводимых работ.

При составлении 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 настройку дополнительных средств защиты информации (как общедоступных, так и коммерческих решений);

Результатом работ на данном этапе является передаваемый Заказчику - План реализации организационных и технических мероприятий, выполнение которых позволит обеспечить выполнение всех требований Стандарта PCI DSS. План также должен включать в себя мероприятия для достижения соответствия требованиям версии стандарта PCI DSS 4.0.1

3.1.5. Обучение основам требований стандарта PCI DSS

В рамках данного этапа Исполнитель проводит разовое обучение специалистов Заказчика основам обеспечения соответствия стандарту PCI DSS.

Обучение по согласованию с Заказчиком может проводиться либо очно в г. Ташкент, в офисе Заказчика во время визита QSA-аудитора в рамках Этапа 1 либо в виде вэбинара.

Обучение проводится в течение не более чем 5 (пяти) часов.

Курсы проводятся по следующей программе:

1. Введение в стандарт PCI DSS
1.1. PCI SSC и обзор стандарта
1.2. Терминология платежной индустрии
1.3. Классификация торгово-сервисных предприятий и сервис-провайдеров
1.4. Жизненный цикл стандарта PCI DSS
1.5. Взаимоотношения участников в рамках стандарта.
2. Роли в стандарте PCI DSS и смежные сертификации
2.1. Роли платежных брендов
2.2. Программы безопасности данных от VISA и MasterCard
2.3. SAQ и ROC.
2.4. Обзор стандарта SSF
2.5. Обзор стандарта PCI PIN Security Requirements
2.6. Роли и обязанности участников
3. Обнаружение данных платежных карт и область аудита
3.1. Как обнаружить данные платежных карт в своей инфраструктуре.
3.2. Сегментация сети. Как правильно выполнить.
3.3. Как определить область аудита.
4. Требования стандарта PCI DSS
5. Внедрение и поддержание соответствия PCI DSS
5.1. Особенности приведения в соответствие требованиям стандарта
5.2. Требования с периодическим контролем
5.3. Требования с постоянным контролем
5.4. Аутсорсинг требований PCI DSS. Как правильно организовать.
5.5. Как применять компенсирующие меры.
6. Вспомогательные документы PCI SSC и работа с Международными платежными системами (МПС)
6.1. Обзор вспомогательных документов от PCI SSC
6.2. Приоритетный подход в достижении соответствия PCI DSS.
6.3. ROC и AOC.
7. Подведение итогов

Программа курсов может быть скорректирована Исполнителем.

3.2. Разработка пакета нормативной документации

Целью данного этапа является разработка пакета проектов нормативной документации, необходимой для выполнения требований Стандарта PCI DSS, включая:

- Стандарты конфигурирования операционных систем и СУБД;
- Политики обеспечения безопасности данных платежных карт;
- Процедуры реагирования на инциденты информационной безопасности;
- Регламенты и инструкции;
- Другая необходимая документация.

Итоговый состав разрабатываемых документов определяется аудиторами Исполнителя по результатам этапа «Разработка рекомендаций по приведению в соответствие требованиям Стандарта PCI DSS».

Результатом работ на данном этапе является переданный Заказчику пакет проектов нормативной документации, необходимой для выполнения требований Стандарта PCI DSS.

3.3. Внешнее сканирование уязвимостей (ASV-сканирование)

В ходе выполнения работ Исполнитель, используя ASV-сертифицированное решение, осуществляет поиск уязвимостей и небезопасных конфигураций сетевых служб, функционирующих на общедоступных сетевых узлах Заказчика.

Внешнее сканирование уязвимостей (ASV-сканирование) выполняется Исполнителем ежеквартально, по запросу Заказчика, в течение 1 года с даты проведения первого из сканирований, для не более чем 5 IP-адресов.

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

По желанию Заказчика, ему могут быть предоставлены права доступа к системе сканирования, для самостоятельного проведения неограниченного числа сканирований в течение 1 года с даты проведения первого из сканирований.

Результатом работ являются отчеты, передаваемые Заказчику по результатам проведения каждого из проведенных сканирований.

3.4. Тестирование на проникновение

Работы 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 ИС 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 ИС.

Состав и ход работ 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 проведения работ и текущих изменений в области информационной безопасности.

Также в ходе тестирования на проникновение Исполнителем используются общепринятые мировые практики проведения подобных работ, включая такие методики, как OSSTMM v3.0 и OWASP Testing Guide v3.

Работы 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 выполнение работ до получения от Заказчика формального разрешения на продолжение работ.

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

По результатам работ Заказчику передаются отчетные документы, содержащие описание выполненных работ, выявленных проблем (уязвимостей) и рекомендации по их устранению.

