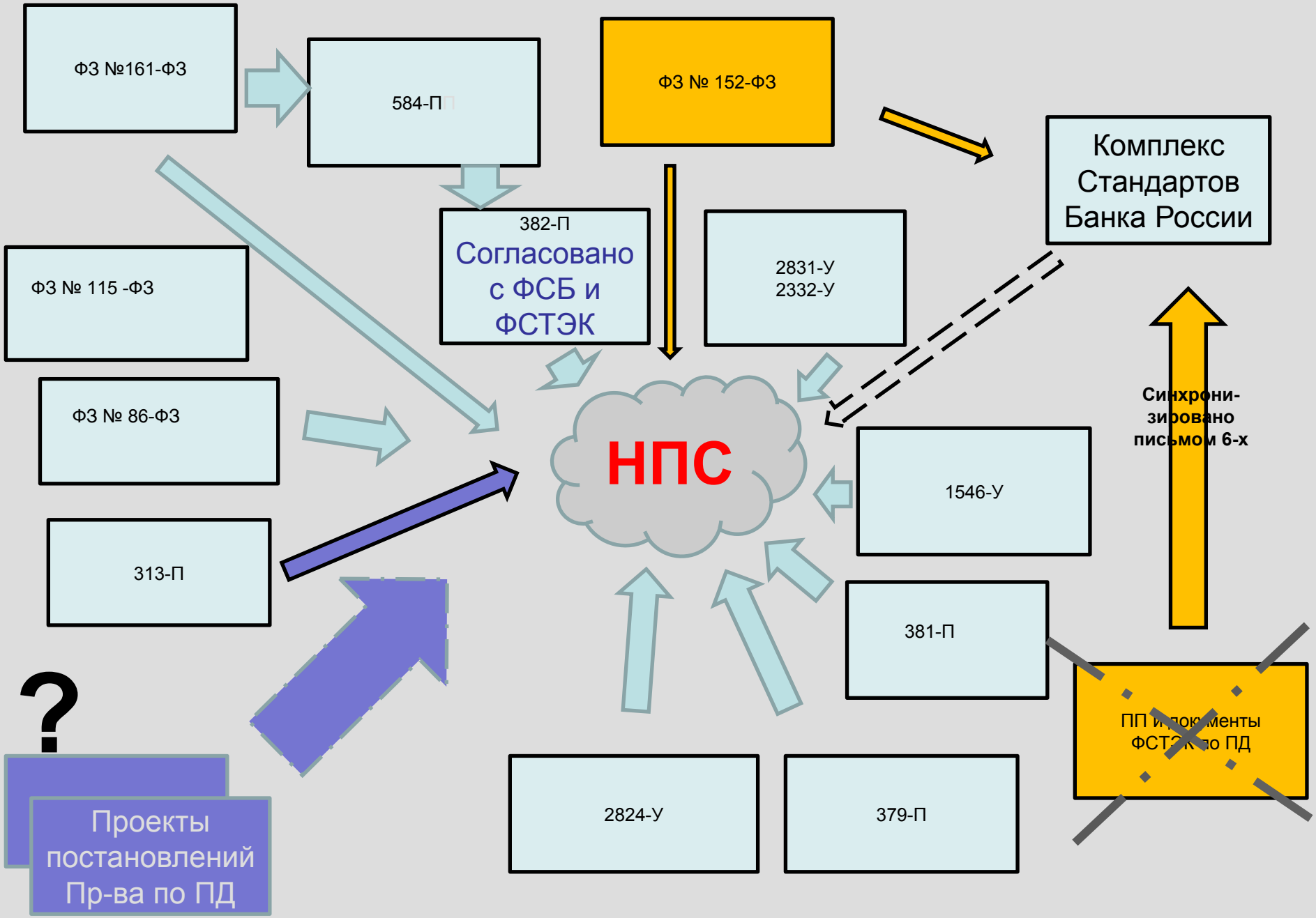
V Юбилейный Уральский форум «Информационная безопасность банков»

Вопросы регулирования, надзора и наблюдения в части защиты информации при осуществлении перевода денежных средств в национальной платежной системе

