Learn. Connect.
Collaborate. together.

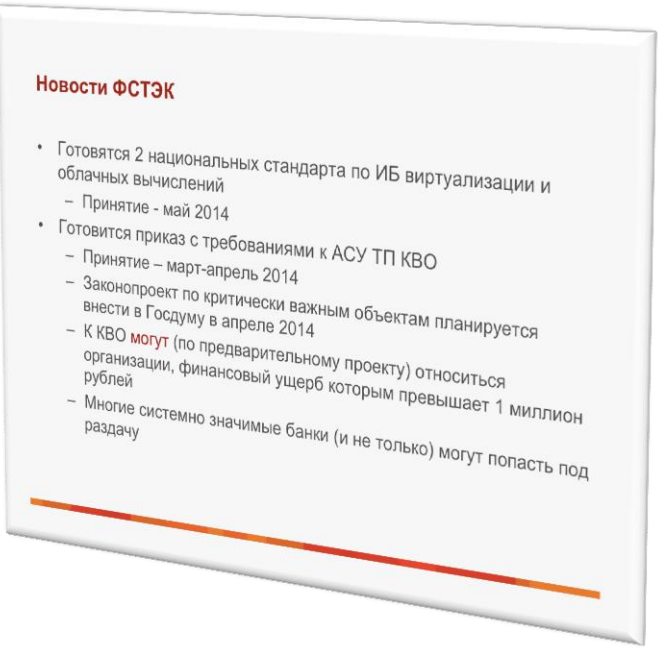
Уральский форум за 15 минут!

Многое ли изменилось за прошедший год?

Лукацкий Алексей, консультант по безопасности

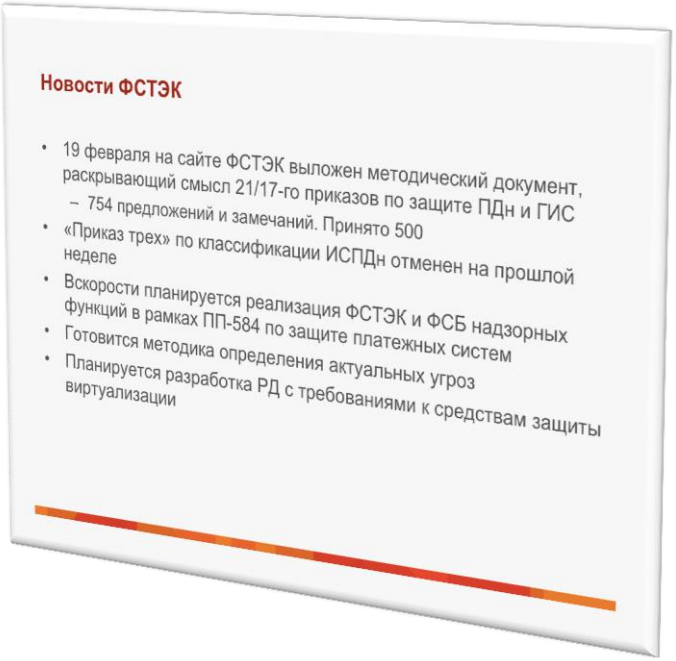
Новости ФСТЭК

- Усиление внимания к безопасности программного обеспечения
  - Новые требования к СрЗИ
  - 3 ГОСТа по уязвимостям
  - Проект ГОСТа по SDLC – конец года
  - База уязвимостей и угроз
  - Методика обновления ПО, включая сертифицированное
- Принятие законопроекта о безопасности критических информационных инфраструктур затянулось
  - Но финансовые организации (как минимум, крупные) попадут в список КИИ