3.4.1. Сведения о моделях злоумышленника

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

- «Интернет-хакер» – злоумышленник, действующий из сети Интернет, не имеющий логических прав в ИС Заказчика и не обладающий сведениями о корпоративной сети и ИС Заказчика;
- «Посетитель» – злоумышленник, имеющий возможность подключения неконтролируемой рабочей станции к ЛВС Заказчика (например, внешний консультант), не имеющий логических прав в ИС Заказчика и не обладающий подробными сведениями о структуре корпоративной сети и используемых средствах защиты;

Потенциальные злоумышленники, соответствующие каждой из описанных моделей, используют общедоступное специализированное ПО и не обладают навыками самостоятельного

исследования уязвимостей ИС и их компонентов, а также не обладают квалификацией, достаточной для самостоятельной разработки вредоносного ПО.

Основными целями потенциальных злоумышленников являются:

- получение доступа в корпоративную сеть Заказчика;
- получение логического доступа в ИС Заказчика;
- получение доступа к конфиденциальной информации, обрабатываемой в ИС Заказчика;
- определение возможности нарушения работоспособности ЦОД Заказчика путем нарушения целостности обрабатываемых данных или нарушения доступности функционирующих сервисов.

3.4.2. Внешнее тестирование на проникновение

Работы по анализу защищенности внешнего периметра сети заключаются в моделировании действий потенциального внешнего злоумышленника, не обладающего подробными сведениями о корпоративной сети и процессинговом центре Заказчика.

Моделирование действий потенциального злоумышленника разделяется на два основных этапа:

1) Предварительный сбор информации. На данном этапе производится сбор сведений о структуре и компонентах корпоративной сети Заказчика, таких как: доменные имена и зоны, сетевая адресация, компоненты сети, используемые средства защиты.

2) Проведение активного внешнего тестирования на проникновение. Работы на данном этапе включают в себя выявление уязвимостей «ручным» методом и с использованием специализированного ПО. Состав работ на данном этапе включает 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 работ и доступных (или ставших доступными в ходе работ) 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 защищенности (проникновение). Представляет собой моделирование атак, с использованием специализированных средств и сведений об известных уязвимостях, в отношении целевых систем. Работы на данном этапе при необходимости могут итеративно повторяться с целью воздействия на связанные информационные системы, вошедшие в границы работ.

3.4.3. Внутреннее тестирование на проникновение

Работы на данном этапе заключаются в моделировании действий потенциального внутреннего злоумышленника. В состав работ входит:

1) Сбор сведений о ЛВС Заказчика изнутри сети;
2) Определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие;
3) Моделирование атак на сетевом уровне;
4) Идентификация уязвимостей рабочих станций пользователей, компонентов информационных систем, сетевого оборудования и сетевых средств защиты;
5) Моделирование атак на уровне приложений, сетевых сервисов и ОС, с использованием специализированных средств и сведений об известных уязвимостях в отношении выявленных систем.

3.5. Тестирование механизмов сегментации

Работы на данном этапе заключаются в проверки эффективности использованных мер сегментации сети (отделении границ сертификации от остальной сети). В состав работ 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 работ на данном этапе является отчет по результатам дополнительного внутреннего тестирования сегментации, содержащий информацию о выполненных работах, включая информацию обо всех выявленных недостатках и рекомендации по их устранению.

3.6. Сертификационный аудит соответствия требованиям стандарта PCI DSS 4.0.1

3.6.1. Определение области сертификации

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

Результатом данного этапа является перечень системных компонент, подлежащих аудиту.

3.6.2. 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.

3.6.3. Формирование отчетной документации

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

a) Построение и поддержание защищенной вычислительной сети;
b) Защита информации держателей платежных карт;
c) Реализация программы управления уязвимостями;
d) Реализация мер по строгому контролю доступа;
e) Регулярный мониторинг и тестирование вычислительных сетей;
f) Поддержание политики информационной безопасности.

и формирует необходимую отчётную документацию.

Результатом работ на данном этапе являются отчетные документы, направляемые Заказчику и в Международные Платежные Системы:

- Report on Compliance (на английском языке);
- Attestation of Compliance (на английском языке);
- Сертификат соответствия PCI DSS 4.0.1 (на русском и английском языках).

3.7. Консультационная поддержка по вопросам выполнения требований Стандарта PCI DSS

Целью работ на данном этапе является консультирование специалистов Заказчика по возникающим вопросам, связанным с разъяснением конкретных требований Стандарта PCI DSS и способам их выполнения.

Консультационная поддержка Заказчика осуществляется в течение 1 года с момента заключения договора. Прием запросов осуществляется по электронной почте и телефону. Время ответа на каждый поступивший запрос может составлять от 1 до 5 рабочих дней с даты приема запроса, в зависимости от сложности запроса.