Курило Андрей Петрович
Заместитель Директора
Департамента
регулирования расчетов

Банное, 12
Февраля
2013 года


ФЗ №161-ФЗ
584-П
ФЗ № 152-ФЗ
Комплекс Стандартов Банка России
382-П
Согласовано с ФСБ и ФСТЭК
2831-У
2332-У
ФЗ № 115 -ФЗ
ФЗ № 86-ФЗ
НПС
Синхрони-зировано письмом 6-х
1546-У
313-П
381-П
?
ПП и документы ФСТЭК по ПД
Проекты постановлений Пр-ва по ПД
2824-У
379-П

Положение дел

До выхода ФЗ №161-ФЗ

Понятие «платежная система» отсутствовало

- Использовалась рекомендательная форма регулирования информационной безопасности в КО (Стандарты Банка России, рекомендации, опросы)
- Работы проводились вне рамок надзорной деятельности, осуществляемой Банком России
- Отсутствовала отчетность

После выхода ФЗ№161-ФЗ

Введены понятия «Национальная и платежная система» и определена область регулирования для Банка России

- Регулирование вопросов защиты информации при переводе денежных средств осуществляется в рамках надзора в НПС
- Улучшение защиты информации при переводе денежных средств осуществляется рамках деятельности по наблюдению и мониторингу в НПС
- Организация сбора и анализа отчетности

Качественное изменение картины в сфере регулирования после выхода ФЗ 161

1. Центральный Банк Российской Федерации перешел от рекомендательной к нормативной форме регулирования вопросов обеспечения защиты информации при переводе денежных средств в НПС.
2. Регулирование осуществляется в рамках мероприятий по надзору и наблюдению за субъектами НПС.
3. Результаты проверок субъектов НПС будут использованы для оценки соответствия закону и требованиям Банка России, а также о вынесении суждения о качестве управления рисками бесперебойности функционирования и безопасности.

О задачах и деятельности в области защиты информации

Задачи - способствование бизнес - целям банка и повышение эффективности используемых им проектов и продуктов путем максимального снижения рисков и издержек.

Цель деятельности – обеспечение, в части касающейся, устойчивости и стабильности НПС, бесперебойности ее функционирования, максимальное сокращение хищений денежных средств, создание условий развития и совершенствования платежных систем, платежной инфраструктуры с учетом минимизации рисков безопасности.

Достигается:

- нормативным регулированием;
- реализацией комплекса мероприятий по надзору и наблюдению;
- сбором и анализом отчетности

Реализуется:

- В правилах платежных систем
- В системе управления рисками в виде порядка обеспечения защиты информации в платежной системе
- В системе управления рисками бесперебойности функционирования платежных систем как фактор влияния в составе операционных рисков

Деятельность в сфере регулирования вопросов защиты информации в НПС

Надзор

Цель: контроль выполнения законов и нормативных актов Банка России

Форма работы

1. Нормативное регулирование

   Положение 382-П

   Указание 2831-У

   Методики проверок выполнения требований Федеральных законов, положений и указаний Банка России

2. Сбор и анализ отчетности

   О выполнении норм. требований

   Об инцидентах

3. Проверки

   Комплексные КО, ОПДС

   инспекционные поднадзорных Орг.

4. Обработка и анализ данных

   выработка мер надзорного реагирования

Наблюдение (+мониторинг)

Цель: улучшение деятельности ПС, их развитие на основе рекомендаций Банка России

Форма работы

1. Сбор и анализ информации
2. Оценка соответствия рекомендациям Банка России к которым относятся собственные рекомендации ЦБ, а также рекомендаций по использованию стандартов или лучшей мировой практики при условии опубликования их на русском языке
3. Инициация изменений по результатам оценки

Особенности нормативного регулирования

ребования положения 382-П распространяются на ОПДС, БПА, ПБСА, ОПС, ОУПИ.

В НПС присутствует две группы объектов регулирования и как следствие, два методических подхода:

а) Группа ОПДС (КО, ЦБ, ВЭБ). В отношении их осуществляется прямое применение требований нормативных документов Банка России (для всех ОПДС).