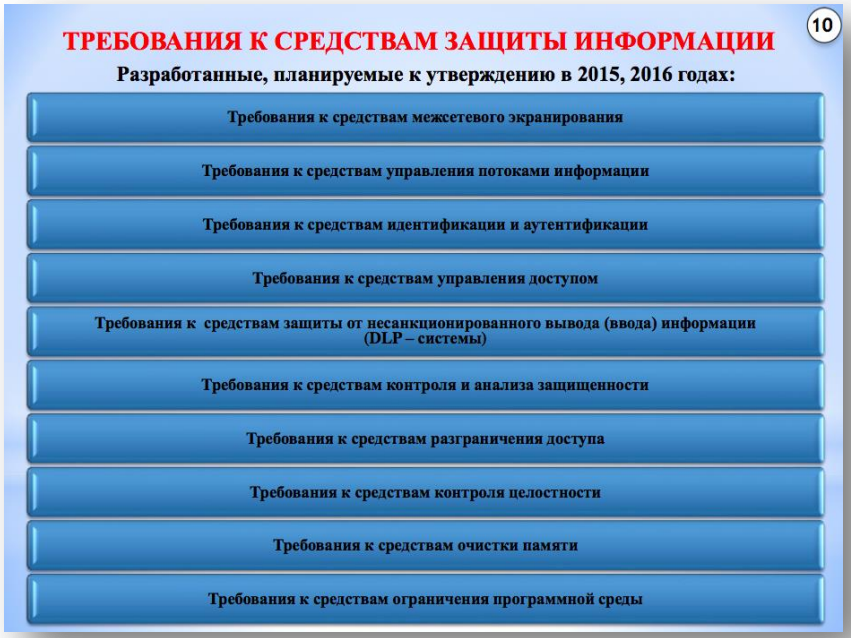
Новости ФСТЭК

- Планируется обновление 17/21-го приказов
- Планируемая реализация ФСТЭК и ФСБ надзорных функций в рамках ПП-584 по защите платежных систем не состоялась
- Готовится методика определения актуальных угроз – до конца марта должна быть опубликована



Новости ФСТЭК

- Совершенствование сертификации средств защиты информации
  - Планируется разработка большого количества РД с требованиями к средствам защиты
  - Изменение подходов к сертификации
  - Совершенствование порядка аккредитации органов по сертификации и испытательных лабораторий
  - Совершенствование порядка сертификации

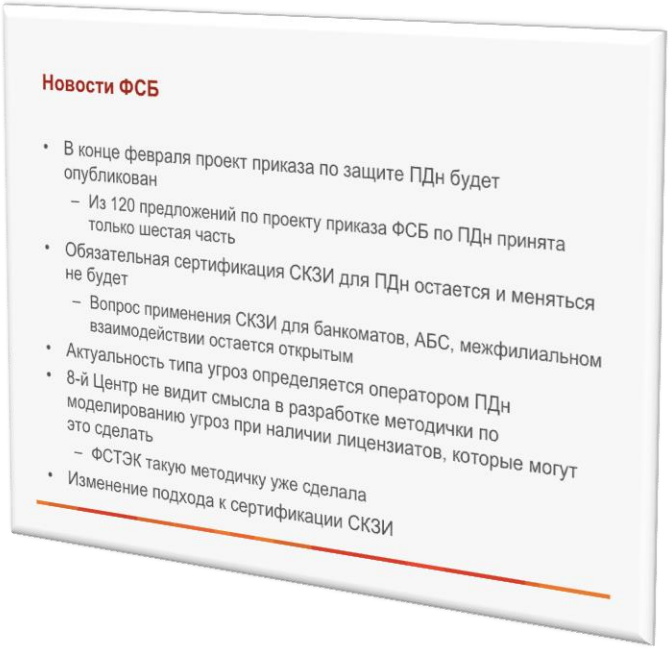


А также

- Требования к средствам защиты виртуализации, BIOS, ОС и СУБД
- Требования к средствам защиты информации от утечки по техническим каналам

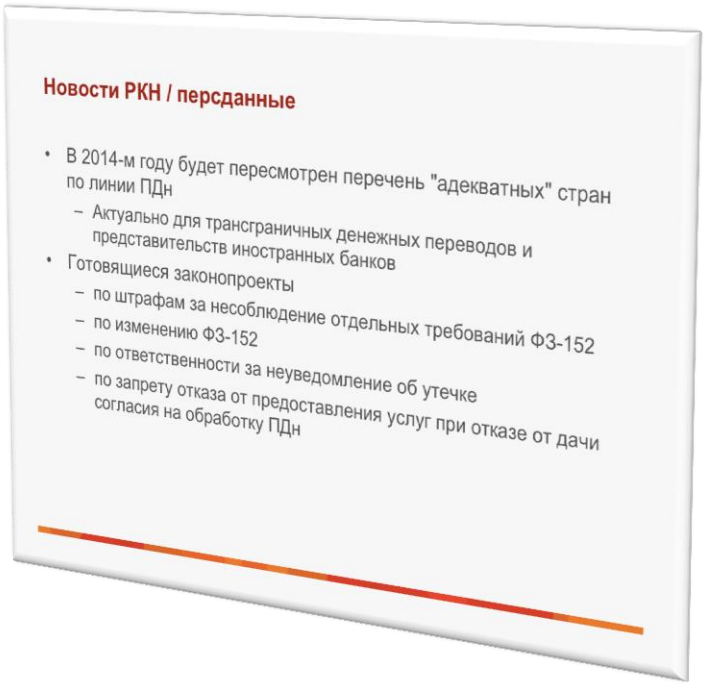
Новости ФСБ

- 378-й приказ опубликован и вступил в силу
- Произошло изменение подхода к сертификации СКЗИ
- ГосСОПКА
  - Банки будут связаны с ГосСОПКА через FinCERT и через закон о КИИ
  - Типовых решений СОПКА нет
  - Все засекречено (как обычно)
- Отечественный HSM в НСПК



