КУРС:

НАЦИОНАЛЬНАЯ ПЛАТЕЖНАЯ СИСТЕМА. ЗАЩИТА ИНФОРМАЦИИ В НПС

ЦАРЕВ ЕВГЕНИЙ

ОБЩИЕ ВОПРОСЫ

- Ожидания;
- Цели и задачи курса;
- Состав курса;
- Программа;
- Перерывы;
- Общие организационные вопросы.

«ГЛОБАЛЬНАЯ СИСТЕМА РАСЧЕТОВ»

- Банк международных расчетов (БМР);
- Европейский центральный банк;
- Всемирный банк;
- Международный валютный фонд;

БАНК МЕЖДУНАРОДНЫХ РАСЧЕТОВ (БМР)

- **Создан в мае 1930 г. в Базеле (Швейцария);**
- **На основе международного соглашения Бельгии, Великобритании, Германии, Италии, Франции, Японии и Швейцарии для распределения репарационных выплат Германии по Версальскому договору;**

- Акционерное общество, учрежден как международная организация;

БАНК МЕЖДУНАРОДНЫХ РАСЧЕТОВ (БМР)

- В 1996 г. в члены БМР был принят ЦБ РФ;
- Членами БМР являются центральные банки 56 стран;
- Основная задача – координация деятельности центральных банков и обеспечение финансовой стабильности.

БАНК МЕЖДУНАРОДНЫХ РАСЧЕТОВ (БМР)

В рамках БМР действуют:

- Базельский комитет по банковскому надзору (BCBS)
- Комитет по платежным и расчетным системам (CPSS/КПРС)
- Институт финансовой стабильности (FSI)
- И т.д.

КОМИТЕТ ПО ПЛАТЕЖНЫМ И РАСЧЕТНЫМ СИСТЕМАМ

- Основные компетенции БМР в части НПС сосредоточены в Комитете по платежным и расчетным системам (КПРС);
- КПРС был создан в 1990 г. Group of Ten (центральные банки 10 государств);
- В рамках БМР действует с 2009 г.

КОМИТЕТ ПО ПЛАТЕЖНЫМ И РАСЧЕТНЫМ СИСТЕМАМ

- **Деятельность КПРС направлена на совершенствование инфраструктуры финансового рынка с позиции совершенствования платежных и расчетных систем;**
- **Осуществляет мониторинг и анализ достижений развития платежных, расчетных и клиринговых систем отдельных стран, а также систем трансграничных и мультивалютных расчетов;**

ПОНЯТИЕ И СТРУКТУРА НПС

В общепринятом значении:

- **НПС –** ***подсистема финансовой системы государства, которая обеспечивает экономических субъектов платежными услугами.***

  При этом НПС представляет собой совокупность платежных элементов национальной финансовой системы, включая государственные и коммерческие платежные и расчетные системы

ПОНЯТИЕ И СТРУКТУРА НПС

КПРС «Общее руководство по развитию национальной платежной системы»:

- **НПС –** ***институциональные и инфраструктурные механизмы финансовой системы, используемые при инициации и переводе денежных требований в форме обязательств ЦБ и коммерческих банков;***
- **Платеж –** ***это перевод денежного требования.***

ПОНЯТИЕ И СТРУКТУРА НПС

КПРС «Общее руководство по развитию национальной платежной системы». НПС включает в себя:

- **Платежные инструменты, для инициирования и направления перевода ДС со счетов плательщика на счет получателя;**
- **Платежную инфраструктуру для исполнения и клиринга платежных инструментов, обработки и передачи платежной информации, а также перевода ДС между институтами плательщика и получателя;**
- **Финансовые институты, предоставляющие счета для осуществления платежей, платежные инструменты и услуги потребителям, а также предприятия и организации, являющиеся операторами сетей операционных, клиринговых и расчетных услуг по платежам для этих финансовых институтов**
- **Рыночные механизмы, такие как договоренности, обязательные предписания и договоры по созданию различных платежных инструментов и услуг, формированию цен на них, а также их предоставлению и приобретению**
- **Законы, стандарты, правила и процедуры, установленные законодательными, судебными и регулирующими органами, которые определяют и регулируют механизм перевода платежей и рынки платежных услуг**

СХЕМА НПС В ДОКУМЕНТАХ КПРС

УЧАСТИЕ БАНКОВСКОЙ СИСТЕМЫ В РАЗВИТИИ НПС

КПРС рекомендует применять принципы:

- **Сохранять главенствующую роль ЦБ (оператор, регулятор, контролер, пользователь, катализатор развития);**
- **Повышать роль устойчивой банковской системы;**

ПЛАНИРОВАНИЕ ИНИЦИАТИВ РАЗВИТИЯ НПС

КПРС рекомендует:

- **Осознавать сложность процесса;**
- **Концентрироваться на потребностях;**
- **Устанавливать четкие приоритеты;**
- **Считать реализацию ключевым этапом;**

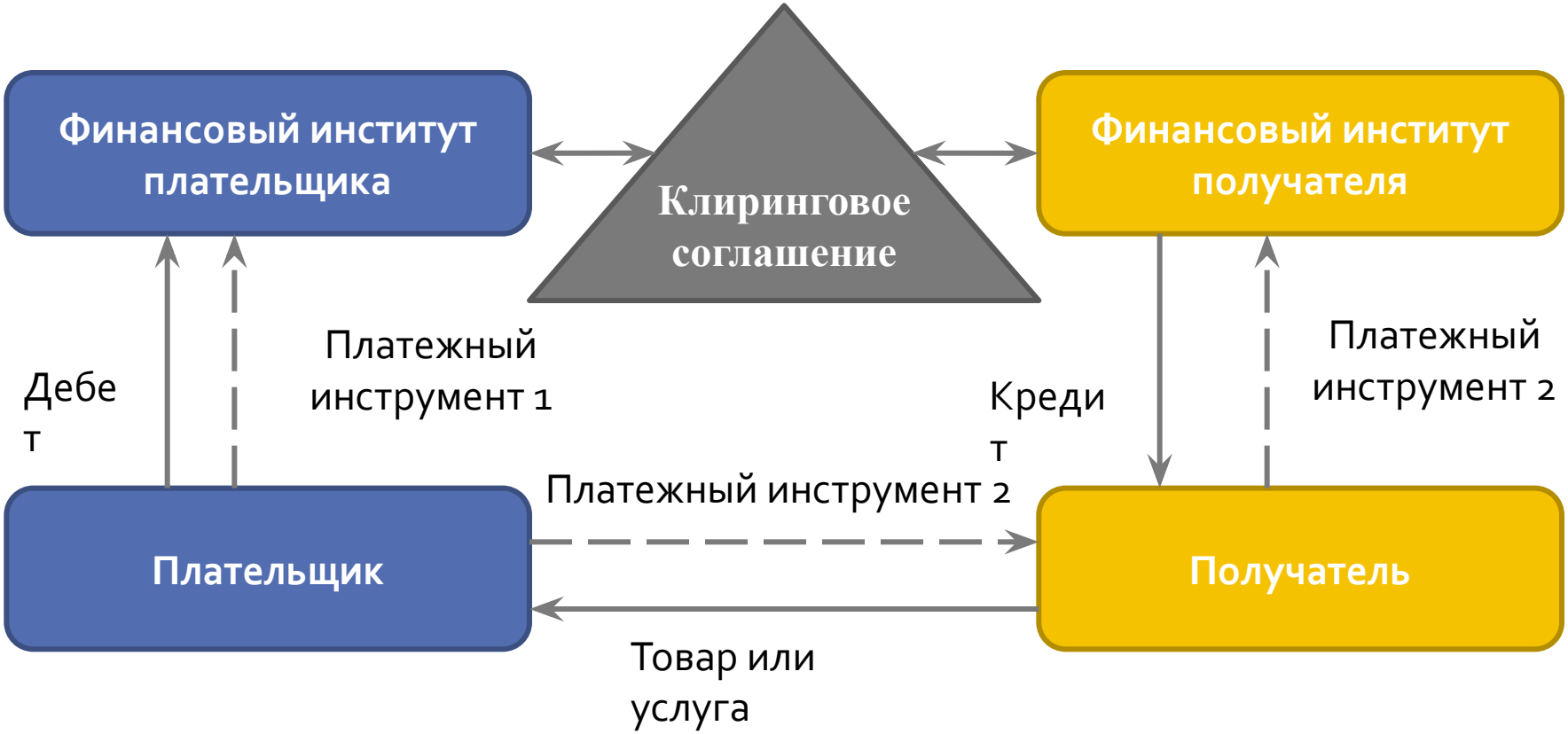
РАЗВИТИЕ ИНСТИТУЦИОНАЛЬНЫХ МЕХАНИЗМОВ НПС

- **Принцип содействия развитию рынка;**
- **Принцип вовлечения заинтересованных сторон;**
- **Принцип сотрудничества в целях эффективного наблюдения;**
- **Принцип обеспечения правовой определенности;**

РОЗНИЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

- **Большое число участников;**
- **Большой набор платежных инструментов;**
- **В большей степени используются частные провайдеры;**

РОЗНИЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ



РОЗНИЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

Платежный процесс включается в себя 3 подчиненных взаимосвязанных процесса:

- **Операционный процесс;**
- **Клиринговый процесс;**
- **Расчетный процесс;**

ОПЕРАЦИОННЫЙ ПРОЦЕСС

Обеспечивает инициирование, подтверждение и перевод платежа. В общем случае включает в себя:

- **Проверка подлинности сторон;**
- **Подтверждение правильности оформления платежного инструмента;**
- **Проверка платежеспособности плательщика;**
- **Авторизация перевода ДС финансовым институтам плательщика и получателя;**
- **Передача информации финансовым институтом плательщика в финансовый институт получателя;**
- **Проведение операции;**

ПРОЦЕСС КЛИРИНГА

Обеспечивает обмен платежными инструментами и другой необходимой платежной информацией между финансовым институтом плательщика и получателя, а также вычисление платежных требований, необходимых для проведения расчета.

Шаги обмена инструментами:

- **Сверка операций;**
- **Сортировка операций;**
- **Сбор и проверка данных;**
- **Агрегирование данных;**
- **Отправка информации;**

ПРОЦЕСС РАСЧЕТА

Обеспечивает исполнение финансовыми институтами плательщика платежных требований, вычисленных в результате клирингового процесса.

Шаги расчета:

- **Сбор предназначенных для проведения расчета платежных требований и проверку их подлинности**
- **Проверка достаточности для расчета ДС на расчетных счетах финансовых институтов**
- **Урегулирование требований между финансовыми институтами посредством отражения денежных сумм на расчетных счетах**
- **Регистрацию информации о результатах расчетного процесса и передачу данной информации заинтересованным финансовым институтам**

При этом используются корреспондентские счета, которые финансовые институты ведут друг у друга или в третьем финансовом институте, выступающим в качестве расчетного банка.

