Кросс-соответствие требованиям операторов платежных систем НПС

Перминов Владимир
Центр информационной безопасности

Центр информационной безопасности R-Style

Ключевые услуги:

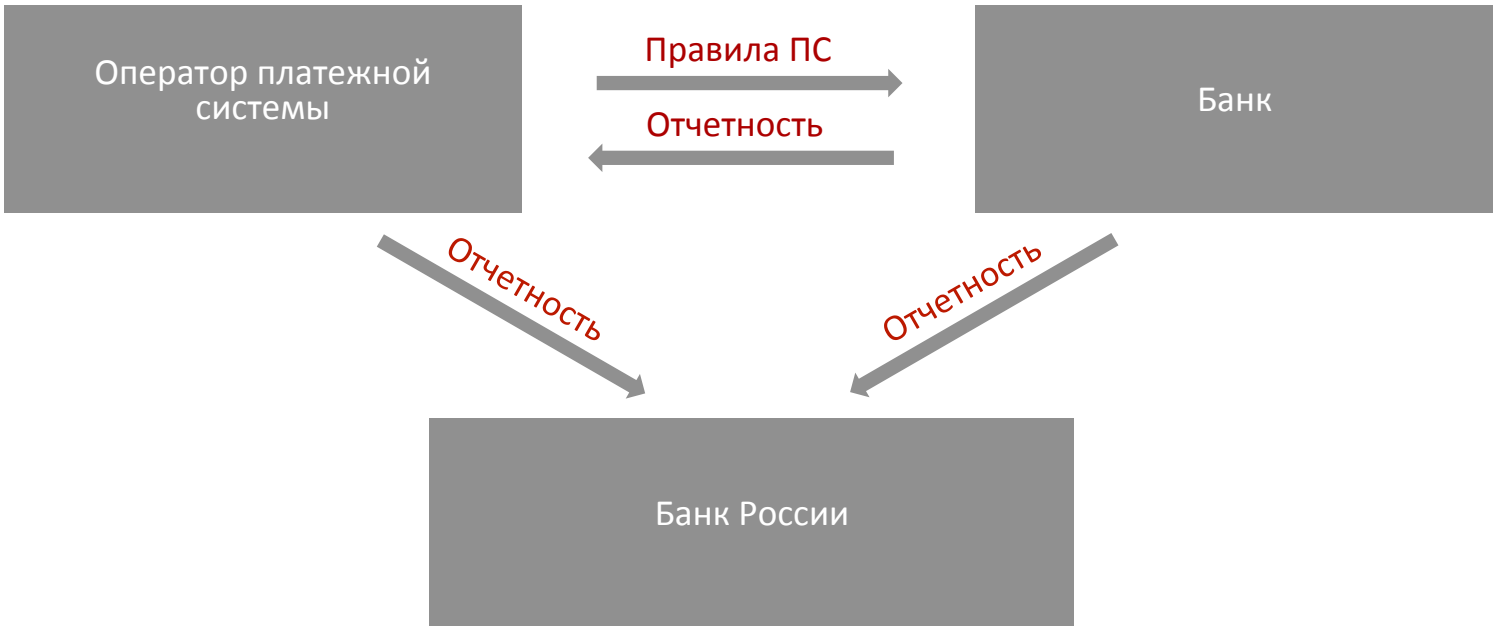
- заказная разработка систем идентификации и аутентификации, систем криптографической защиты информации;
- проектирование и внедрение Центров операций безопасности (SOC), комплексных интегрированных подсистем информационной безопасности, сложных решений DLP, WAF, DAM;
- проектирование и внедрение систем управления доступом, а также систем управления идентификацией и авторизацией (IDM+);
- консалтинговые услуги по выполнению требований законодательства, управления рисками и повышения эффективности процессов информационной безопасности.

50 экспертов, в том числе, сертифицированных (CISM, CISA, ITIL Expert, Cisco, Symantec, Oracle, IBM и др.)

