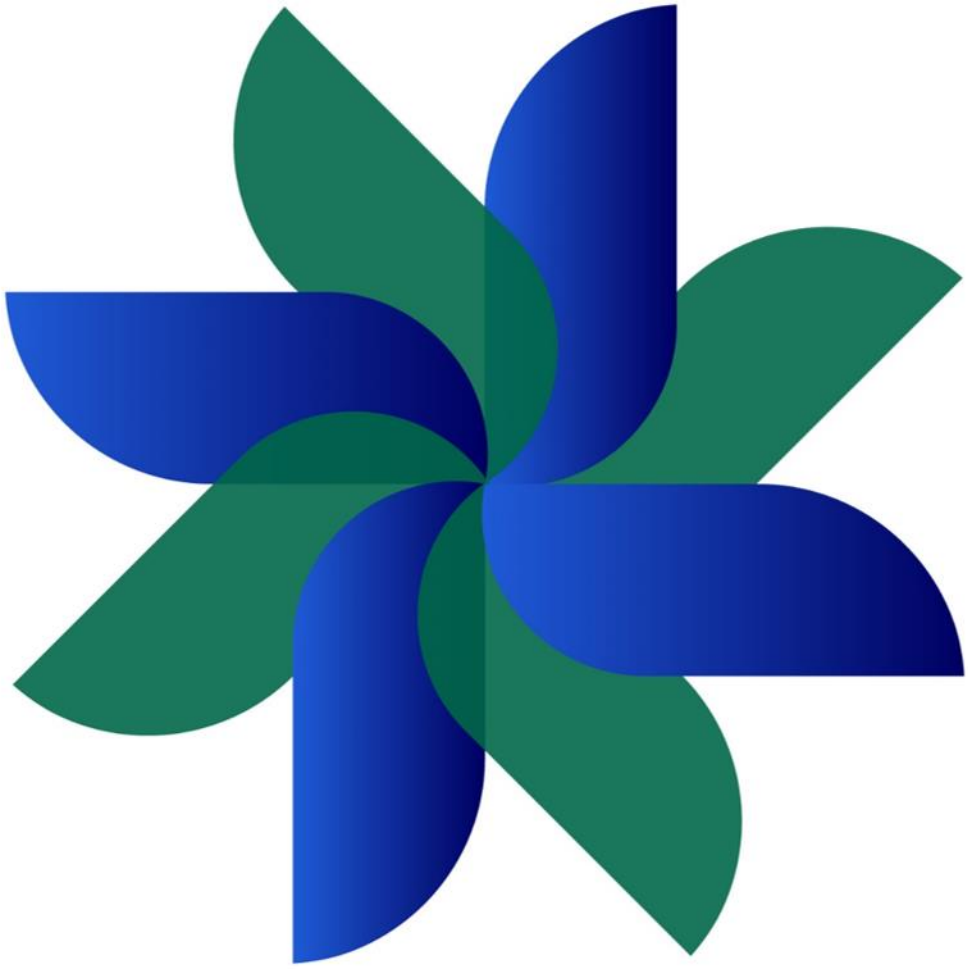
Требования по безопасности для ТСП

Версия 1.0



НСПК

Москва, 2020

Содержание:

Документ содержит выдержки из документа «Стандарт ПС “Мир”. «Программа безопасности» версии 1.3. Положения данного документа не заменяют собой положения основной версии стандарта. В случае спорных ситуаций текст документа «Стандарт ПС “Мир”. Программа безопасности» считать приоритетным.

Обратная связь:

В случае возникновения вопросов, связанных с данным документом, ТСП необходимо направить письмо на адрес mirsecurity@nspk.ru, в котором указать суть вопроса

Оглавление

1. Общие положения

1.1. Термины, определения и сокращения

Акционерное общество «Национальная система платежных карт» (НСПК) – оператор ПС «Мир».

Данные карт ПС «Мир» – набор данных, включающий данные о держателе карты и критичные аутентификационные данные, указанные в документе «PCI DSS and PA-DSS. Glossary of Terms, Abbreviations, and Acronyms»[1].

ИБ – информационная безопасность.

