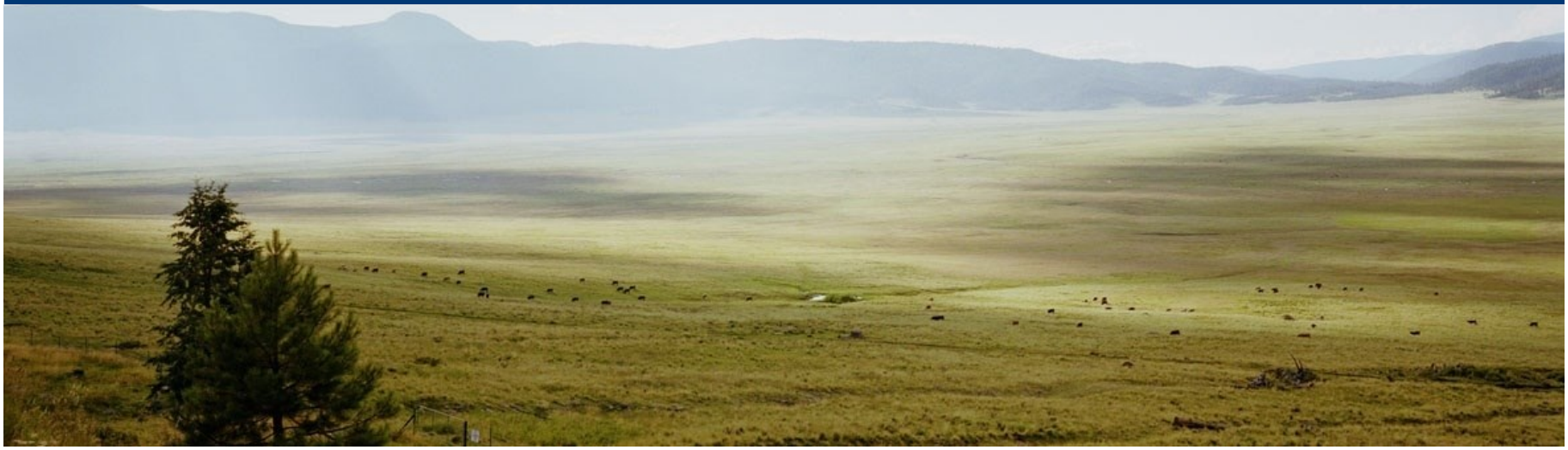
ВОЗРОЖДЕНИЕ БАНК

БАНК, КОТОРЫЙ ВСЕГДА С ТОБОЙ

Практические аспекты внедрения Стандарта PCI DCC в Банке

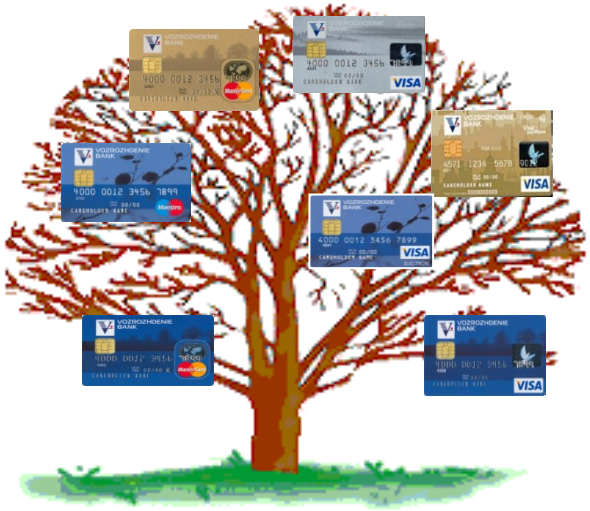


Докладчик: **Заместитель начальника СИБ Банка – начальник ОББК Ларионов Анатолий Петрович**

