

МИР

МЫ СЕГОДНЯ



376

 Банки

Присоединились
к ПС «Мир»

362

Банков
эквайреров

159

Банки
эмитента



125 509

банкоматов

принимают карты «Мир» (99,82%)



1 797 055

POS-терминалов

принимают карты «Мир» (99,77%)

выпущено карт

31 254 574



НСПК

Платёжная система «Мир» – программа безопасности

Платёжная система



15 февраля 2018,
Магнитогорск

Агенда

- Основные положения программы безопасности ПС «Мир»
- Контроль качества аудитов
- Порядок взаимодействия с участниками
- Оптимизация комплайнс-нагрузки в скоупе процессинга

01

Основные положения
программы безопасности ПС «Мир»

Свод основных требований по безопасности

Правила ПС «Мир»

382-П

Стандарты PCI

Подтверждение соответствия PCI DSS: субъекты ПС



Подтверждать статус соответствия должны процессоры, сервис провайдеры и ТСП

Подтверждение PCI DSS: процессоры и сервис-провайдеры

Уровень	Описание	Форма оценки	Аудитор
L1	Все, имеющие прямое подключение к ОПКЦ Сервис-провайдеры, обрабатывающие >300 000 трн. РС «Мир» (в год)	Аудит	Аккредитован в РС «Мир»
L2	Остальные сервис-провайдеры	Самооценка	

Подтверждение PCI DSS: торгово-сервисные предприятия

Уровень	Описание	Форма оценки	Аудитор
L1	обрабатывающие > 6 млн трн ПС «МИР» (в год)	Полный аудит/ самооценка	Аккредитован в ПС «МИР»/ ISA
L2	обрабатывающие от 1 до 6 млн трн ПС «МИР» (в год)	Частичный Аудит*/ самооценка	Аккредитован в ПС «МИР»/ ISA
L3	обрабатывающие от 20 000 до 1 млн е-сот трн ПС «МИР» (в год)	Самооценка + сканирования	



* - оценка соответствия по приоритетам 1 и 2 согласно утвержденной PCI SSC приоритезации

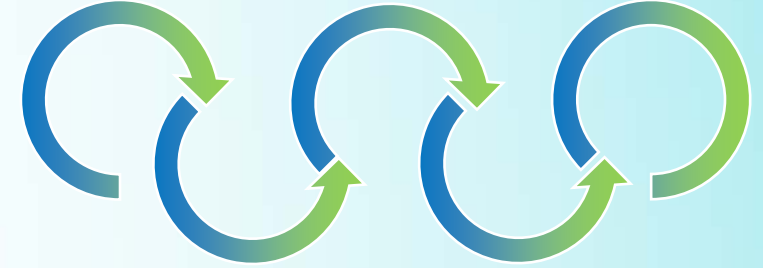
Особые условия

Для всех типов субъектов ПС «Мир» требуется оценка соответствия PCI DSS путем сертификационного аудита **на следующий год после подтвержденной компрометации** платежных карт/платежной инфраструктуры

Отчетность по результатам оценки PCI DSS:

Форма оценки	Отчетность	Периодичность	Кому предоставляется
Аудит	Отчет об аудите (ROC) Заключение (AOC)	Ежегодно	Процессоры и сервис-провайдеры -> АО «НСПК» ТСП -> банк-эквайрер
Самооценка	Отчет о самооценке (SAQ)	Ежегодно	Процессоры и сервис-провайдеры -> АО «НСПК» ТСП -> банк-эквайрер

Программа безопасности: не только PCI DSS



- Все субъекты ПС «Мир» должны использовать ПО, сертифицированное по PA-DSS (если применимо)
- Участники ПС «Мир» используют только сертифицированных согласно PCI DSS сервис-провайдеров
- Все участники ПС «Мир» отчитываются ежегодно по используемым ими сервис-провайдерами (по утвержденной форме)
- Эквайрер обеспечивает классификацию и контроль соответствия PCI DSS своих торгово-сервисных предприятий
- Эквайрер отчитывается в АО «НСПК» по своим торгово-сервисным предприятиям и их статусу PCI DSS один раз в полгода (по утвержденной форме)

Программа безопасности: сроки

Ввод в действие

3 кв. 2018

02

Реализация программы
безопасности ПС «Мир»

Контроль качества аудитов PCI DSS

- Аккредитация на право проведения сертификационных аудитов
 - первичная аккредитация = статус PCI QSA
- Периодический контроль качества на основании отчетов
 - критерии качества по программе PCI SSC
- При выявлении нарушений:
 - особый статус до устранения
 - оповещение PCI SSC
- Систематические нарушения – **приостановка аккредитации** сроком на 1 год
- Старт программы контроля качества – 2 кв. 2018