Инцидент информационной безопасности (Инцидент ИБ) – инцидент, связанный с нарушениями требований к обеспечению защиты информации при осуществлении Операций, к которому относятся:

- события, которые привели или могут привести к осуществлению Операций без согласия Клиента;
- события, которые привели или могут привести к нарушению непрерывности или несвоевременности оказания платежных услуг, операционных услуг, услуг платежного клиринга и расчетных услуг
- события, включенные в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на официальном сайте Банка России в сети Интернет.

Несанкционированный перевод денежных средств – перевод денежных средств лицами, не обладающими правом распоряжения денежными средствами.

Платежный сервис-провайдер – Сервис-провайдер, который оказывает Участникам и третьим лицам, с которыми Участник осуществляет взаимодействие, услуги по авторизации и клирингу, а также услуги обмена информацией при осуществлении операций с использованием Карт (реквизитов Карт) между Участниками, Держателями Карт, ТСП, иными Платежными сервис-провайдерами.

ПО – программное обеспечение.

Сервис-провайдер – организация, предоставляющая Участникам, Платежным Сервис-провайдерам и/или ТСП услуги по хранению, обработке или передачи данных платежных карт и имеющая возможность влиять на безопасность таких данных. Примерами таких компаний могут

[1] Глоссарий терминов, аббревиатур и сокращений PCI DSS и PA-DSS

являться компании, предоставляющие услуги co-location, IaaS (Infrastructure-as-a-Service), SaaS (Software-as-a-Service), разработки ПО, а также услуги по авторизации, клирингу. Организации, предоставляющие услуги связи (телекоммуникационные услуги), не являются Сервис-провайдерами.

AOC (Attestation of Compliance) – Аттестат соответствия.

ISA (Internal Security Assessor) – внутренние аудиторы, прошедшие обучение и сертифицированные по программе Совета PCI SSC, согласно перечню https://www.pcisecuritystandards.org/assessors_and_solutions/internal_security_assessors/.

ROC (Report on Compliance) – Отчет о соответствии.

SAQ (Self Assessment Questionnaire) – Лист самооценки.

Иные термины, используемые в настоящем документе, применяются в значениях, установленных в Правилах ПС «Мир»[2] и документе «PCI DSS and PA-DSS. Glossary of Terms, Abbreviations, and Acronyms»[3].

1.2. Нормативные ссылки

[1] *Правила Платежной системы «Мир»*.

[2] *Стандарт ПС «Мир». Порядок обработки инцидентов ИБ Участником*.

1.3. Уведомления

Перевод документов

Перевод любого документа, разработанного АО «НСПК», может быть выполнен третьим лицом исключительно после получения письменного разрешения АО «НСПК». АО «НСПК» не контролирует и не несет ответственности за содержание переведенного текста документа.

Переведенные тексты документов, разработанных АО «НСПК», применяются третьим лицом исключительно в целях установления содержания и смысла этих документов и не имеют юридической силы.

Тексты документов, составленных на русском языке, имеют приоритет перед текстами на другом языке.

[2] Документ доступен на сайте https://www.nspk.ru/cards-mir/terms-and-tariffs/

[3] Документ доступен на сайте https://www.pcisecuritystandards.org/document_library

Внесение изменений	Настоящий документ публикуется на сайте https://www.nspk.ru/cards-mir/security/security-program/. АО «НСПК» вправе в одностороннем порядке вносить изменения в настоящий документ. Настоящий документ актуализируется в случае обновления основного документа *«Стандарт ПС “Мир”. Программа безопасности»*. Срок вступления в силу изменений основной версии документа *«Стандарт ПС “Мир”. Программа безопасности»* устанавливается АО «НСПК».

2. Защита данных платежных карт

2.1. Требования к обеспечению безопасности

2.1.1 Участники, а также третьи лица, с которыми Участник осуществляет взаимодействие (Платежные сервис провайдеры, ТСП и иные организации), которые хранят, передают или обрабатывают данные Карт ПС «Мир», должны обеспечивать выполнение требований стандарта безопасности PCI DSS.

2.1.2 Участники должны обеспечить подтверждение ТСП соответствия этим требованиям. Соответствие должно подтверждаться в порядке, предусмотренном настоящим документом.