SWIFT

- **SWIFT (Society for Worldwide Interbank Financial Telecommunications) - Сообщество всемирных межбанковских финансовых телекоммуникаций.**
- **Создано в 1973 году.**
- **По сути SWIFT – это инфраструктура по передачи финансовых сообщений.**
- **Пользователями системы являются примерно 9000 банков (включая центральные банки) и финансовых организаций (брокеры, биржи, депозитарии), плюс масса корпораций из 209 стран.**
- **SWIFT — кооперативное общество, созданное по бельгийскому законодательству, принадлежащее его пользователям**
- **На базе SWIFT реализованы системы платежей более 50 стран мира. В частности все страны Евросоюза. Из СНГ только Азербайджан.**
- **После длительного использования SWIFT свои системы расчетов создали Босния и Герцеговина, Латвия и Хорватия.**
- **Через SWIFT проводится около 2,5 млрд платежных поручений в год.**
- **ЦБ РФ и Федеральная резервная система США запустили систему расчетов на базе SWIFT параллельно с собственной расчетной системой. Поэтому в США и России банки сами выбирают, каким инструментом пользоваться в системе БЭСП (Банковских электронных срочных платежей).**

SWIFT В РОССИИ

Год	Число пользователей	Год	Число пользователей
1995	229	2003	389
1996	255	2004	413
1997	250	2005	448
1998	247	2006	475
1999	256	2007	496
2000	271	2008	517
2001	293	2009	530
2002	344	2010	541

SWIFT В РОССИИ

Год	Кол-во сообщений	Год	Кол-во сообщений
1995	3 179 346	2003	12 450 561
1996	3 783 823	2004	15 281 128
1997	5 463 857	2005	17 810 861
1998	5 517 072	2006	20 532 533
1999	4 479 650	2007	24 429 961
2000	6 642 263	2008	28 819 790
2001	8 309 709	2009	27 437 545
2002	9 964 562	2010	31 632 539

SWIFT В РОССИИ

Распределение трафика	В мире	В России
Платежи	49,4%	78,3%
Ценные бумаги	43,4%	10,8%
Операции на финансовых рынках	5,8%	8,9%
Финансирование торговли	1,1%	0,4%
Системные сообщение	0,3%	1,6%

РОССВИФТ

- Интересы мирового SWIFT почти 20 лет представляет РОССВИФТ (создана в мае 1994г.);
- Около 600 организаций в РФ являются пользователями SWIFT;
- Участниками могут быть не только банки, но и другие финансовые организации и крупные корпоративные клиенты (н-р, «Лукойл»).

Russia
National Member and User Group
SWIFT
Российская Национальная Ассоциация SWIFT

МЕЖДУНАРОДНЫЕ КАРТОЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

- Рынок платежный карт стал формироваться с 1950г. (компания Diners Club выпустила первую платежную карту)
- Первая карта была из картона и принималась к оплате в нескольких ресторанах
- Схема: Клиент посещал ресторан, его счет оплачивала Diners Club, клиент возмещал ДС Diners Club.
- За первый год число держателей карт составило 42 тыс. человек.
- С 1953 года карты Diners Club начинают принимать в Великобритании, Канаде, Мексике и на Кубе
- В 1967 году принималась к оплате в 130 странах
- В 1969 году стала первой картой принимаемой в СССР!!!
- Со временем компания утратила лидерские позиции пропустив вперед компании Visa и MasterCard
- Другими крупным участниками рынка международных платежных карт сегодня являются: American Express, Discover, Diners Club, JCB (Japan Credit Bureau) и CUP (China Union Pay)

ПРОДУКТЫ МЕЖДУНАРОДНЫХ КАРТОЧНЫХ ПЛАТЕЖНЫХ СИСТЕМ

Инструменты:

- **Традиционные карточные инструменты (кредитные, дебетовые, расчетные, предоплаченные и иные типы карт)**
- **Развивающиеся формы платежей (н-р, платежи и с использованием мобильного телефона)**

Самый распространенный инструмент – карты общего назначения.

КАРТЫ ОБЩЕГО НАЗНАЧЕНИЯ

Свойства карты зависят от типа счета, к которому привязана карта:

- **Кредитные или расчетные карты**
- **Дебетовые карты**

Различают 2 типа транзакций:

1. **Офлайн-транзакции, требующие подпись держ**
2. **Онлайн-транзакции, требующие введения ПИ**

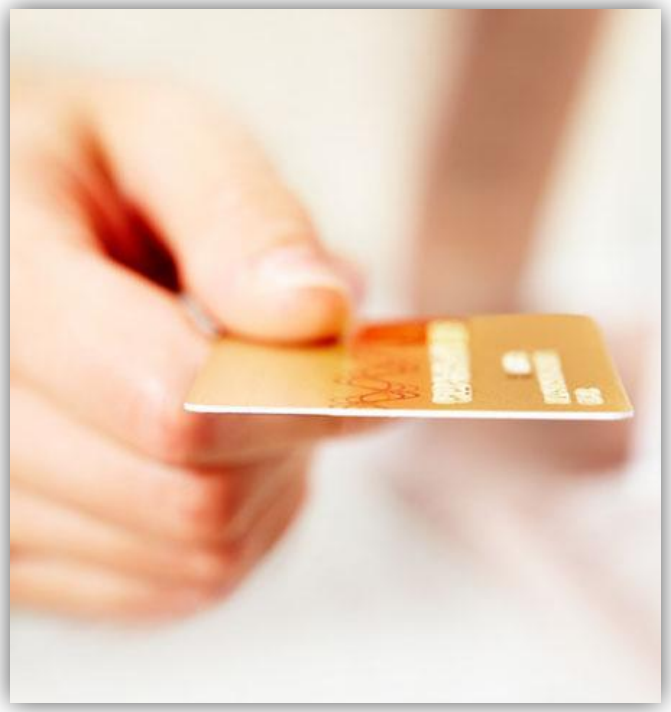
Также используются технологий , н-р RFID (Radio frequency identification), позволяющие совершать бесконтактные платежи, которые не требуют ПИН и подписи. Относятся к офлайн-транзакциям.

УЧАСТНИКИ МЕЖДУНАРОДНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ (МПС)

Международные платежные системы могут быть:

- **Открытые (Visa, MasterCard)**
- **Закрытые (American Express, Diners Club, JBC)**

Закрытые сами являются эквайерами и эмитентами карт. Другими словами, в таких системах владелец структуры также является собственником технологической сети, используемой для клиринга и совершения транзакций.



МЕЖДУНАРОДНЫЕ КАРТОЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

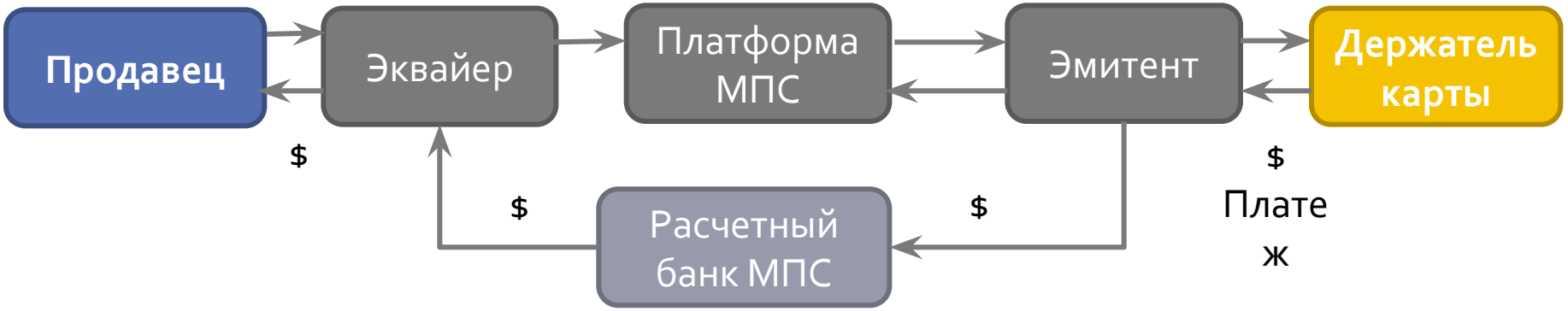
К таковым относятся Visa и MasterCard.

Процесс осуществления транзакции:

- **Держатель передает продавцу карту**
- **Терминал переводит информацию эквайеру**
- **Эквайер формирует авторизационный запрос и отправляет его в МПС**
- **МПС пересылает его эмитенту**
- **Эмитент направляет в МПС ответ разрешая или отклоняя транзакцию**

МЕЖДУНАРОДНЫЕ КАРТОЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

Процесс клиринга и расчетов между эмитентом и эквайером:



Продавец передает информацию о покупках эквайру

Эквайер формирует клиринговое извещение и пересылает его в МПС

МПС переправляет клиринговое извещение эмитенту, а также рассчитывает обязательства эмитента по расчетам и сумму, которая должна быть перечислена эквайеру