Новости РКН / персданные

- Пересмотрен перечень "адекватных" стран
- Готовящиеся законопроекты
  - по штрафам за несоблюдение отдельных требований ФЗ-152
  - по изменению ФЗ-152 – завис в ГД
  - по ответственности за неуведомление об утечке – не будет
  - по запрету отказа от предоставления услуг при отказе от дачи согласия на обработку ПДн – не будет
- Незапланированный 242-ФЗ
  - В марте будет встреча банков с РКН

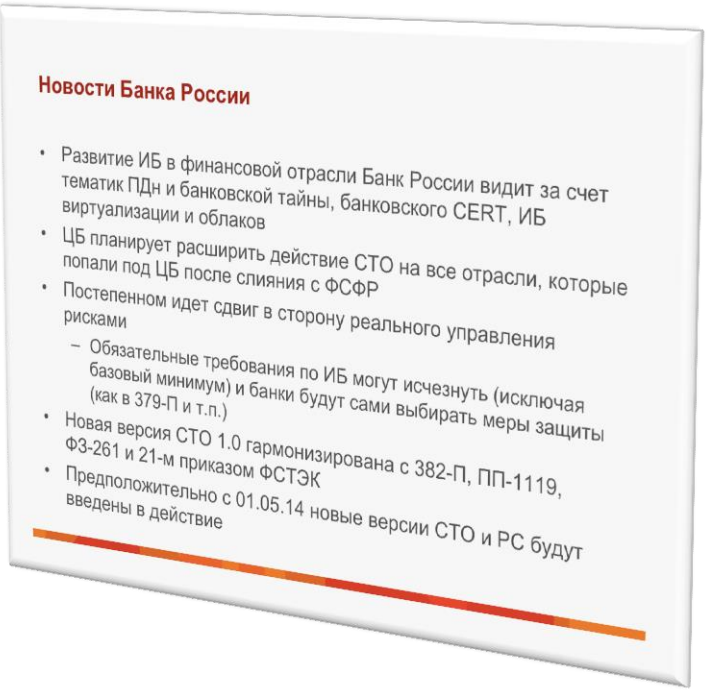


Наиболее актуальные риски и угрозы по мнению ЦБ

- Неправомерное распоряжение финансовыми средствами
- Воздействие злоумышленников на ИС и платежные приложения с целью дискредитации участников финансовой системы и препятствования ее устойчивому функционированию
- Политическое давление на экономику Российской Федерации, путем отключения финансовых сервисов
- Преднамеренное воздействие на ИС и приложения использующие оборудование и зарубежное ПО и не прошедшее надлежащую оценку соответствия ИБ