Партнеры:

FORTINET, TREND MICRO, IMPERVA, KASPERSKY lab, ZECURION, Check Point SOFTWARE TECHNOLOGIES LTD., DELL, websense ESSENTIAL INFORMATION PROTECTION, symantec, McAfee, POSITIVE TECHNOLOGIES

Введение



Ключевая новация – операторы ПС получают возможность устанавливать требования по защите информации (в рамках соответствующих платежных процессов)

Проблема регулирования

Регуляторы

- РКН
- ФСТЭК
- ФСБ
- Банк России
- PCI Council
- Операторы ПС

Проблема

- Большое количество новых регуляторов
- Динамичное изменение нормативных требований

Список операторов платежных систем

Согласно ст. 15 ФЗ-161, Банк России включает информацию о зарегистрированных операторах платежных систем (ПС) в общедоступный реестр операторов ПС на основе решения о регистрации организации в качестве оператора ПС. Реестр размещен на сайте Банка России

30.01.2014 – 29 зарегистрированных операторов платежных систем (ПС)

№п/п	Оператор платежной системы							Наименование платежной системы
	Регистрационный номер оператора платежной системы	Дата регистрации оператора платежной системы (число, месяц, год)	Некредитные организации	Кредитные организации		Наименование оператора платежной системы	Место нахождения оператора платежной системы	
			ОГРН	ОГРН	Рег. номер в соответствии с Книгой государственной регистрации кредитных организаций			
1	2	3	4	5	6	7	8	9
1	0001	03.08.2012		1027739837366	1073	Коммерческий банк "Русский Славянский банк" (закрытое акционерное общество), АКБ "РУССЛАВБАНК" (ЗАО)	119049, г.Москва,ул.Донская, д. 14, стр.2	Платежная система CONTACT
2	0002	10.08.2012		1067711004437	3467	Открытое акционерное общество коммерческий банк "ЮНИСТРИМ", ОАО КБ "ЮНИСТРИМ"	127083, г. Москва, ул. Верхняя Масловка, д.20, стр.2	Международная платежная система денежных переводов "ЮНИСТРИМ"
3	0003	05.09.2012	1026301986370			Закрытое акционерное общество "Национальные кредитные карточки", ЗАО "НКК"	445012, Самарская область, г. Тольятти, ул. Коммунистическая, д. 8	Платежная система NCC (NATIONAL CREDIT CARDS)

Что могут потребовать операторы ПС?

- ISO 27001
- Тотальное шифрование
- Аттестация
- Аудит
- Противодействие продвинутым угрозам

УТВЕРЖДЕНО
постановлением Правительства
Российской Федерации
от 13 июня 2012 г. № 584

П О Л О Ж Е Н И Е

о защите информации в платежной системе

1. Настоящее Положение устанавливает требования к защите информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемой операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем и операторами услуг платежной инфраструктуры в платежной системе (далее соответственно - информация, операторы, агенты).

2. Защита информации осуществляется в соответствии с требованиями к защите информации, которые включаются операторами этих платежных систем в правила платежных систем в том числе в соответствии с настоящим Положением.

Требования операторов платежных систем

Мы проанализировали требования операторов ПС в рамках проекта по приведению платежных процессов одного из банков ТОП-50 в соответствие требованиям ИБ НПС

Название ПС	Ссылка на правила ПС	Объем, стр.	
		Всего	ИБ
Western Union	http://www.westernunion.ru/WEB-INF/pdf/Russia_PaymentSystemTerms.pdf	144	19
Visa	http://www.visa.com.ru/common/pdf/Visa_Payment_System_Operating_Regulations_Russia.pdf	266	24
Mastercard	http://www.mastercard.com/ru/company/ru/_assets/pdf/Rules.pdf	91	0
American Express	http://corp.americanexpress.com/gcs/intl/russia/corporatecards/docs/RussiaTerms.pdf	76	7
Contact	http://www.contact-sys.com/docs/rules/Contact_rules-01102012.pdf	73	1
Золотая Корона	http://www.zolotayakorona.ru/rules/Pages/-table-of-contents-2.aspx	98	8
Юнистрим	http://www.unistream.ru/support/rules/rules-of-transfers/#11	37	4

Последствия несоответствия

Со стороны Банка России

- Направление предписания об устранении недостатка.
- Наложение административного штрафа на должностных лиц в размере от 30 000 до 50 000 рублей; на юридических лиц – от 100 000 до 500 000 рублей за повторное неисполнение предписания.
- Ограничения на проведение платежных операций.