Эмитент направляет средства через банк, выбранный МПС

МОДЕЛИ НПС РОССИИ. 2003

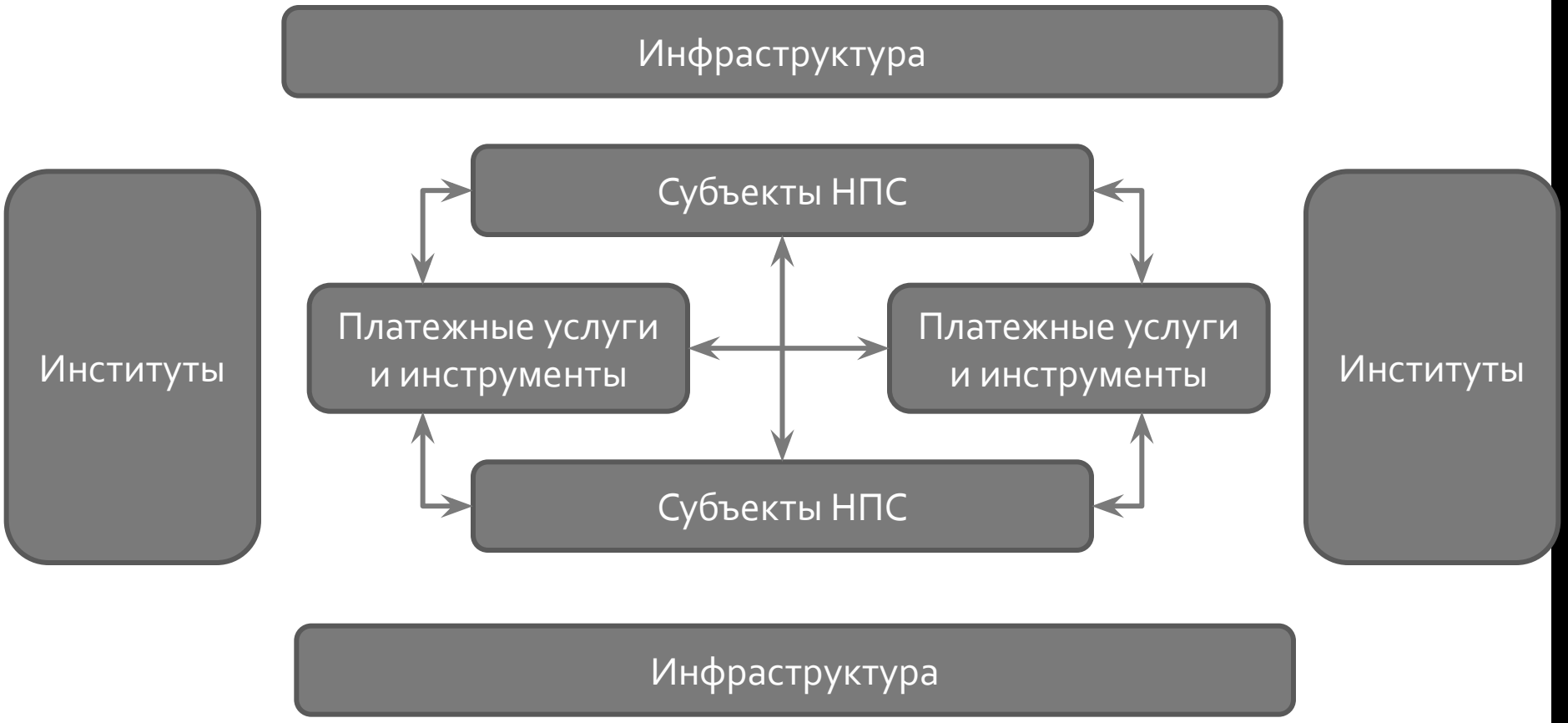
- **Термин НПС появился в документах КПРС в 1980 году, а в документах Банка России только в 2003 году**
- **Справочный материал по ПС России в рамках Red Book (Красная книга) или «Платежные, клиринговые и расчетные системы в отдельных странах»**
- **НПС России состоит и 6 элементов:**
  - Общие правовые аспекты (ГК, ФЗ о Банке России, О банках и банковской деятельности)
  - Институциональные аспекты (БР, Казначейство, Почта России, Биржи и т.д.)
  - Платежные инструменты (наличные и безналичные)
  - Межбанковские ПС (ПС Банка России, ПС кредитных организаций для расчетов по корреспондентским счетам, внутрибанковские ПС)
  - Международные платежи (международные межбанковские платежи, дорожные чеки и платежные карты)
  - Системы расчетов по операциям с ценными бумагами (ММВБ и РТС)

СОВРЕМЕННАЯ МОДЕЛЬ НПС

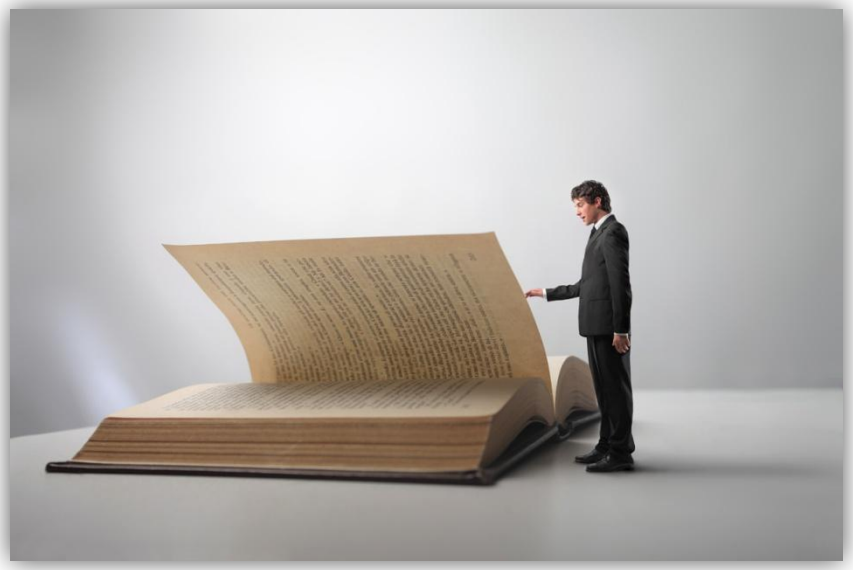
ТРЕХУРОВНЕВАЯ (3L) МОДЕЛЬ НПС РОССИИ

Системный уровень – уровень платежных систем и прочих систем НПС	Третий уровень
Промежуточный компонентный уровень – уровень субъектов и объектов НПС (платежных услуг и платежных инструментов)	Второй уровень
Базовый уровень – уровень институциональных и инфраструктурных механизмов	Первый уровень

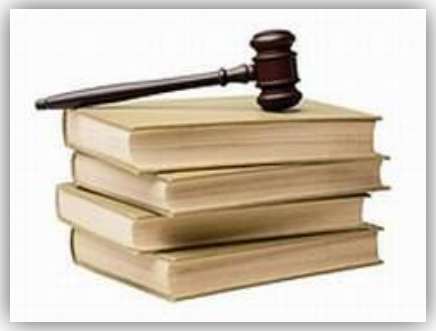
СХЕМА ВЗАИМОДЕЙСТВИЯ В НПС РОССИИ



ПРАВОВОЕ ПОЛЕ НПС

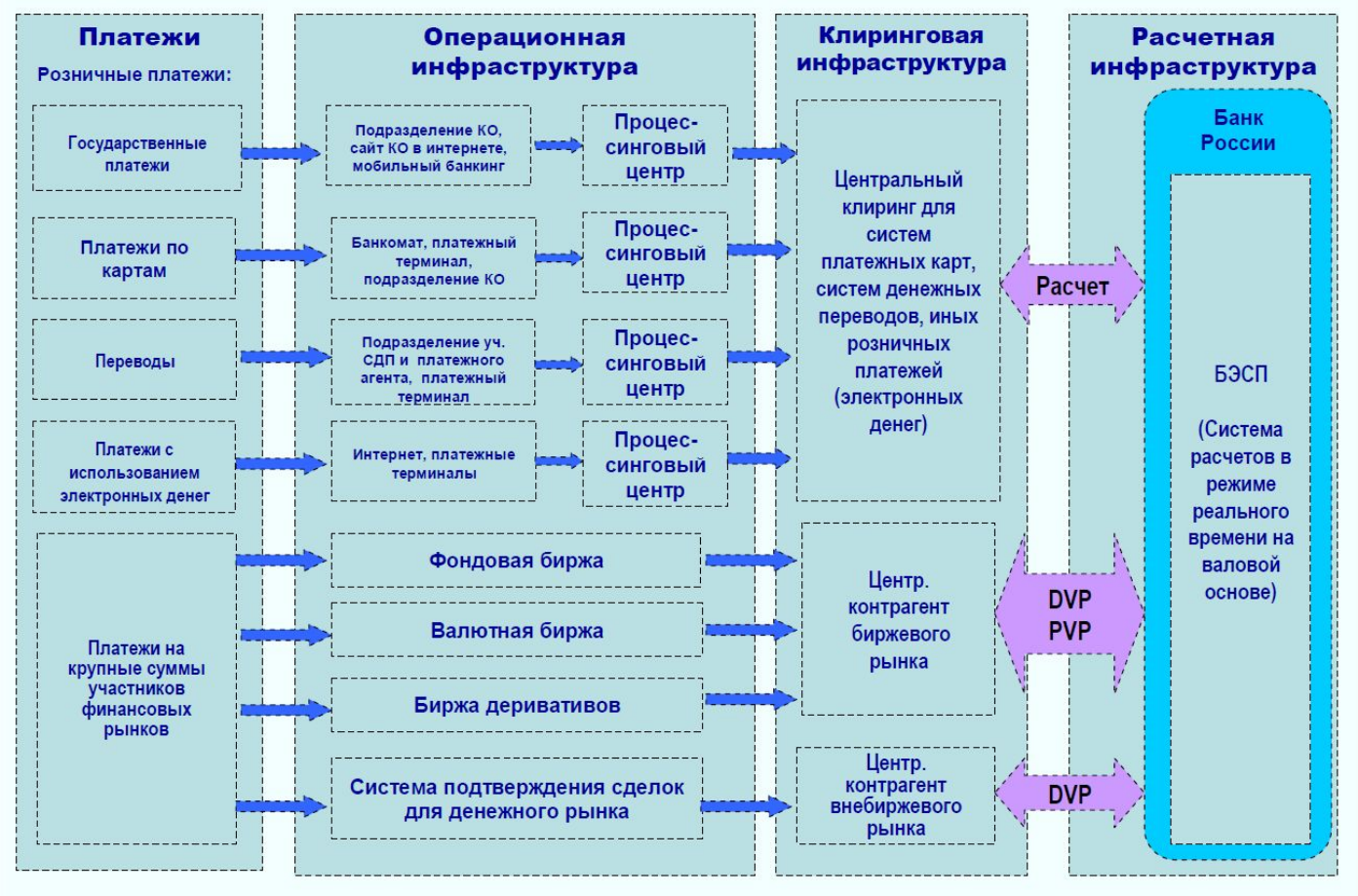


РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА



- О банках и банковской деятельности (№ 395-1 от 02.12.1990)
- Гражданский кодекс Российской Федерации
- Налоговый кодекс Российской Федерации
- Бюджетный кодекс Российской Федерации
- О несостоятельности (банкротстве) кредитных организаций
- О почтовой связи (№176-ФЗ от 17.07.1999)
- О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма
- Кодекс Российской Федерации об административных правонарушениях
- О Центральном банке Российской Федерации (Банке России)
- О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт (№54-ФЗ от 22.05.2003)
- О деятельности по приему платежей физических лиц, осуществляемой платежными агентами (№103-ФЗ от 03.06.2009)
- О национальной платежной системе (№161-ФЗ от 27.06.2011)

СХЕМА ПЕРСПЕКТИВНОЙ НПС



КЛЮЧЕВЫЕ НАЦИОНАЛЬНЫЕ РЕГУЛЯТОРЫ И УЧАСТНИКИ ОТРАСЛИ

БАНК РОССИИ

АССОЦИАЦИЯ РОССИЙСКИХ БАНКОВ
ASSOCIATION OF RUSSIAN BANKS

« РОССИЯ »