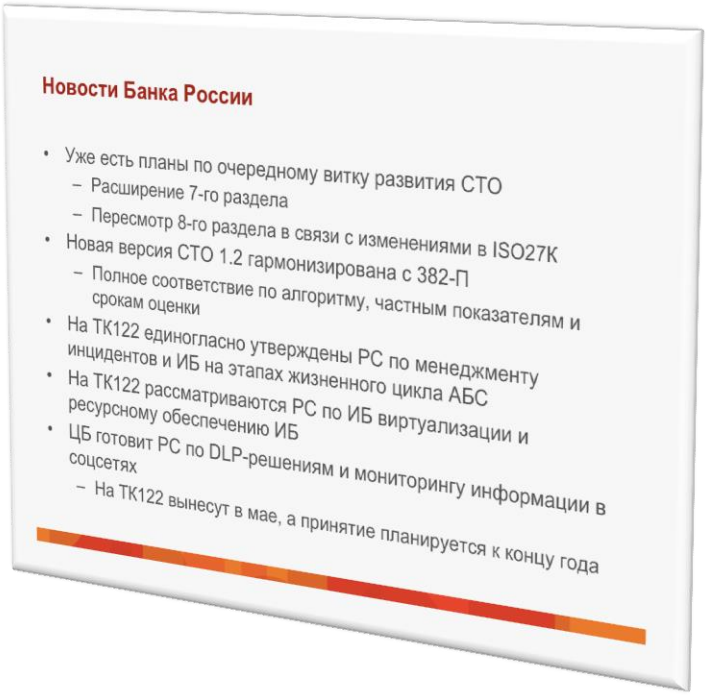
Новости Банка России

- Принята новая редакция 382-П
- Принят новый СТО 1.0 и 1.2
  - Гармонизация с 382-П и др.
- Приняты новые РС
  - По менеджменту инцидентов
  - По жизненному циклу
- Отменены «старые» РС
  - По безопасности ПДн
  - По частной модели угроз
- Сформирована и согласована с Минкомсвязь России позиция по аккредитации УЦ банков
- Сдвига в сторону управления рисками не произошло



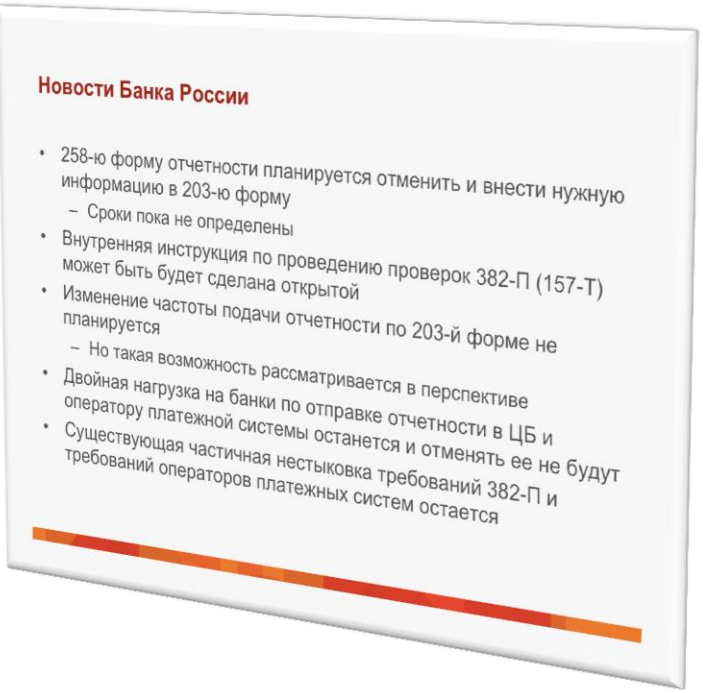
Новости Банка России

- На подписании находятся РС по ИБ виртуализации и ресурсному обеспечению ИБ
- ЦБ готовит в 2015-2016 гг. РС по предотвращению утечек, по антифроду, по распределению ролей, по облакам и аутсорсингу, по расследованию инцидентов
- ЦБ планирует пересмотреть СТО БР ИББС-1.1, РС БР ИББС-2.0, РС БР ИББС-2.1, РС БР ИББС-2.2
- ЦБ планирует расширить действие СТО 1.0 и 1.2 на все отрасли, которые попали под ЦБ после слияния с ФСФР



Новости Банка России

- Вопрос о слиянии 258-й и 203-й форм так и не решен
  - Т.к. они разработаны для разных целей – развития и надзора в НПС
- Результаты 202-й и 203-й отчетности будут опубликованы в марте
- Передавать (отменять) 203-ю отчетность под FinCERT пока не планируется
  - И цели у 203-й отчетности иные, и FinCERT пока не заработал



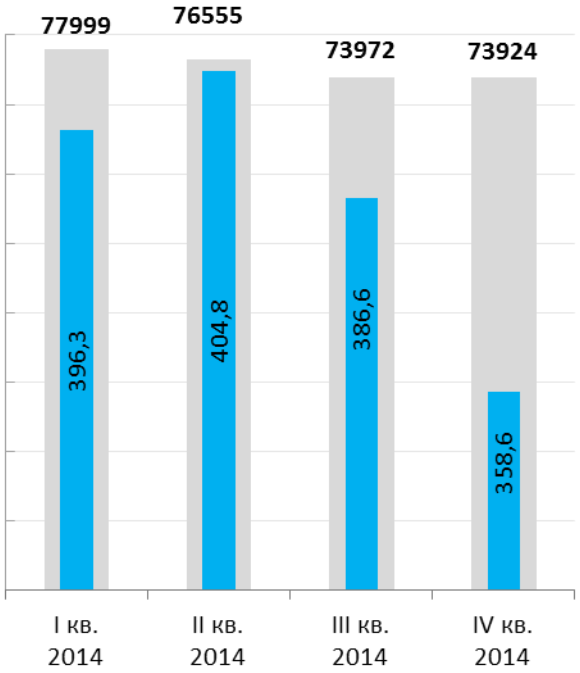
Предварительные результаты оценки по 202-й форме