Дата: 29 мая 2014 года

Эмиссия и эквайринг банковских карт – одно из направлений бизнеса Банка

Более 800 штук



Более 1,5 миллионов

Более 6000 штук

Подразделения Банка, обеспечивающие функционирование Процессинговой системы

Департамент банковских карт и дистанционных каналов обслуживания

Процессинговый центр

Департамент поддержки информационных систем

Служба информационной безопасности

Управление режима и инкассации

Департамент развития банковских технологий

Другие подразделения Банка

Первый аудит Процессинговой системы (ПС) Банка на соответствие требованиям Стандарта PCI DSS прошел в декабре 2007 года

Процент несоответствия	Требования Стандарта PCI DSS											
	1	2	3	4	5	6	7	8	9	10	11	12
41%	**23**	**11**	**19**	**2**	**3**	**9**	**2**	**21**	**20**	**26**	**11**	**23**

Не актуальна Схема сети ПС

Не документирован перечень протоколов\сервисов

Не достаточны защитные меры при применении протоколов FTP и POP3

Пересмотр правил МСЭ превышает 1 квартал

Часть правил МСЭ не обеспечивают принцип минимальной достаточности

Не разработаны стандарты настроек отдельных ОС

Выявлены открытые сетевыми службами порты, не используемые для бизнес-целей

Данные, содержащие Track2, обнаружены на сетевом сервере

Не производится шифрование данных при резервном копировании

Не используется сервер централизации АБС

На некоторых системах установка критичных обновлений превышает 30 дней

Данные видеонаблюдения хранятся 2 месяца

Пароли пользователей известны администрато-рам безопасности

Журналы регистрации событий хранятся 3 месяца

Не проведено внешнее сканирование и пентест, поиск точек беспроводного доступа

Не на всех серверах обеспечивается контроль целостности критичных файлов

Не обеспечивается реагирование на инциденты ИБ в режиме 7\24

ПЛАН

действий по устранению несоответствий Банка «Возрождение» (ОАО) по результатам аудита требованиям стандарта международных платежных систем Payment Card Industry Data Security Standard (PCI DSS) v 1.1-2006

По результатам проведенного 17 - 21 декабря 2007 г. ежегодного аудита сделано заключение, что по состоянию на 21 декабря 2007 г. Банк «Возрождение» (ОАО) **не соответствует** требованиям стандарта МПС VISA и MasterCard Int. PCI DSS v 1.1 - 2006. Дата устранения несоответствия по правилам МПС не может быть позднее, чем 24 декабря 2008 г.

№ п/п	Пункт требов. PCI DSS	Описание несоответствия	Рекомендации аудитора	Подраз-ние, ответств. за устранение	Планируемые действия по устранению несоответствия	Дата устранения несоотв. планир.\ фактич.	Примечание
1	2	3	4	5	6	7	8
1	1.1.2.b.	Схема сети не актуальна (не отражены все подключения к сегменту процессингового центра, в частности не отражена управляющая сеть 172.20.10.X).	Поддерживать схему сети процессинга в актуальном состоянии. На схеме должны быть отражены все подключения к внешним сетям и все сегменты, в которых размещены ресурсы, участвующие в процессе обработки и хранения данных держателей карт.	УОИ, УБК, СИБ	УОИ назначает ответственного за подготовку телекоммуникационной схемы сети ПЦ УБК, разрабатывает совместно с УБК схему, согласовывает с СИБ и поддерживает в дальнейшем схему в актуальном состоянии	1.04.08	В качестве рекомендаций по размещению и физическому подключению СВТ ПЦ возможно использовать положения технологической инструкции 21010002-100-ТИ (2000г.). Для схемы логических подключений СВТ ПЦ целесообразно использовать формат разрабатываемых УОИ телекоммуникационных схем подключения для различных систем Банка.