НПС
некоммерческое партнерство
национальный платежный совет

АССОЦИАЦИЯ
НАЦИОНАЛЬНЫЙ
ПЛАТЕЖНЫЙ СОВЕТ

ABISS

КЛЮЧЕВЫЕ НАЦИОНАЛЬНЫЕ РЕГУЛЯТОРЫ И УЧАСТНИКИ ОТРАСЛИ

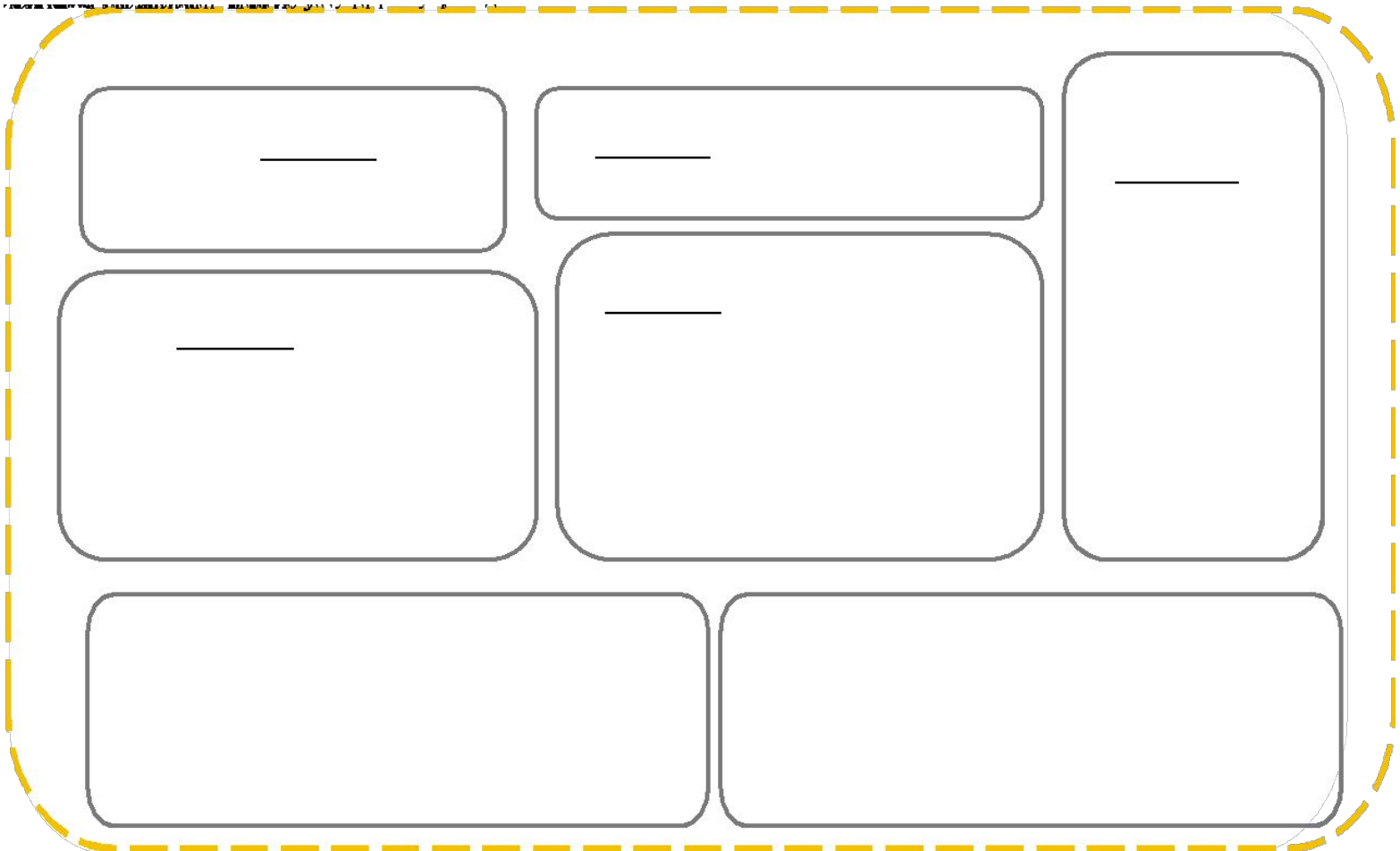
- **Некоммерческое партнерство «Национальной платежных совет» (НПС). НП НПС это универсальная межотраслевая и межассоциативная площадка для обсуждения, согласования подходов и выработки консолидированной позиции различных сегментов Национальной платежной системы. В число учредителей НПС вошли Сбербанк, Банк ВТБ, Альфа-Банк, Дойчебанк, Промсвязьбанк, Вымпелком, ЗАО «Золотая Корона» и банк Юнистрим. Первыми участниками НПС стали РСПП, АРБ, РОССВИФТ, системы денежных переводов «Вестерн Юнион» и ЛИДЕР, ЗАО «КИБЕРПЛАТ», Банк Открытие, Ситибанк и Банк «ХОУМ КРЕДИТ». Соглашения о взаимодействии с НПС уже подписали Ассоциация РАТЭК, НП «Национальное партнерство участников микрофинансового рынка» (НАУМИР), Ассоциация «Электронные деньги».**

- **Ассоциация «Национальный платежный совет». Целью данной ассоциации заявлено содействие планомерному и ускоренному развитию российской индустрии электронных платежей, а также повышение экономической и социальной роли платёжной индустрии в России. Членами ассоциации являются таможенная платежная система «ЗЕЛЕНЫЙ КОРИДОР», система платёжных сервисов для розничного платёжного рынка «Золотая Корона», компания MasterCard и Visa (сообщество операторов платежей по «карточкам»).**

- **Некоммерческое партнерство «Сообщество пользователей стандартов по информационной безопасности АБИСС». «Партнерство» основано на принципах добровольного объединения ее членов – субъектов предпринимательской и профессиональной деятельности, обеспечивающих информационную безопасность в кредитно-финансовых и других организациях – участниках национальной платежной системы Российской Федерации, а также оказывающих услуги в области обеспечения информационной безопасности. Партнерство создано в целях реализации стандартов и правил, направленных на обеспечение информационной безопасности в кредитных и других организациях–участниках национальной платежной системы Российской Федерации.**

Федеральный закон Российской Федерации от 27 июня 2011 г. **№ 161-ФЗ** "О национальной платежной системе"

Постановление Правительства Российской Федерации от 13 июня 2012 г. **№ 584** "Об утверждении Положения о защите информации в платежной системе



ФЕДЕРАЛЬНЫЙ ЗАКОН РФ ОТ 27 ИЮНЯ 2011 Г. N 161-ФЗ "О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ"

№161-ФЗ "О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ"

- **Принят Государственной Думой 14 июня 2011 года**
- **Одобрен Советом Федерации 22 июня 2011 года**
- **Устанавливает правовые и организационные основы национальной платежной системы, регулирует порядок оказания платежных услуг, в том числе осуществления перевода денежных средств, использования электронных средств платежа, деятельность субъектов национальной платежной системы, а также определяет требования к организации и функционированию платежных систем, порядок осуществления надзора и наблюдения в национальной платежной системе**

ЗНАЧИМЫЕ СТАТЬИ №161-ФЗ С ТОЧКИ ЗРЕНИЯ ИБ

Статья 3. **Основные понятия, используемые в настоящем Федеральном законе;**

Статья 20. **Правила платежной системы;**

Статья 26. **Обеспечение банковской тайны в платежной системе;**

Статья 27. **Обеспечение защиты информации в платежной системе;**

Статья 28. **Система управления рисками в платежной системе.**

ЧТО ТАКОЕ НПС?

национальная платежная система *- совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры (субъекты национальной платежной системы)*

ОПРЕДЕЛЕНИЯ

- ***оператор по переводу денежных средств*** *- организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств;*

- ***оператор электронных денежных средств*** *- оператор по переводу денежных средств, осуществляющий перевод электронных денежных средств без открытия банковского счета (перевод электронных денежных средств);*

ОПРЕДЕЛЕНИЯ

- ***банковский платежный агент/субагент*** *- юридическое лицо, за исключением кредитной организации, или индивидуальный предприниматель, которые привлекаются кредитной организацией/банковским платежным агентом в целях осуществления деятельности, предусмотренной настоящим Федеральным законом;*

- ***оператор платежной системы*** *- организация, определяющая правила платежной системы, а также выполняющая иные обязанности, предусмотренные настоящим Федеральным законом;*

ОПРЕДЕЛЕНИЯ

- ***оператор услуг платежной инфраструктуры*** *- операционный центр, платежный клиринговый центр и расчетный центр;*

- ***операционный центр*** *- организация, обеспечивающая в рамках платежной системы для участников платежной системы и их клиентов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями (далее - операционные услуги);*

- ***платежный клиринговый центр*** *- организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках платежной системы прием к исполнению распоряжений участников платежной системы об осуществлении перевода денежных средств и выполнение иных действий, предусмотренных настоящим Федеральным законом (далее - услуги платежного клиринга);*

- ***расчетный центр*** *- организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках платежной системы исполнение распоряжений участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы, а также направление подтверждений, касающихся исполнения распоряжений участников платежной системы (далее - расчетные услуги);*

ОПРЕДЕЛЕНИЯ

- **электронные денежные средства - денежные средства!!!, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций;**

- **электронное средство платежа - средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств;**

ОПРЕДЕЛЕНИЯ

- **платежная система - совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, включающая оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств;**

Например:

- PayPal
- Webmoney
- Яндекс.Деньги
- ОСМП (Qiwi)
- MasterCard
- VISA

- **участники платежной системы - организации, присоединившиеся к правилам платежной системы в целях оказания услуг по переводу денежных средств;**

- **значимая платежная система (N 2836-У) - платежная система, отвечающая критериям, установленным настоящим Федеральным законом (системно значимая платежная система или социально значимая платежная система);**

СУБЪЕКТЫ НПС И УЧАСТНИКИ ПС

- ***<u>участники платежной системы</u> - организации, присоединившиеся к правилам платежной системы в целях оказания услуг по переводу денежных средств***
- ***<u>субъекты национальной платежной системы</u>:***
  - *операторы по переводу денежных средств (включая операторов электронных денежных средств),*
  - *банковские платежные агенты (субагенты),*
  - *платежные агенты,*
  - *организации федеральной почтовой связи,*
  - *операторы платежных систем,*
  - *операторов услуг платежной инфраструктуры;*