б) Группа ПС, участниками которых являются ОПДС. В отношении их предусматривается включение требований в правила ПС и распространение их на участников при присоединении их к правилам.

Особенности:

Выполнение требований по безопасности и контроль у БПА и БПСА осуществляет ОПДС

в) Нормативные требования по отчетности по формам №№ 0403202 0403203, установленные Указанием 2831-У являются документами прямого действия.

Исключения:

- отчетность по форме 0403203 операторами платежных систем не представляется.

Особенности механизма применения требований к среде

1. КО может быть: ОПДС, участником ПС Банка России, Участником N ПС, ОПС, элементом ИПС, например, расчетным центром.
2. Применение различных наборов требований по безопасности к одному и тому же субъекту со стороны разных ПС, в которых он участвует, дублирование этих требований, недопустимо.
3. Недопустимо также дублирование отчетности по указанию 2831-У

Вывод:

Требования по безопасности, предъявляемые субъектами НПС друг к другу, должны быть едины и базироваться на Положении 382-П.

Требования по защите информации про переводе денежных средств мы единообразно внедряем в правила платежных систем, когда их регистрируем.

Закон дает такую возможность.

Важно:

Минимально при этом нагрузить рынок нашими новыми требованиями.

Об отчетности в области защиты информации при переводе денежных средств

Отчетность дает знание объекта регулирования. Без этой информации невозможно разработать эффективные защитные меры, проводить сбалансированную политику управления безопасностью, в том числе и финансирования.

Цели сбора отчетности

- Получение объективной картины об уровне, видах, специфике, частоте, распространению и трендах инцидентов связанных с нарушением требований защиты информации при переводе денежных средств в НПС
- Получение информации о степени соответствия операторов по переводу денежных средств и платежных систем (через операторов платежных систем) требованиям Банка России
- Использование полученной информации для выработки предложений и мер надзорного регулирования, а также выработки предложений по улучшению и совершенствованию деятельности операторов по переводу денежных средств и поднадзорных организаций, а также по совершенствованию требований Банка России по защите информации и совершенствованию мер защиты систем ДБО и ЭСП.

Направления сбора отчетности

- По видам действий, направленных на добывание атрибутов управления счетом
- По видам оборудования, на котором совершались мошенничества
- По суммам, на которые совершены покушения
- По похищенным суммам
- По видам платежных систем, через которые выводятся обналиченные средства
- Информация должна допускать обработку в разрезе региона и периода времени по каждому показателю.

Как распределяются инциденты на сегодняшний день

- Фрод 50%
- Сбои в результате ошибок или преднамеренных действий персонала 15 %
- Компроментация ключей подписи 7%
- Подмена экрана 7%
- Отказ в обслуживании 0.7%
- Воздействие вируса – комплексный параметр, сложно определяется
- DDoS-атаки – фактически не определяются

Направления деятельности.

Определяются:

- Стратегией развития НПС, изложенной в «Проекте основных направлений»
- Результатами анализа собираемой отчетности
- По результатам надзорной деятельности и деятельности по наблюдению.

Задачи, требующие решения

А. На уровне регулятора

- Улучшение и совершенствование координации работ в сфере безопасности ДБО и ЭСП
- Совершенствование системы сбора отчетности и самой отчетности
- Совершенствование методического аппарата, повышение точности измерений и качества представляемой информации
- Совершенствование и расширение нормативных требований по безопасности. Доработка и развитие нормативных документов, устанавливающих требования по безопасности
- Развитие стандартов защиты информации при переводе денежных средств как лучших практик
- Создание системы стандартов разработки систем ЭСП, и ДБО, Содействие в создании системы сертификации этих систем.

Б. На уровне рынка

- Улучшение координации и взаимодействия заинтересованных субъектов
- Создание эффективной централизованной системы борьбы с фродом, действующей в интересах всего банковского сообщества
- Создание системы сертификации продуктов ЭСП и ДБО по требованиям безопасности

Благодарю за внимание!

А. Курило
ЦБ РФ, ДРР