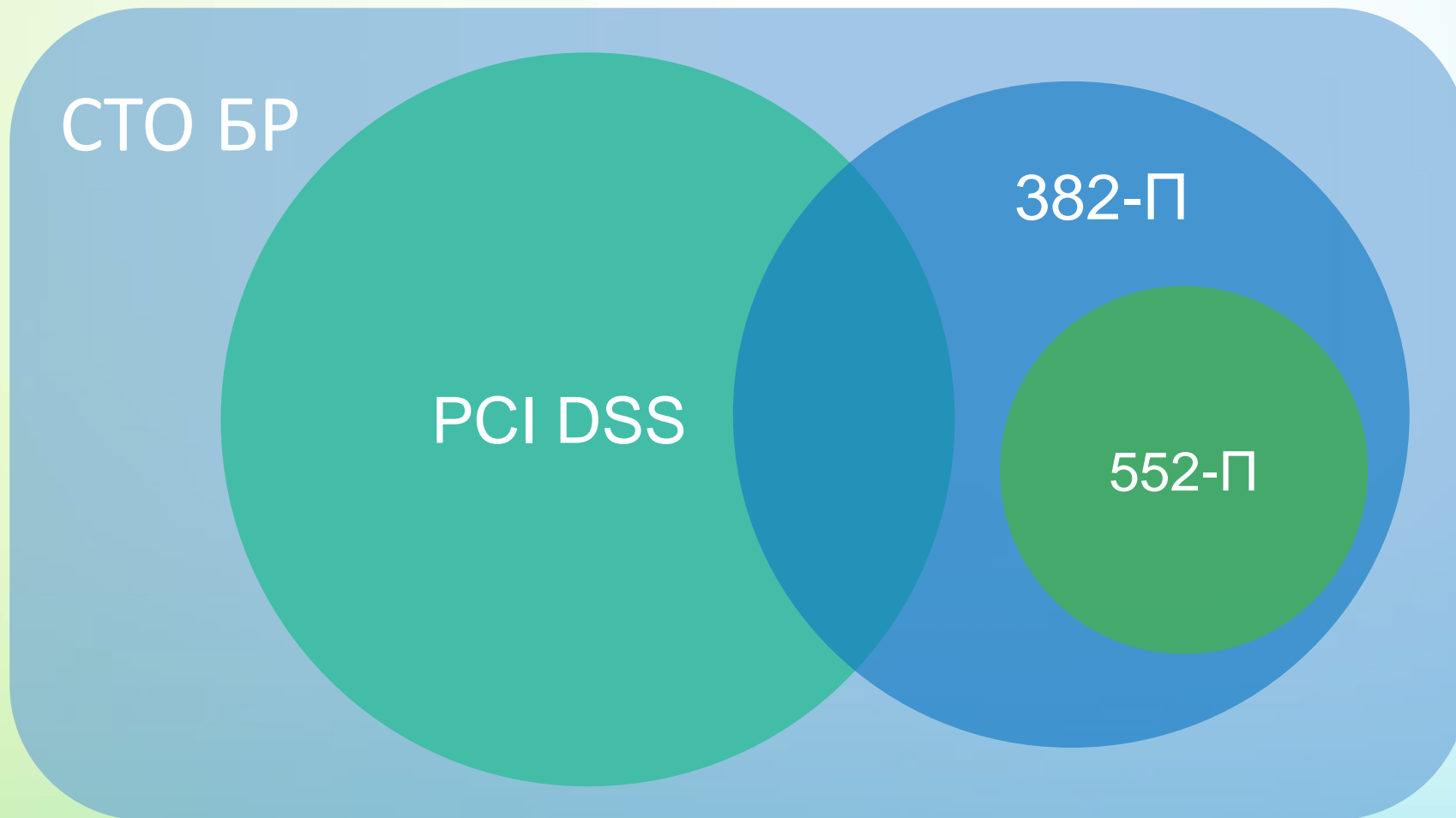
Организация взаимодействия

- Единые формы отчетности
- Единые каналы информационного обмена и предоставления отчетности – портал участника и СЭДО
- Портал участника:
 - Публичные информационные материалы
 - Коллективные обсуждения
 - Проект «Информационная безопасность» в Личном кабинете
- Рабочая группа по актуальным вопросам безопасности в ПС «Мир»
- Запуск – 2 кв. 2018

03

Оптимизация комплайнс-нагрузки

Регулирование по ИБ в банке



Оптимизация комплайнс-нагрузки: решение

Утвержденная таблица соответствия **методик оценки PCI DSS и 382-П**

N	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств	Оценка выполнения требования	Факторы, учитываемые при оценке, краткая формулировка обоснования выставленной оценки
1	2	3	4



PCI DSS Requirements and Testing Procedures	Reporting Instruction	ROC Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place with CCW	N/A	Not Tested	Not in Place
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.							
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: <ul style="list-style-type: none">• Network connections, and• Changes to firewall and router configurations.	Identify the document(s) reviewed to verify procedures define the formal processes for: <ul style="list-style-type: none">• Testing and approval of all network connections.• Testing and approval of all changes to firewall and router configurations.	<Report Findings Here>					
		<Report Findings Here>					

Один аудит = 2 оценки

Участники и статус



Центральный банк
Российской Федерации



WORK IN PROGRESS



НСПК

Спасибо за внимание!
Ваши вопросы?

Гольдштейн Анна

Заместитель начальника
Управление безопасности
АО «НСПК»

Платёжная система



15 февраля 2018,
Магнитогорск