Качественная оценка	Значение итогового показателя $R_{пс}$	Всего операторов	Доля, %	ОПДС	ОПС	ОУПИ
Неудовлетворительная	$0 < R_{пс} < 0,5$	20	2,38%	19	0	1
Сомнительная	$0,5 R_{пс} < 0,7$	139	16,55%	138	1	1
Удовлетворительная	$0,7 R_{пс} < 0,85$	532	63,33%	251	18	28
Хорошая	$0,85 R_{пс} < 1$	134	15,95%	130	4	7
	$R_{пс} = 1$	**15**	**1,79%**	**14**	**1**	**0**
Итого		**840**		**822**	**24**	**38**

Среднее значение $R_{пс}$ **0,74**

Предварительные результаты оценки по 203-й форме

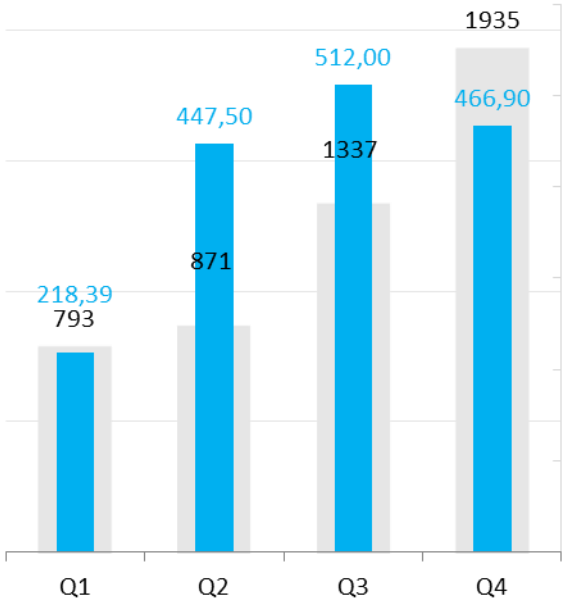
По платежным картам 0409258



Количество несанкционированных операций, ед.

Объем несанкционированных операций, млн р.

По системам ДБО 0403203

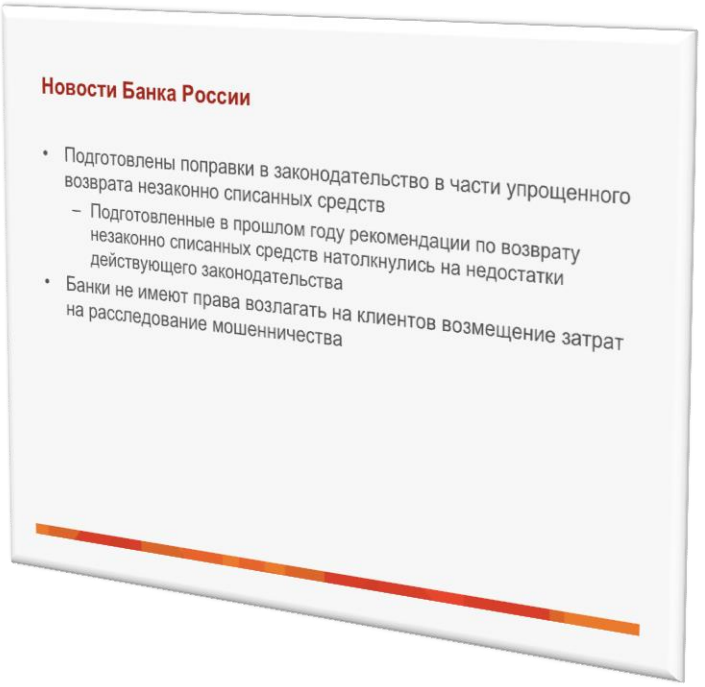


Количество инцидентов, связанных с использованием систем ДБО, ед.

Сумма, на которую были исполнены распоряжения, млн р.