2.2. Требования к ТСП

2.2.1 Для ТСП состав обязательных к выполнению требований PCI DSS и перечень обязательных процедур для подтверждения соответствия PCI DSS определяется в зависимости от годового объема обрабатываемых Операций по Картам ПС «Мир».

2.2.2 ТСП делятся на четыре уровня: L1, L2, L3, L4.

2.2.3 Уровень ТСП может измениться в случае изменения годового объема осуществляемых в ТСП операций с использованием Карт ПС «Мир». Актуализация уровня ТСП должна проводиться Эквайрером каждые полгода при предоставлении АО «НСПК» сведений о ТСП. Эквайрер отслеживает изменение уровня и должен обязать ТСП:

- выполнять требования, актуальные для текущего уровня;
- подтвердить соответствие новым требованиям в течение года с момента изменения уровня.

2.2.4 К ТСП уровня L1 относятся:

- ТСП, у которых ежегодно проводится более 6 миллионов операций по Картам ПС «Мир»;
- любые ТСП, по которым в предыдущем календарном году была подтверждена компрометация[4] Карт «Мир».

2.2.5 ТСП уровня L1 должны подтверждать свое соответствие стандарту PCI DSS, выполняя:

[4] Компрометация Карт ПС «Мир» у ТСП считается подтвержденной, когда уполномоченные сотрудники Эквайрера подтвердили факт несанкционированного доступа к данным Карт ПС «Мир» в точке обслуживания в ТСП и сообщили об этом АО «НСПК» в порядке, предусмотренном в настоящем документе.

- ежегодный сертификационный аудит;
- ежеквартальное ASV-сканирование (если применимо).

2.2.6 По результатам сертификационного аудита ТСП уровня L1 предоставляет своему Эквайреру заполненный по шаблонам PCI SSC Аттестат соответствия (AOC). Аттестат соответствия (AOC) должен быть подписан аудитором и уполномоченным представителем ТСП. Формат предоставления AOC (на бумажном носителе или в электронном виде) ТСП Эквайреру определяется Эквайрером.

2.2.7 К ТСП уровня L2 относятся организации, у которых ежегодно проводится от 1 до 6 миллионов операций по Картам ПС «Мир».

2.2.8 ТСП уровня L2 должны подтверждать свое соответствие требованиям, выполняя:

- ежегодный сертификационный аудит в объеме milestone 1 и milestone 2 Концепции приоритетного подхода[5] к достижению соответствия PCI DSS;
- ежеквартальное ASV-сканирование (если применимо).

2.2.9 По результатам сертификационного аудита ТСП уровня L2 предоставляет своему Эквайреру заполненный по шаблонам PCI SSC Аттестат соответствия (AOC). Аттестат соответствия (AOC) должен быть подписан аудитором и уполномоченным представителем ТСП. Формат предоставления AOC (на бумажном носителе или в электронном виде) ТСП Эквайреру определяется Эквайрером.

2.2.10 К ТСП уровня L3 относятся организации, у которых ежегодно проводится от 20 000 до 1 миллиона операций по картам ПС «Мир» посредством электронной коммерции.

2.2.11 ТСП уровня L3 должны выполнять требования PCI DSS, указанные в Листе самооценки (SAQ). Тип Листа самооценки (SAQ) выбирается Эквайрером, исходя из того, каким способом ТСП принимает платежи[6].

2.2.12 В случае изменения в ТСП способа приема платежей Эквайрер должен обязать ТСП выполнить требования ставшего применимым Листа самооценки (SAQ). Срок предоставления ТСП подтверждения соответствия требованиям PCI DSS устанавливается Эквайрером.

2.2.13 ТСП уровня L3 должны подтверждать свое соответствие стандарту PCI DSS, выполняя:

[5] Концепция приоритетного подхода (Prioritized Approach for PCI DSS) доступна в разделе Documentation Library по ссылке https://www.pcisecuritystandards.org/document_library.

[6] При выборе подходящего типа листа самооценки, следует руководствоваться документом: https://www.pcisecuritystandards.org/documents/SAQ-InstrGuidelines-v3_2_1.pdf

- ежегодную самооценку по выбранному Эквайрером типу Листа самооценки (SAQ);
- ежеквартальное ASV - сканирование (если применимо).