Второй аудит ПС Банка на соответствие требованиям Стандарта PCI DSS прошел в марте 2009 года

Процент несоответствия	Требования Стандарта PCI DSS											
	1	2	3	4	5	6	7	8	9	10	11	12
41%	23	11	19	2	3	9	2	21	20	26	11	23
26%	5	7	4	-	1	5	-	4	3	11	5	5

Не завершена сегментация сети

Не актуальна Схема сети ПС

На TRU64 серверах не проводится настройка параметров безопасности

Не производится шифрование данных при резервном копировании

Не для всех АРМ обеспечивается требуемый срок хранения журналов регистрации событий антивируса

На некоторых системах установка критичных обновлений превышает 30 дней

Процесс идентификации уязвимостей реализован не для всех ОС

Не настроена синхронизация времени Cisco-ASA

Установка обновлений, не требующих перезагрузки ОС, проводится администраторами самостоятельно

Не завершен в полной мере ввод двухфакторной аутентификации пользователей

Не маркируются диски, содержащие данные из БД ПС

Не для всех серверов регистрируются действия сотрудников с административными полномочиями

Не на всех серверах обеспечивается контроль целостности критичных файлов

Тест на проникновение проведен, но недостатки до аудита не устранены

Не обеспечивается реагирование на инциденты ИБ в режиме 7\24

Что же делать дальше?

?

Работы по приведению ПС в соответствие требованиям Стандарта

ПЛАН
работ по приведению Процессинговой системы Банка в соответствие требованиям стандарта защиты данных держателей карт Payment Card Industry Data Security Standard (PCI DSS) v 1.2-2008

№ п/п	Пункт требов. PCI DSS	Описание несоответствия	Планируемые действия подразделений Банка по устранению несоответствия	Дата устранения несоотв. планир.\фактич.	Примечание
1	2	3	6	7	8
1	1.1.2.b	Не реализован процесс поддержки схемы сети в актуальном состоянии	УОИ: 1. совместно с СИБ и УБК доработать схему сети Процессинговой системы; 2. в документе, описывающем построение сети ПС, определить порядок внесения изменений	до 01 07	

Первый сертификат соответствия Банка требованиям Стандарта PCI DSS

PCI DSS COMPLIANCE CERTIFICATE

Информзащита
Системный интегратор

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

СЕРТИФИКАТ

Данным сертификатом ЗАО НИП «Информзащита» удостоверяет, что компания

Банк «Возрождение» (ОАО)

Успешно прошла процедуру аудита и соответствует требованиям стандарта PCI DSS Standard v. 1.2.1 в рамках согласованной области проверки, указанной в отчете Report On Compliance

Сертификат выдан: 27.12.2010

Сертификат действителен до: 27.12.2011

Директор департамента аудита _____ Эмм Максим Сергеевич

Выводы по результатам внедрения Стандарта PCI DSS

Должно быть достигнуто четкое понимание требований Стандарта PCI DSS как руководителями подразделений, так и сотрудниками, обеспечивающими поддержание требуемого уровня Процессинговой системы

Стандарт должен изучаться всеми сотрудниками банка, отвечающими за обеспечение выполнения конкретного требования

Необходимо организовать четкое взаимодействие всех подразделений Банка, обеспечивающих выполнение требований Стандарта

Необходим постоянный контроль выполнения требований Стандарта со стороны владельца соответствующего информационного ресурса – Процессинговой системы Банка

Должно осуществляться своевременное реагирование на все изменения не только в сфере индустрии платежных карт, информационных технологий, но и происходящих в Банке

Сертификационный аудит – только заключительная часть работ по обеспечению безопасности среды данных платежных карт

Банк Возрождение работает с компанией-аудитором ЗАО НИП «ИНФОРМЗАЩИТА» и постоянно поддерживает соответствие стандарту, включая:

1. независимую оценку соответствия проектных решений для новых платежных сервисов Банка

2. анализ защищённости платежных информационных систем, особенно системы с высоким уровнем риска - ДБО