Платежная система
Оператор платежной системы
Центральный платежный клиринговый контрагент
Платежный клиринговый центр
Операционный центр
Расчетный центр
Оператор услуг платежной инфраструктуры……
Оператор по переводу денежных средств
Оператор электронных денежных средств
Банковский платежный агент
Банковский платежный субагент

Платежная система

Определяет правила платежной системы

Оператор платежной системы

Платежный клиринговый центр + выступает плательщиком и получателем денежных средств участников платежной системы

Центральный платежный клиринговый контрагент

Оказывает операционные услуги: перевод денежных средств, в т.ч. с использованием электронных средств платежа, а также обмен электронными сообщениями

Операционный центр

Платежный клиринговый центр

Расчетный центр

Оператор услуг платежной инфраструктуры……

Обеспечивает прием к исполнению распоряжений участников платежной системы об осуществлении перевода денежных средств и выполнение иных действий

Обеспечивает исполнение распоряжений участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы

Определяет перевод денежных средств между участниками платежной системы

Оператор по переводу денежных средств

Оператор электронных денежных средств

По договору с оператором осуществляет прием-выдачу наличных денежных средств и(или) распоряжений на осуществление переводов + иную деятельность по 161-ФЗ

Банковский платежный агент

Банковский платежный субагент

Определяет перевод **электронных** денежных средств без открытия банковского счета

По договору с банковским платежным агентом выполняет те же функции, но с рядом ограничений

История
Правовой статус и функции Банка России
Совет директоров
Организационная структура
Национальный банковский совет
Платежная система Российской Федерации
- Общая информация
- Стандарты и технологии
- Платежная система Банка России
- Регулирование в платежной системе Российской Федерации
- Наблюдение в платежной системе Российской Федерации
- Аналитические материалы, публикации, доклады
- Статистика платежной системы Российской Федерации
- Международная статистика
- **Реестр операторов платежных систем**
- Перечень операторов электронных денежных средств

Публикации и доклады
Международное сотрудничество
Карьера в Банке России
Образовательные учреждения и учебно-

Реестр операторов платежных систем

Публикуется в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ "О национальной платежной системе" (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) и Положением Банка России от 2 мая 2012 года № 378-П "О порядке направления в Банк России заявления о регистрации оператора платежной системы", зарегистрированного Министерством юстиции Российской Федерации 5 июня 2012 года № 24463 ("Вестник Банка России" от 15 июня 2012 года № 30 (1348)).

- Реестр операторов платежных систем (22.01.2013 14:52 / 13 Кб)
- Рекомендации по оформлению документов, направляемых в Банк России в целях регистрации операторов платежных истем
- Таблица для проведения заявителем проверки правил платежной системы на соответствие требованиям Федерального закона от 27.06.2011 № 161 – ФЗ "О национальной платежной системе" и принятыми в соответствии с ним нормативными актами Банка России

Контактный телефон: 8 (495) 771-91-80.

Реестр операторов ПС

№ п/п	Оператор платежной системы							Наименование платежной системы	Расчетный центр			
	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		Наименование	Место нахождения	ОГРН	Рег. номер соответствии Книго государств регистр кредит организ
			ОГРН	ОГРН	Рег. номер в соответствии с Книгой государственной регистрации кредитных организаций							
1	2	3	4	5	6	7	8	9	10	11	12	13
17	0017	27.12.2012		1027739445337	3304-К	Небанковская кредитная организация закрытое акционерное общество "ЛИДЕР", НКО ЗАО "ЛИДЕР"	127015, г. Москва, ул. Бутырская, д.77	Платежная система "Международные Денежные Переводы ЛИДЕР"	Небанковская кредитная организация закрытое акционерное общество "ЛИДЕР", НКО ЗАО "ЛИДЕР"	127015, г. Москва, ул. Бутырская, д.77	1027739445337	3304-
18	0018	29.12.2012	1107746323926			Общество с ограниченной ответственностью "МастерКард", "МастерКард" ООО	107031, г. Москва, ул. Большая Дмитровка, дом 10, строение 4	Платежная система "МастерКард"	Открытое акционерное общество "Сбербанк России", ОАО "Сбербанк России"	117997, г. Москва, ул. Вавилова, д.19	1027700132195	1481
19	0019	29.12.2012	1107746390949			Открытое акционерное общество "Универсальная электронная карта", ОАО "УЭК"	119021, г. Москва, улица Тимура Фрунзе, дом 11, стр. 15	Платежная система "Универсальная электронная карта" (ПС "УЭК")	Открытое акционерное общество "Сбербанк России", ОАО "Сбербанк России"	117997, г. Москва, ул. Вавилова, д.19	1027700132195	1481
20	0020	22.01.2013	1087746840422			Общество с ограниченной ответственностью "РСА-Клиринг", ООО "РСА-Клиринг"	115093, г. Москва, ул. Люсиновская, д.27, стр.3	Платежная система "Страховая платежная система"	Открытое акционерное общество "Альфа-Банк", ОАО "Альфа-Банк"	107078, г. Москва, ул. Каланчевская, д.27	1027700067328	1326

ПРАВИЛА ПЛАТЕЖНОЙ СИСТЕМЫ (СТ.20)

Правилами ПС определяется:

1) порядок взаимодействия между оператором платежной системы, участниками платежной системы и операторами услуг платежной инфраструктуры;

2) порядок осуществления контроля за соблюдением правил платежной системы;

…

13) система управления рисками в платежной системе, включая используемую модель управления рисками, перечень мероприятий и способов управления рисками;

14) порядок обеспечения бесперебойности функционирования платежной системы;

…

18) порядок взаимодействия в рамках платежной системы в спорных и чрезвычайных ситуациях, включая информирование операторами услуг платежной инфраструктуры, участниками значимой платежной системы оператора значимой платежной системы о событиях, вызвавших операционные сбои, об их причинах и последствиях;

19) требования к защите информации;

…

22) порядок досудебного разрешения споров с участниками платежной системы и операторами услуг платежной инфраструктуры.

ПРАВИЛА ПЛАТЕЖНОЙ СИСТЕМЫ (СТ.20)

- **Оператор платежной системы обязан предоставлять организациям, намеревающимся участвовать в платежной системе, правила платежной системы для предварительного ознакомления без взимания платы, за исключением расходов на изготовление копий правил платежной системы.**
- **Правила платежной системы, включая тарифы, являются публично доступными. Оператор платежной системы вправе не раскрывать информацию о требованиях к защите информации и информацию, доступ к которой ограничен в соответствии с федеральным законом.**

ОБЕСПЕЧЕНИЕ БАНКОВСКОЙ ТАЙНЫ В ПЛАТЕЖНОЙ СИСТЕМЕ (СТ.26)

- **Операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры и банковские платежные агенты (субагенты) обязаны гарантировать банковскую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности.**

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНОЙ СИСТЕМЕ (СТ.27)

1. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации. Правительство Российской Федерации устанавливает требования к защите указанной информации.

2. Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с защищаемой информацией.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНОЙ СИСТЕМЕ (СТ.27)

3. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России, согласованными с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи. Контроль за соблюдением установленных требований осуществляется Банком России в рамках надзора в национальной платежной системе в установленном им порядке, согласованном с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи.

ОПЕРАТОР ПО ПЕРЕВОДУ ДС И ОПЕРАТОР ЭЛЕКТРОННЫХ ДС

Условие	Операторов по переводу денежных средств	Операторов электронных денежных средств
Может предоставлять средства клиенту (например, кредит)	Да	Нет
Может начислять проценты на остаток	Да	Нет
Юридические лица обязаны открывать банковский счет	Нет	Да
Обязан получать лицензию ЦБ	Да	Да ("упрощенную")
Может не осуществлять перевод средств (не заключать договор)	Нет	Да
Лимит по обороту и максимальному остатку на счете клиента	Нет	Да
Скорость осуществения перевода	До 3 дней	Сразу

ЭЛЕКТРОННЫЕ СРЕДСТВА ПЛАТЕЖА

161-ФЗ формулирует 3 вида Электронных средств платежа (ЭСП):

- Неперсонифицированное ЭСП (максимальный остаток на счете 15 тыс. руб., максимальный оборот 40тыс. руб./мес.)
- Персонифицированное ЭСП (максимальный остаток 100 тыс. руб.)
- Корпоративное ЭСП (для юр.лиц, максимальный остаток на конец дня 100 тыс. руб.)

РЕГУЛИРОВАНИЕ В НПС

Документы	Контроль и надзор
№584-ПП	ФСТЭК России, ФСБ России
№ 379-П, № 380-П, № 381-П, № 382-П	Банк России (по согласованию с ФСТЭК России и ФСБ России)
№2831-У	Банк России (по согласованию с ФСТЭК России и ФСБ России)
Правила ПС	Оператор ПС

ВЕХИ ПО БЕЗОПАСНОСТИ

- ✔ **«Участники НПС» обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.**
- ✔ **Правительство Российской Федерации устанавливает требования к защите информации.**
- ✔ **Контроль и надзор за выполнением требований Правительства РФ осуществляются ФСБ и ФСТЭК, в пределах их полномочий и без права ознакомления с защищаемой информацией.**
- ✔ **Требования по ИБ устанавливает Банк России и согласует с ФСТЭК и ФСБ.**
- ✔ **Контроль осуществляется Банком России в порядке, согласованном с федеральными органами исполнительной власти.**
- ✔ **Ключевая цель защиты информации – обеспечение бесперебойности функционирования платежной системы**

ВЕХИ ПО БЕЗОПАСНОСТИ

- **Вводится понятие системы управления рисками, под ней понимается комплекс мероприятий и способов снижения вероятности!!! возникновения неблагоприятных последствий для бесперебойности функционирования платежной системы с учетом размера причиняемого ущерба.**
- **Оператор обязан определить одну из моделей управления рисками в платежной системе:**
  - 1) самостоятельное управление рисками в платежной системе оператором платежной системы;
  - 2) распределение функций по оценке и управлению рисками между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы;
  - 3) передача функций по оценке и управлению рисками оператором платежной системы, не являющимся кредитной организацией, расчетному центру.
- **Система управления рисками должна предусматривать определение порядка обеспечения защиты информации в платежной системе.**

ВЕХИ ПО БЕЗОПАСНОСТИ

- ***В случае хищения денежных средств со счета клиента банк обязан возместить полную сумму похищенных средств*** **(Закон о национальной платежной системе, статья 9 пп. 11-16, вступил в силу с 1 января 2014 года)**

ГК РФ

"Статья 856.1. Риск убытков банка и клиента-гражданина при использовании электронного средства платежа

…

4. В случае, если банк исполнил обязанность по информированию клиента о совершении операции с использованием электронного средства платежа, а клиент уведомил банк по правилам пункта 7 статьи 847 настоящего Кодекса, клиент несет риск убытков от совершения такой операции до момента направления банку уведомления, предусмотренного пунктом 7 статьи 847 настоящего Кодекса, в размере не более десяти процентов от суммы денежных средств, списанных при совершении операции с использованием электронного средства платежа, если докажет одно из следующих обстоятельств:

1. клиент лишился электронного средства платежа не по своей воле;
2. направление уведомления клиентом в срок, указанный в пункте 7 статьи 847 настоящего Кодекса, было невозможно по причинам, не зависящим от клиента;
3. в момент совершения операции с использованием электронного средства платежа клиент не находился и не мог находиться в месте совершения операции или не утратил владения электронным средством платежа.