2.2.14 По результатам самооценки ТСП уровня L3 предоставляет своему Эквайреру Лист самооценки (SAQ), заполненный по шаблонам PCI SSC. Лист самооценки (SAQ) должен быть подписан уполномоченным представителем ТСП. В случае привлечения к заполнению Листа самооценки (SAQ) аккредитованного в ПС «Мир» аудитора или Внутреннего аудитора (ISA), Лист самооценки (SAQ) должен быть подписан аудитором и уполномоченным представителем ТСП. В Листе самооценки (SAQ) необходимо указать роль и функции, которые выполнял аудитор в рамках проведенной самооценки.

2.2.15 К ТСП уровня L4 относятся все остальные ТСП, которые не подпадают под уровень L1, L2 или L3.

2.2.16 ТСП уровня L4 должны выполнять требования PCI DSS, указанные в Листе самооценки (SAQ). Тип листа самооценки определяется Эквайрером, исходя из того, каким способом ТСП принимает платежи[6].

2.2.17 В случае изменения способа приема платежей Эквайрер должен обязать ТСП выполнить требования ставшего применимым Листа самооценки (SAQ). Срок предоставления ТСП подтверждения соответствия требованиям PCI DSS устанавливается Эквайрером.

2.2.18 ТСП уровня L4 отчитывается о соответствии стандарту PCI DSS перед своим Эквайрером. Сроки и форму отчетности устанавливает Эквайрер.

2.2.19 Допускается использовать русскоязычную версию SAQ, доступную на сайте PCI SSC[7].

2.2.20 АО «НСПК» оставляет за собой право запрашивать Аттестат соответствия (AOC) и Лист самооценки (SAQ) ТСП у Участника, который взаимодействует с ТСП. По запросу АО «НСПК» участник должен предоставить запрошенные документы в порядке и сроки, указанные в запросе АО «НСПК».

2.2.21 ТСП уровня L1, L2, L4, которые используют только POS-терминалы для приема карт в целях оплаты товаров (работ, услуг) с предъявлением карты, вправе не подтверждать свое соответствие стандарту PCI DSS посредством сертификационного аудита или самооценки в случае обеспечения Участником, который взаимодействует с такими ТСП, соответствия данного ТСП критериям, указанным в документе *«Стандарт ПС “Мир”. Специальная программа подтверждения соответствия ТСП требованиям безопасности»*.

[7] Листы самооценки (SAQ) на русском и английском языке доступны на сайте https://www.pcisecuritystandards.org/document_library?category=saqs

2.3. Правила проведения сертификационного аудита и ASV-сканирования

2.3.1 Сертификационный аудит PCI DSS могут проводить организации, имеющие статус QSA. Перечень QSA-организаций доступен по ссылке: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors/.

2.3.2 Результатом сертификационного аудита являются заполненные по шаблонам PCI SSC Отчет о соответствии (ROC) и Аттестат соответствия (AOC). Аттестат соответствия (AOC) должен быть подписан аудитором и уполномоченным представителем организации, в которой проходил аудит.

2.3.3 Сертификационный аудит PCI DSS в ТСП могут проводить Внутренние аудиторы (ISA), прошедшие обучение и сертифицированные по программе Совета PCI SSC, согласно перечню https://www.pcisecuritystandards.org/assessors_and_solutions/internal_security_assessors/.

2.3.4 Ежеквартальное ASV-сканирование должно выполняться организацией, обладающей статусом PCI ASV из списка совета PCI SSC: https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors/. Отчеты о результатах ASV-сканирования должны предоставляться в АО «НСПК» по запросу.

2.4. Регистрация ТСП

2.4.1 Участники, осуществляющие свою деятельность в ПС «Мир» по типам A и C, должны контролировать статус соответствия привлеченных ТСП требованиям PCI DSS и представлять АО «НСПК» сведения о ТСП уровней L1, L2 и L3 два раза в год по следующему графику:

- 1-й отчетный период: с 1 по 31 марта – за отчетный период с 1 сентября по 28 февраля;
- 2-й отчетный период: с 1 по 30 сентября – за отчетный период с 1 марта по 31 августа.