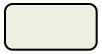
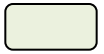
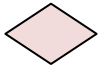
3. предварительную оценку выполнения требований за несколько месяцев до сертификации

4. консультации по совершенствованию процессов информационной безопасности платежных систем

Реализованный процессный подход к выполнению требований PCI DSS версии 2.0 позволил частично выполнить новые требования PCI DSS версии 3.0:

- в соответствии с Требованием 1.1.3 документирована Схема потоков данных держателей карт;
- в соответствии с требованиями 2.4, ведется учет системных компонентов, на которых распространяется действие Стандарта PCI DSS

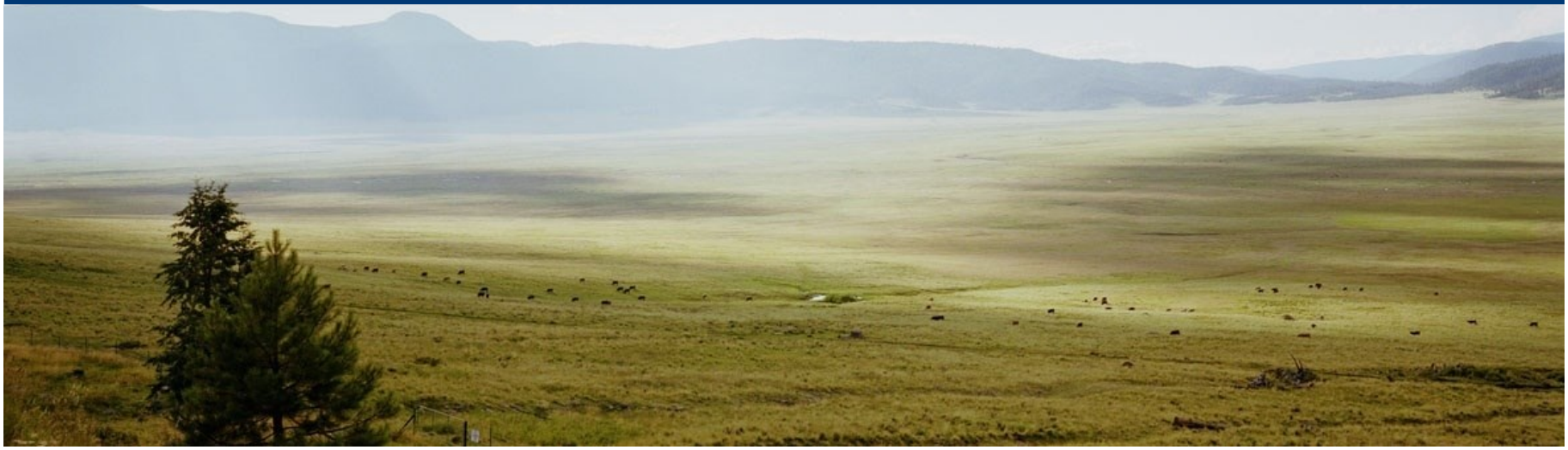
ПЕРЕЧЕНЬ РАБОТ
по поддержанию Процессинговой системы в соответствии требованиям Стандарта PCI DSS

№№ пп	мероприятия	январь	февраль	март	апрель	май	июнь	….
1	Продление договора на проведение внешнего сканирования							
2	Внешнее сканирование сети		до 30.02			до 1.05		
3	Внутреннее сканирование сети							
4	Тестирование точек беспроводного доступа		18.02			5.05		
5	Обучение сотрудников, получивших доступ к БД ПС				СЗ – до 28.04			
6	Тестирование Плана реагирования на инциденты ИБ		25.02		18.04			
7	Проконтролировать ……							

ВОЗРОЖДЕНИЕ БАНК

БАНК, КОТОРЫЙ ВСЕГДА С ТОБОЙ

БЛАГОДАРЮ ЗА ВНИМАНИЕ



Докладчик: **Заместитель начальника СИБ – начальник ОББК А. П. Ларионов**