5. Банк обязан по требованию клиента предоставить клиенту все имеющиеся у банка доказательства, подтверждающие наличие обстоятельств, указанных в пункте 4 настоящей статьи, а также запросить такие доказательства у третьих лиц.

МОСКОВСКИЙ ГОРОДСКОЙ СУД

ОПРЕДЕЛЕНИЕ
от 2 февраля 2012 г. по делу N 33-3013

Судья Колмыкова И.Б.

Судебная коллегия по гражданским делам Московского городского суда в составе председательствующего Строгонова М.В., судей Шубиной И.И. и Мухортых Е.Н.,
при секретаре П.,
заслушав в открытом судебном заседании по докладу судьи Мухортых Е.Н. дело по кассационной жалобе М. на решение Тушинского районного суда г. Москвы от *** года, которым постановлено:
В удовлетворении исковых требований *** к ОАО "***" о взыскании денежных средств, компенсации морального вреда, взыскании судебных расходов отказать,

установила:

М. обратилась в суд с иском к ОАО "***", просила взыскать с ответчика в свою пользу денежные средства в размере *** руб., компенсацию морального вреда в размере ***руб., расходы на оплату услуг представителя в размере *** руб. В обоснование заявленных требований М. указала о том, что она является владельцем карты *** Master Card ***, выданной подразделением *** на основании договора N *** от *** г. С указанной карты *** г. без ведома истца были списаны тремя переводами на неизвестные ей счета денежные средства на общую сумму *** руб. При этом сама карта находилась у истца. В службе технической поддержки банка карту заблокировали. *** г. истец обратилась в отделение *** с заявлением о несанкционированном списании денежных средств. В отделении банка истца уверили в том, что списание денежных средств произошло вследствие технической неисправности и они будут ей возвращены. Однако до настоящего времени деньги истцу не возвращены. *** г. истец направил в адрес ответчика претензию с требованием возврата денежных средств. На данную претензию ответ получен не был. *** г. при получении выписки из лицевого счета по вкладу истец узнал, что денежные средства, с учетом комиссии, были фактически списаны с лицевого счета истца *** г., т.е. через 3 дня после получения банком сообщения о несанкционированных операциях и через 2 дня после обращения в отделение банка с заявлением о незаконных операциях по банковскому счету и блокировки карты.

*** г. М. обратилась в ОВД по району *** г. Москвы с заявлением по факту снятия денежных средств с банковской карты ОАО "***". В ходе проверки по данному заявлению ОВД установил, что ***г. М., находясь по месту жительства, пользовалась услугами интернета на сайте "***", производила операции по оплате коммунальных услуг. В это время на ее мобильный телефон поступило смс-сообщение о том, что с ее карты сняты денежные средства в сумме *** руб. Ответ на запрос из службы безопасности до окончания срока проверки о том, где были обналичены денежные средства, получен не был. Документальных подтверждений о том, что данная сумма денег была снята со счета М., также не имеется. Постановлением УУМ ОВД по району *** г. Москвы от *** г. в возбуждении уголовного дела отказано за отсутствием события преступления.

В судебном заседании специалист *** пояснила, что идентификатор и постоянный пароль для входа в систему "***" был получен М. самостоятельно с введением ПИН-кода через банкомат. *** г. М. вошла в систему, вход был подтвержден паролем и идентификатором, и провела три операции по переводу денежных средств. Данные операции были подтверждены одноразовыми паролями, переданными банком М. на ее личный мобильный телефон. Все финансовые операции подтверждаются паролями, без которых денежные средства с карты не могут быть списаны. В смс-сообщении банка указывается и текст операции, т.е. к какой операции предоставлен данный пароль. По результатам проведенного службой безопасности банка расследования выяснилось, что персональный компьютер М. был заражен вирусом, действие которого проявляется в том, что при входе на сайт ОАО "***" вирус перенаправлял клиента на сайт, имитирующий сайт ОАО "***". Одновременно мошенники, которые заразили персональный компьютер, входили на оригинальный сайт ОАО "***". При проведении операций мошенники направили запрос в банк на получение паролей, в ответ на который ОАО "***" направил ответ на мобильный телефон клиента. А клиент, не сравнив информацию о параметрах операции, в своем персональном компьютере ввел данный пароль на сайте, имитирующем сайт ОАО "***", в связи с чем он стал доступен мошенникам. Они его подтвердили и деньги были списаны с карты истца.

Выводы и решение суда

Подписав заявление на получение международной дебетовой карты Master Card Standart, М. согласилась с "Условиями использования международных карт России ОАО", а именно: не сообщать ПИН-код и не передавать карту (ее реквизиты) для совершения операций другими лицами, предпринимать необходимые меры для предотвращения утраты, повреждения, хищения карты, нести ответственность по операциям, совершенным с использованием ПИН-кода.
Действия истца М. по использованию банковской карты ОАО "*" нельзя признать добросовестными, поскольку она надлежащим образом принятые на себя обязательства по договору не исполнила. Истец М. как клиент ОАО "***" должна была осознавать возможность наступления рисков, связанных с операциями, проводимыми через систему "***", "Мобильный банк". В связи с этим суд первой инстанции посчитал, что в данном случае ответственность за причиненный истцу ущерб, возникший вследствие несанкционированного использования третьими лицами средств подтверждения клиента, если такое использование стало возможно не по вине банка, не может быть возложена на ответчика.**
С утверждениями истца в кассационной жалобе о том, что доводы специалиста * о том, что компьютер истца был заражен вирусом, являются недостоверными, т.к. осмотр компьютера не производился, судебная коллегия согласиться не может. То обстоятельство, что компьютер истца не был обследован специалистами, с учетом имеющихся в банке технических средств и информационных ресурсов, консультацию специалиста не опровергает.**
Доводы кассационной жалобы о том, что в * г. при входе в систему "***" истец подтверждения об этом от банка не получил, являются голословными и ничем не подтверждены. Судом установлено, что истцу оказывается услуга смс-оповещение, которая предусматривает предоставление клиенту информации обо всех совершаемых по счетам карт операциях путем немедленной передачи сообщения на мобильный телефон, указанный клиентом. Претензий к качеству указанной услуги от М. не поступало.**

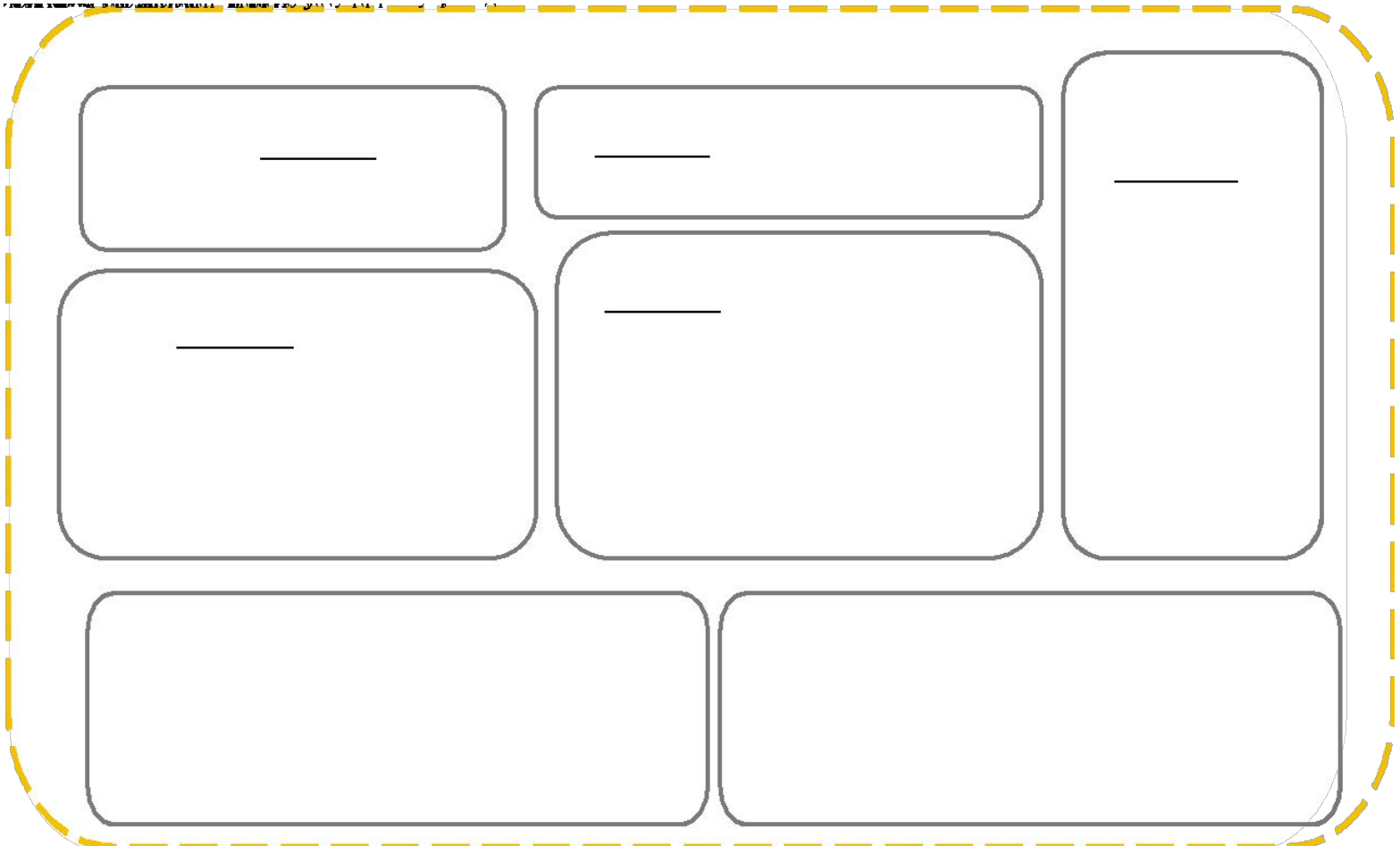
КОНТРОЛЬ БАНКА РОССИИ

- **Если нарушения влияют на бесперебойность функционирования платежной системы либо на услуги, оказываемые участникам платежной системы и их клиентам, Банк России :**
  - направляет предписание об устранении нарушения с указанием срока для его устранения;
  - ограничивает (приостанавливает) оказание операционных услуг
  - исключает оператора платежной системы из реестра операторов платежных систем
  - привлекает поднадзорную организацию и ее должностных лиц к административной ответственности