2.4.2 В отчете должны предоставляться сведения о ТСП, с которыми у Эквайрера были установлены договорные отношения в указанные отчетные периоды.

3. Безопасность платежного программного обеспечения

3.1 В случае использования Участником, Платежным сервис-провайдером или ТСП стороннего платежного программного обеспечения, такое ПО должно быть сертифицировано по стандарту PCI PA-DSS, если применимо. Условия применимости стандарта PCI PA-DSS к стороннему платежному программному обеспечению указаны в PCI PA-DSS Program Guide, размещенному в сети Интернет по адресу https://www.pcisecuritystandards.org/document_library. Участники обязаны обеспечить соблюдение привлеченными ими Платежными сервиспровайдерами или ТСП указанных требований..

4. Управление инцидентами ИБ

4.1 Участники должны осуществлять обработку Инцидентов ИБ, в результате которых появились подозрения в компрометации или которые привели к компрометации данных карт ПС «Мир» в своей инфраструктуре, в инфраструктуре ТРР, а также в инфраструктуре привлеченных ими организаций, в том числе которые привели или могли привести к нарушению непрерывности или несвоевременности оказания услуг по осуществлению Операций Участниками согласно положениям документа *«Стандарт ПС “Мир”. Порядок обработки инцидентов ИБ Участником»* [2].

Приложение № 1. Сводная таблица уровней и форм отчетности

Уровень	Организация	Форма оценки	Перед кем отчитывается	Форма отчетности
Торгово-сервисные предприятия				
L1	ТСП, которые обрабатывают ежегодно более 6 млн операций по Картам ПС «Мир»	• ежегодный сертификационный аудит (QSA или ISA) • ежеквартальное ASV-сканирование (если применимо) **или** • соответствие критериям документа *«Стандарт ПС “Мир”. Специальная программа подтверждения соответствия ТСП требованиям безопасности»*	Эквайрер	АОС
			Эквайрер перед АО «НСПК»	Согласно требованиям документа *«Стандарт ПС “Мир”. Специальная программа подтверждения соответствия ТСП требованиям безопасности»*
	ТСП, для которых в предыдущем году была подтверждена компрометация Карт ПС «Мир»	• сертификационный аудит в текущем году (QSA или ISA) • ежеквартальное ASV-сканирование (если применимо)	Эквайрер	АОС
L2	ТСП, которые обрабатывают ежегодно от 1 до 6 млн операций по Картам ПС «Мир»	• ежегодный сертификационный аудит (QSA или ISA) • ежеквартальное ASV-сканирование (если применимо) **или** • соответствие критериям документа *«Стандарт ПС “Мир”. Специальная программа подтверждения соответствия ТСП требованиям безопасности»*	Эквайрер	АОС по требованиям, обозначенным, как milestone 1 и milestone 2 в документе *«Концепция приоритетного подхода к достижению соответствия PCI DSS»*
			Эквайрер перед АО «НСПК»	Согласно требованиям документа *«Стандарт ПС “Мир”. Специальная программа*

Уровень	Организация	Форма оценки	Перед кем отчитывается	Форма отчетности
				подтверждения соответствия ТСП требованиям безопасности»
L3	ТСП, которые обрабатывают ежегодно от 20 000 до 1 млн операций по картам ПС «Мир» в среде электронной коммерции	• ежегодная самооценка по выбранному Эквайрером листу самооценки SAQ • ежеквартальное ASV-сканирование (если применимо)	Эквайрер	SAQ
L4	Остальные ТСП	На усмотрение Эквайрера **или** соответствие критериям документа *«Стандарт ПС “Мир”. Специальная программа подтверждения соответствия ТСП требованиям безопасности»*	Эквайрер	На усмотрение Эквайрера
			Эквайрер перед АО «НСПК»	Согласно требованиям документа *«Стандарт ПС “Мир”. Специальная программа подтверждения соответствия ТСП требованиям безопасности»*

Приложение № 2. Схема формы отчетности по PCI DSS для Торгово-сервисных предприятий