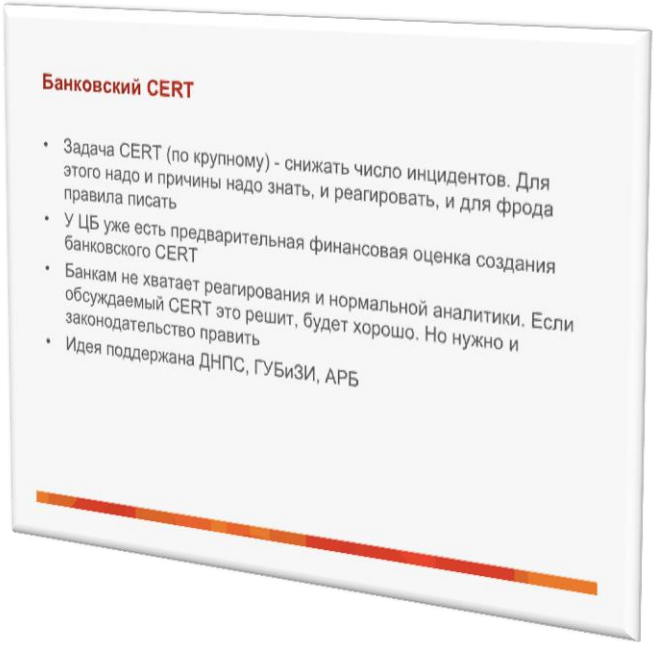
Новости Банка России

- Подготовлены изменения в законодательство направленное на противодействие преступлениям в финансовой сфере с применением современных технологий
  - ФЗ-395-1, ФЗ-86, ФЗ-161
  - В статьи 159.3 УК РФ, 187 УК РФ, 272 УК РФ, статью 152 УПК РФ, проекты статей 183.1 УК РФ и 183.2 УК РФ
  - Изменения в АПК
  - Подготовлены предложения по проекту ФЗ «О внесении изменений в некоторые законодательные акты РФ (в части противодействия хищению денежных средств)»