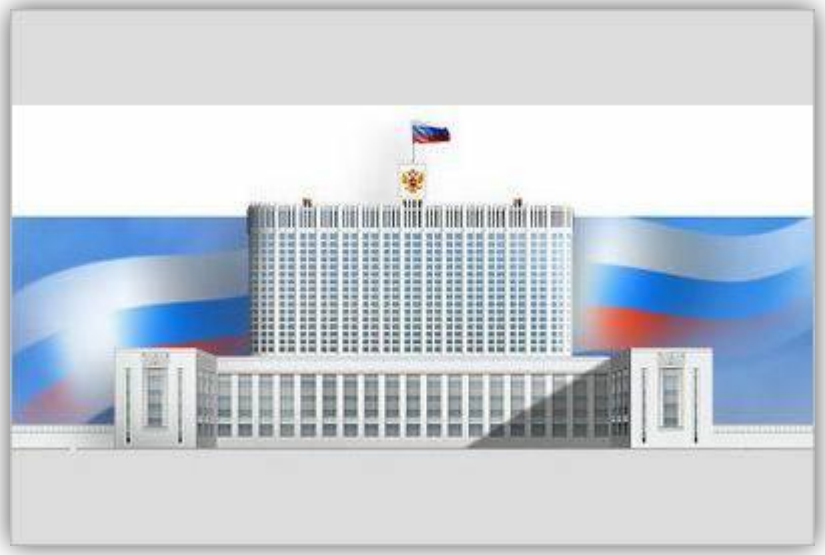
Описание	Дата
Начало регистрации операторов платежных систем	1 июля 2012 года
Вступление в силу статьи 27 Закона об НПС «Обеспечение защиты информации в платежной системе»	1 июля 2012 года
Вступление в силу Постановления Правительства РФ от 13.06.2012 № 584	1 июля 2012 года
Вступление в силу требований Банка России по обеспечению защиты информации при осуществлении переводов денежных средств	1 июля 2012 года
Вступление в силу требований Банка России к обеспечению БФПС	1 июля 2012 года
Крайний срок предоставления в Банк России первого отчета о выявленных инцидентах безопасности в платежной системе	14 августа 2012 года
Крайний срок подачи заявления о регистрации в качестве оператора платежной системы (для банков, соответствующих критериям Указания Банка России № 2814-У)	30 октября 2012 года
Крайний срок определения порядка обеспечения БФПС и организации деятельности по его исполнению	1 января 2013 года
Крайний срок завершения первой оценки соответствия требованиям Положения Банка России № 382-П	1 июля 2014 года
Крайний срок предоставления Банк России отчета об обеспечении защиты информации при осуществлении переводов денежных средств	11 августа 2014 года

Федеральный закон Российской Федерации от 27 июня 2011 г. **№ 161-ФЗ** "О национальной платежной системе"

Постановление Правительства Российской Федерации от 13 июня 2012 г. **№ 584** "Об утверждении Положения о защите информации в платежной системе



ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 13 ИЮНЯ 2012 Г. N 584 "ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ В ПЛАТЕЖНОЙ СИСТЕМЕ"



ИНФОРМАЦИИ ПРЕДЪЯВЛЕНЫ НЕ ДЛЯ ВСЕХ

- **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).**

10 ТРЕБОВАНИЙ 584-ПП

1. **Создание службы информационной безопасности или назначение должностного лица, ответственного за организацию защиты информации**
2. **Включение в должностные обязанности работников, участвующих в обработке информации, обязанности по выполнению требований к защите информации**
3. **Осуществление мероприятий, имеющих целью определение угроз безопасности информации и анализ уязвимости информационных систем**
4. **Проведение анализа рисков нарушения требований к защите информации и управление такими рисками**
5. **Разработка и реализация систем защиты информации в информационных системах**

10 ТРЕБОВАНИЙ 584-ПП

6. **Применение средств защиты информации (шифровальные (криптографические) средства, средства защиты информации от несанкционированного доступа, средства антивирусной защиты, средства межсетевого экранирования, системы обнаружения вторжений, средства контроля (анализа) защищенности)**
7. **Выявление инцидентов, связанных с нарушением требований к защите информации, реагирование на них**
8. **Обеспечение защиты информации при использовании информационно-телекоммуникационных сетей общего пользования**
9. **Определение порядка доступа к объектам инфраструктуры платежной системы, обрабатывающим информацию**
10. **Организация и проведение контроля и оценки выполнения требований к защите информации на собственных объектах инфраструктуры не реже 1 раза в 2 года**

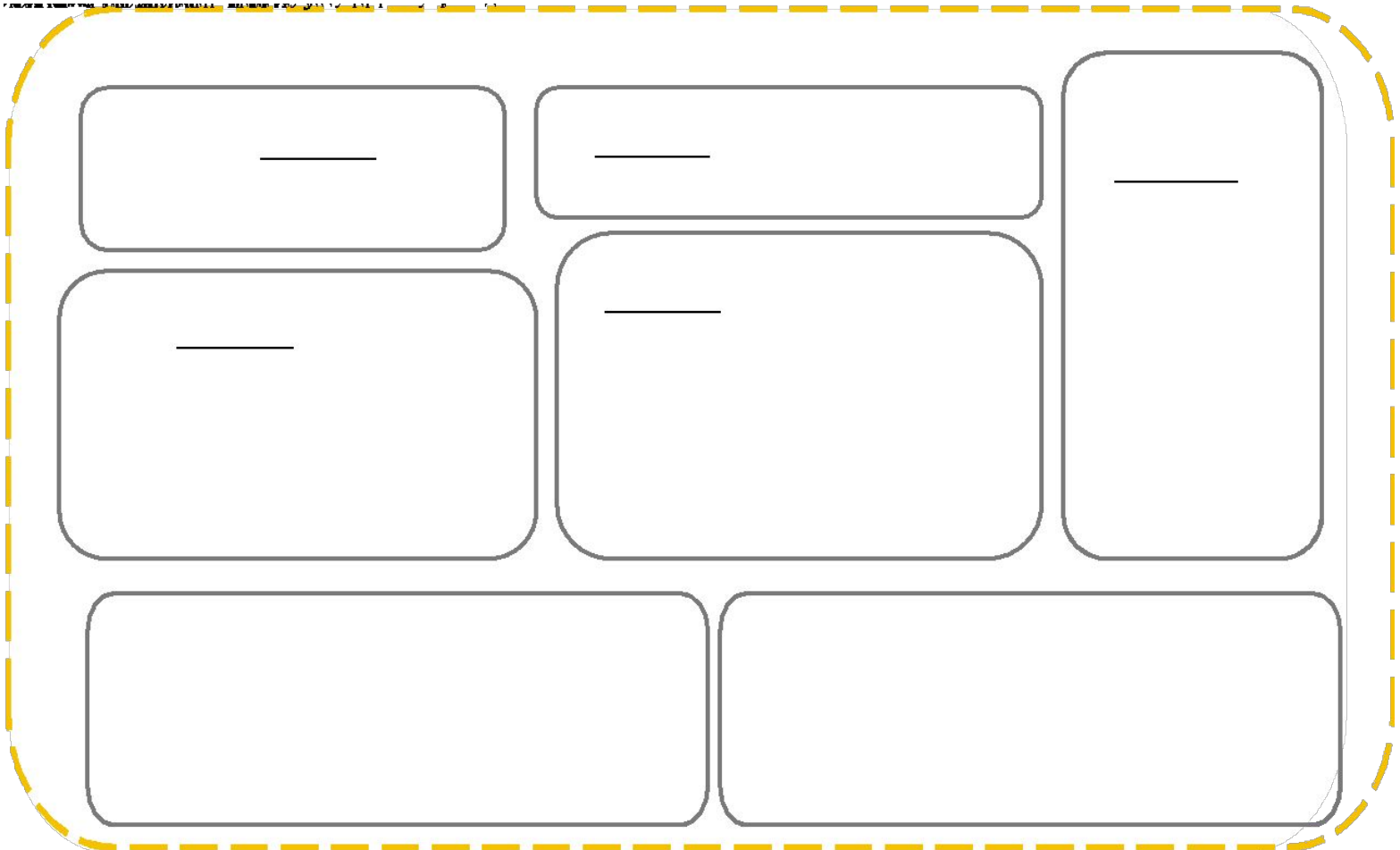
ДЛЯ РАБОТ ПРИВЛЕКАЮТ ЛИЦЕНЗИАТОВ

- ✔ **Для проведения работ по защите информации операторами и агентами могут привлекаться организации, имеющие лицензии на ТЗКИ и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.**

- ✔ **Контроль (оценка) соблюдения требований к защите информации осуществляется операторами и агентами самостоятельно или с привлечением организации, имеющей лицензию на ТЗКИ.**

Федеральный закон Российской Федерации от 27 июня 2011 г. **№ 161-ФЗ** "О национальной платежной системе"

Постановление Правительства Российской Федерации от 13 июня 2012 г. **№ 584** "Об утверждении Положения о защите информации в платежной системе



ПОЛОЖЕНИЕ БАНКА РОССИИ ОТ 31 МАЯ 2012 Г. № 379-П “О БЕСПЕРЕБОЙНОСТИ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНЫХ СИСТЕМ И АНАЛИЗЕ РИСКОВ В ПЛАТЕЖНЫХ СИСТЕМАХ”

ПРЕДМЕТ ДОКУМЕНТА

- ✔ **В Законе о национальной платежной системе перечислены мероприятия, которые должна предусматривать система управления рисками. К таковым, в частности, относится определение показателей и порядка обеспечения бесперебойности функционирования платежной системы (далее - БФПС), а также методик анализа рисков в таковой согласно нормативным актам ЦБР.**

- ✔ **Установлены требования к порядку обеспечения и показателям БФПС и методикам анализа рисков в платежных системах.**

- ✔ **Так, БФПС подразумевает способность предупреждать нарушения законодательства, правил платежной системы, заключенных договоров при взаимодействии субъектов платежной системы, а также восстанавливать надлежащее функционирование системы при его нарушении.**