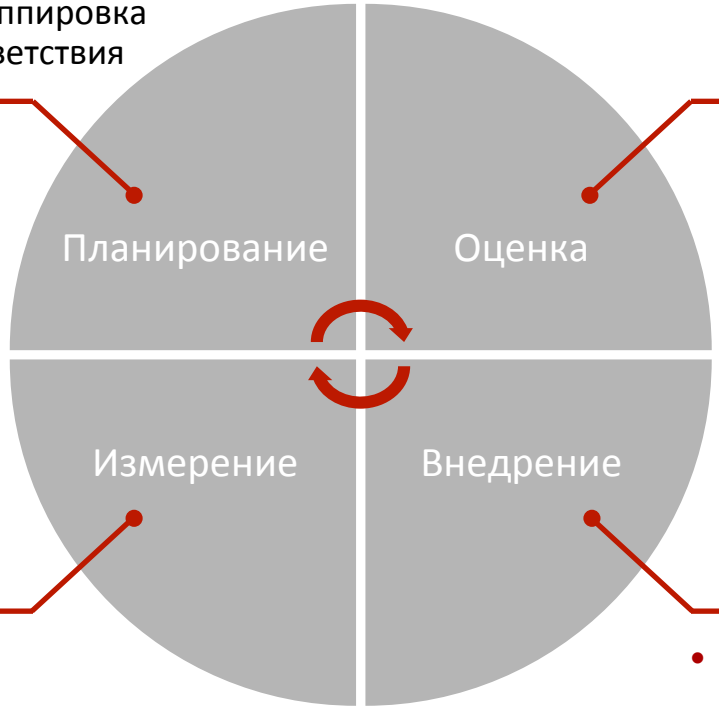
Со стороны операторов ПС

- Последствия нарушений правил ПС устанавливаются в правилах ПС.
- Примеры последствий – штрафы (правила Visa), уменьшение комиссии за перевод, приостановка членства или исключение из ПС (правила WU).
- Нарушение правил ПС является нарушением правил НПС, а значит, возможны санкции со стороны Банка России.

Подход R-Style к управлению соответствием

- Инвентаризация платежных процессов и поддерживающих активов
- Определение регуляторов (в т. ч., операторов ПС) и группировка требований в профили соответствия

- Оценка соответствия на основе профилей
- Составление матрицы соответствия платежных процессов требованиям ПС