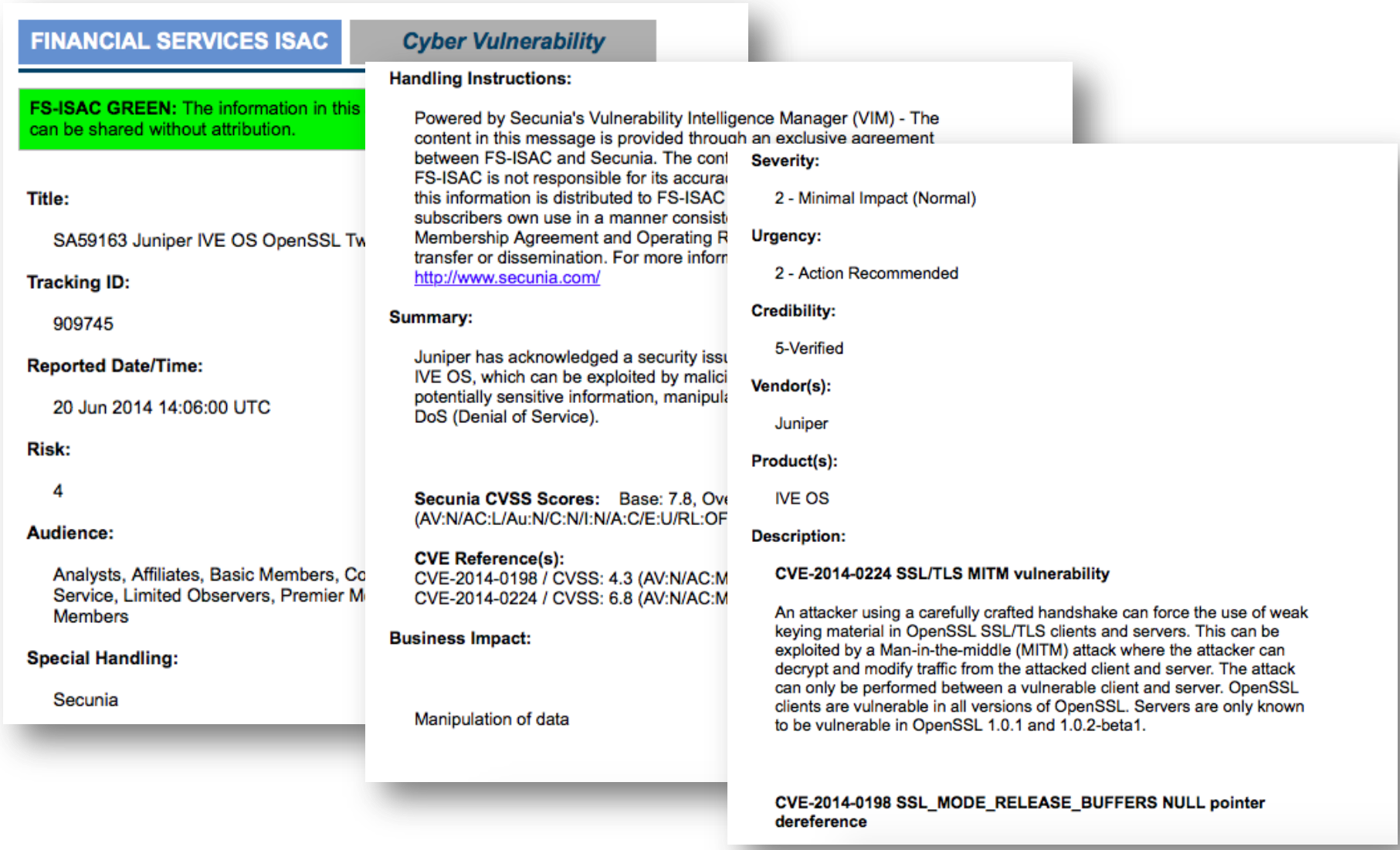


FinCERT

- Задержка с созданием FinCERT связана с Крымом и текущей экономической ситуацией
- Не только НПСК
- Большое количество вопросов, связанных с функционированием FinCERT, порядок предоставления в него информации, ответственности/обязанности, предоставляемой из FinCERT информации
  - Только техническая информация (черные списки, домены, IP, анализ malware, Threat Intelligence и т.п.) или правила антифрода?
- Интеграция с ГосСОПКА



Что выдает FS-ISAC в США?



FINANCIAL SERVICES ISAC

Cyber Vulnerability

FS-ISAC GREEN: The information in this
can be shared without attribution.

Title:

SA59163 Juniper IVE OS OpenSSL Tw

Tracking ID:

909745

Reported Date/Time:

20 Jun 2014 14:06:00 UTC

Risk:

4

Audience:

Analysts, Affiliates, Basic Members, Co
Service, Limited Observers, Premier M
Members

Special Handling:

Secunia

Handling Instructions:

Powered by Secunia's Vulnerability Intelligence Manager (VIM) - The
content in this message is provided through an exclusive agreement
between FS-ISAC and Secunia. The cont
FS-ISAC is not responsible for its accura
this information is distributed to FS-ISAC
subscribers own use in a manner consist
Membership Agreement and Operating R
transfer or dissemination. For more inform
http://www.secunia.com/

Summary:

Juniper has acknowledged a security issu
IVE OS, which can be exploited by malici
potentially sensitive information, manipul
DoS (Denial of Service).

Secunia CVSS Scores: Base: 7.8, Ov
(AV:N/AC:L/Au:N/C:N/I:N/A:C/E:U/RL:OF

CVE Reference(s):
CVE-2014-0198 / CVSS: 4.3 (AV:N/AC:M
CVE-2014-0224 / CVSS: 6.8 (AV:N/AC:M

Business Impact:

Manipulation of data

Severity:

2 - Minimal Impact (Normal)

Urgency:

2 - Action Recommended

Credibility:

5-Verified

Vendor(s):

Juniper

Product(s):

IVE OS

Description:

CVE-2014-0224 SSL/TLS MITM vulnerability

An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server. The attack can only be performed between a vulnerable client and server. OpenSSL clients are vulnerable in all versions of OpenSSL. Servers are only known to be vulnerable in OpenSSL 1.0.1 and 1.0.2-beta1.

CVE-2014-0198 SSL_MODE_RELEASE_BUFFERS NULL pointer dereference

Импортозамещение и санкции

- В прошлом году про импортозамещение и санкции не говорили
- Снижение числа импортных средств защиты, прошедших сертификацию в ФСТЭК в 2014-м году
  - С 123 до 113
- Появление требований Банка России к отечественному ПО в социально значимых платежных системах
- Усиление требований к оценке соответствия для средств защиты, применяемых в Банке России и НСПК
- Отказ от неактуальности угроз 1-го и 2-го типа (по ПП-1119)
- Бурные дебаты с отсутствием четкого результата
  - Непонимание целей и заказчика импортозамещения, а также отсутствие продуктов-заместителей в должном количестве