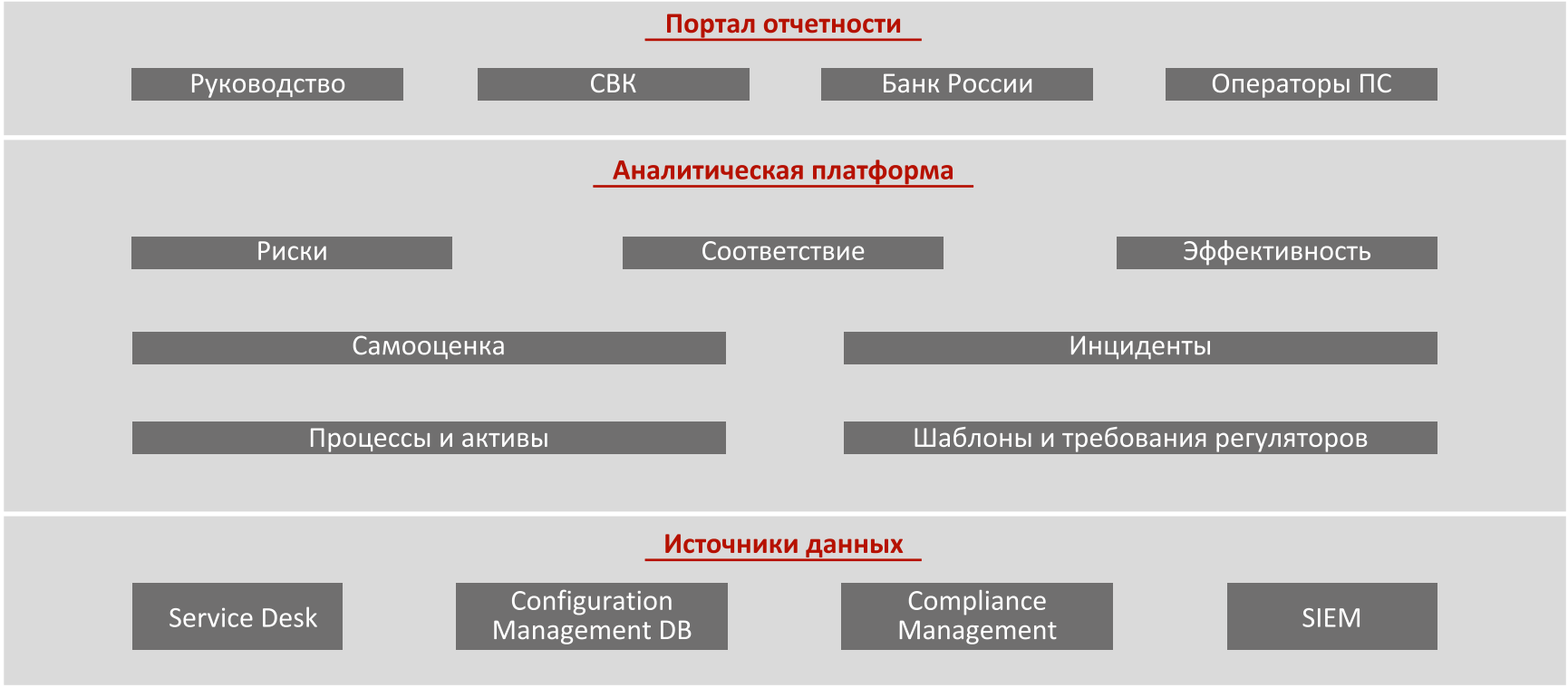


- Оценка эффективности применяемых мер ИБ
- Внешняя/внутренняя оценка соответствия требованиям ИБ

- Разработка плана мероприятий по приведению в соответствие
- Проектирование и интеграция необходимых мер защиты

Концепция системы автоматизации управления соответствием

Миссия – эффективное управление соответствием требованиям Банка России и операторов ПС, ФЗ-152, PCI DSS и другим применимым требованиям



Синергетические эффекты

Внедрение и автоматизация процесса управления соответствием дополнительно позволит:

- автоматизировать подготовку отчетности по эффективности системы ИБ;
- своевременно выявлять и эскалировать «узкие места» и проблемы в процессах ИБ;
- обосновывать развитие и модернизацию средств защиты информации в целях обеспечения соответствия и снижения рисков;
- автоматизировать и привязывать к понятным «физическим» метрикам расчёт численности службы ИБ;
- снизить стоимость и повысить эффективность контроля за уровнем безопасности отдельных подразделений и регионов.

Контактная информация

Владимир Перминов

Начальник отдела

Отдел продвижения и поддержки продаж

Центр информационной безопасности

Т. +7 (495) 514 14 10 (доб. 4863)

М. +7 (926) 671 53 86

Vladimir.Perminov@R-Style.com

ул. Рочдельская д. 15 к. 16а, г. Москва, 123022

Т. +7 (495) 640-6010

www.r-style.com