НСПК

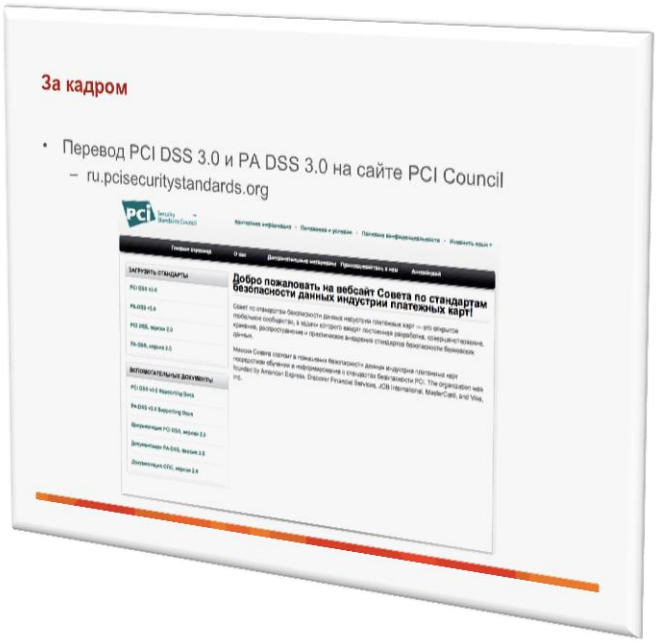
- Созданы НСПК и СПФС
  - Новая геополитическая ситуация
  - Новые риски
- Запуск НСПК с повышенными требованиями по безопасности
- НСПК – часть НПС и подчиняется требованиям 382-П
- Отдельных документов по безопасности НСПК пока не планируется

Все в СРО по ИБ

- Вновь поднимается идея об оценке качества ПО АБС и платежных приложений
  - Распоряжение Совета Безопасности
  - Не до конца проработан механизм оценки – через СРО или сертификацию?
- Кто будет входить в СРО?
  - Разработчики ПО
  - Интеграторы
  - Аудиторы
- Много открытых вопросов про СРО
  - Как минимум, требуется изменение законодательства

За кадром: PCI DSS

- На форуме ни разу не упоминался стандарт PCI DSS
- Предыдущая редакция перевод PCI DSS 3.0 и PA DSS 3.0 на сайте PCI Council не выдерживала никакой критики
  - ru.pcisecuritystandards.org
- В настоящий момент идет очередной виток перевода PCI DSS 3.0
  - Согласовано с PCI Council
  - Под эгидой АБИСС
  - Перевод осуществляется компанией ООО «Дейтерий»

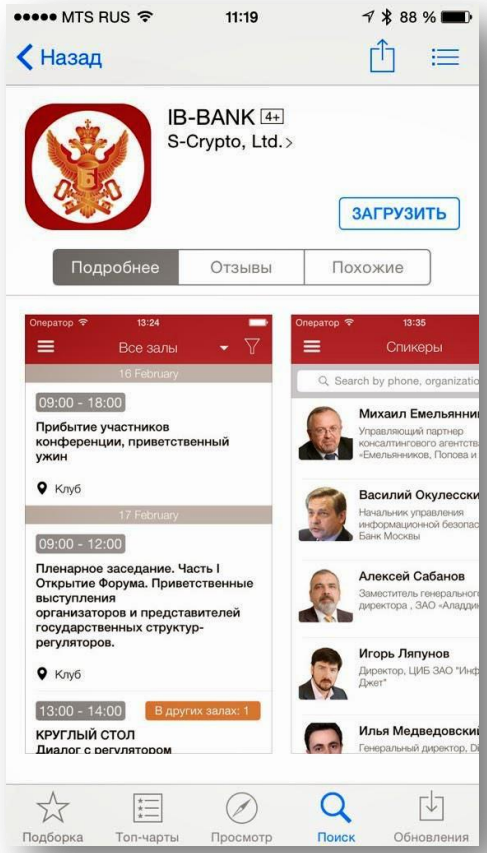


Особенности выступлений: ничего не поменялось

- Непонимание банковской специфики и потребностей целевой аудитории со стороны интеграторов и производителей
- Неумение выступать публично и готовить презентации
  - Их часто не видно даже с 1-го ряда
- Отсутствие тренировки для молодых организмов
- Голимая реклама

Новые фишки форума

- Мобильное приложение
  - Программа, спикеры, объявления, голосование
- Закрытая сессия
  - По FinCERT
- Воркшопы
- Больше круглых столов
  - Живое общение
- Бесплатное обучение от УЦ
- Киберучения
- Типография Авангард-Про
  - Книги по ИБ



http://ural.ib-bank.ru/

security-request@cisco.com

Благодарю вас за внимание