ПРЕДМЕТ ДОКУМЕНТА

- ✔ **Оператор платежной системы контролирует деятельность по обеспечению БФПС. Субъекты платежной системы организуют реализацию порядка обеспечения БФПС в рамках внутренних систем управления рисками своей деятельности.**

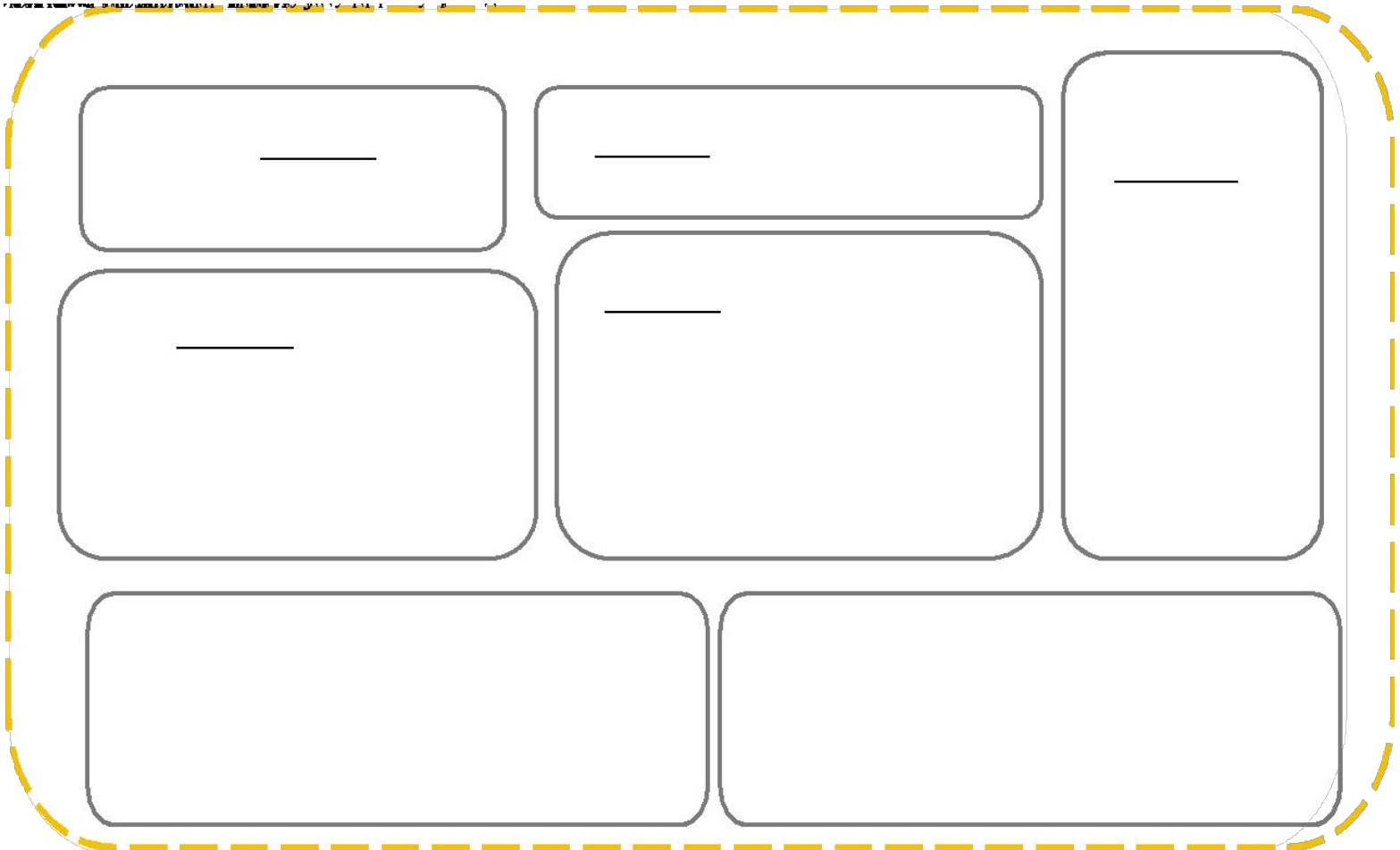
- ✔ **Для каждого устанавливаемого показателя БФПС определяются процедура и методика его формирования на основе первичной информации о функционировании платежной системы и сведений о факторах риска нарушения БФПС.**

- ✔ **Указано, что должны обеспечивать методики анализа рисков в платежной системе.**

- ✔ **Операторы платежных систем должны регламентировать порядок обеспечения БФПС, организовать его реализацию, определить показатели БФПС, методики анализа рисков в платежной системе до 1 января 2013 г.**

Федеральный закон Российской Федерации от 27 июня 2011 г. **№ 161-ФЗ** "О национальной платежной системе"

Постановление Правительства Российской Федерации от 13 июня 2012 г. **№ 584** "Об утверждении Положения о защите информации в платежной системе



ПОЛОЖЕНИЕ БАНКА РОССИИ ОТ 31 МАЯ 2012 ГОДА № 380-П "О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ НАБЛЮДЕНИЯ В НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ"

ПРЕДМЕТ ДОКУМЕНТА

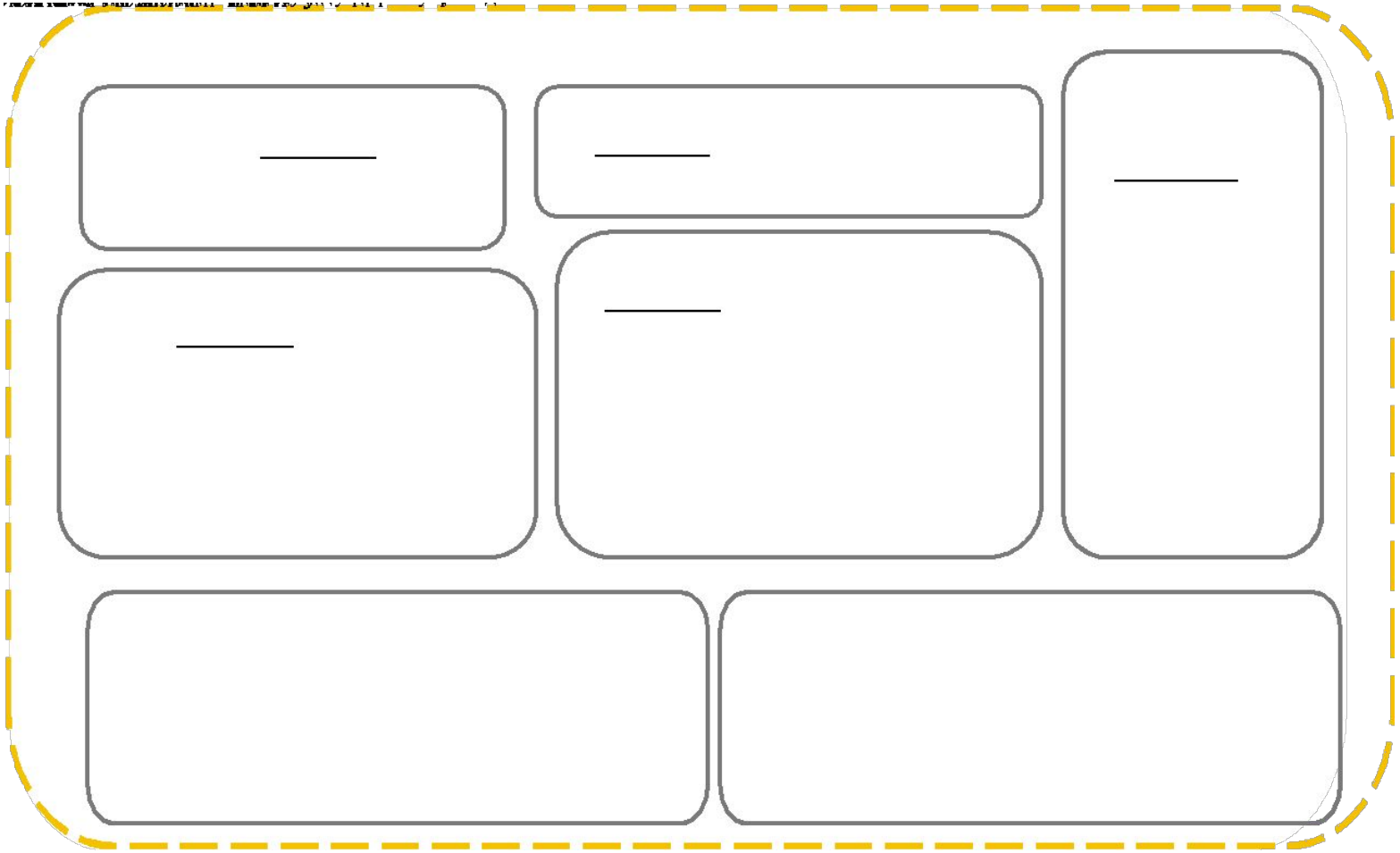
- **Банк России осуществляет наблюдение за деятельностью операторов по переводу денежных средств, операторов платежных систем, операторов услуг платежной инфраструктуры (наблюдаемых организаций), других субъектов национальной платежной системы (далее - НПС), за оказываемыми ими услугами, а также за развитием платежных систем, платежной инфраструктуры.**

ЧТО ЗАПРАШИВАЕТ ЦБ?

- ✔ **Банк России наблюдает за деятельностью операторов и других субъектов национальной платежной системы (НПС), а также за развитием платежных систем и инфраструктуры.**
- ✔ **Банк России вправе запрашивать необходимую информацию у субъектов НПС, в т.ч. по защите информации, которые обязаны ее предоставить в установленные сроки. Также с их уполномоченными представителями могут проводиться рабочие встречи. Допускаются иные формы взаимодействия.**
- ✔ **ЦБР оценивает значимую платежную систему (ЗПС) , в т.ч. по защите информации, не реже 1 раза в 2 года. Эта процедура длится не более 3 месяцев. В ходе нее определяется, насколько наблюдаемые организации и связанных с ними ЗПС соответствуют рекомендациям Банка России.**
- ✔ **Обобщенные результаты оценки ЗПС, в т.ч. по защите информации, публикуются в изданиях Банка России и размещаются на его официальном сайте.**
- ✔ **Не реже 1 раза в 2 года Банком России готовится обзор результатов всего наблюдения. В нем, в частности, отражаются состояние рынков платежных услуг, динамика их развития, положительные и отрицательные факторы, информация об инновациях в области переводов денежных средств, клиринга и операционных услуг.**

Федеральный закон Российской Федерации от 27 июня 2011 г. **№ 161-ФЗ** "О национальной платежной системе"

Постановление Правительства Российской Федерации от 13 июня 2012 г. **№ 584** "Об утверждении Положения о защите информации в платежной системе



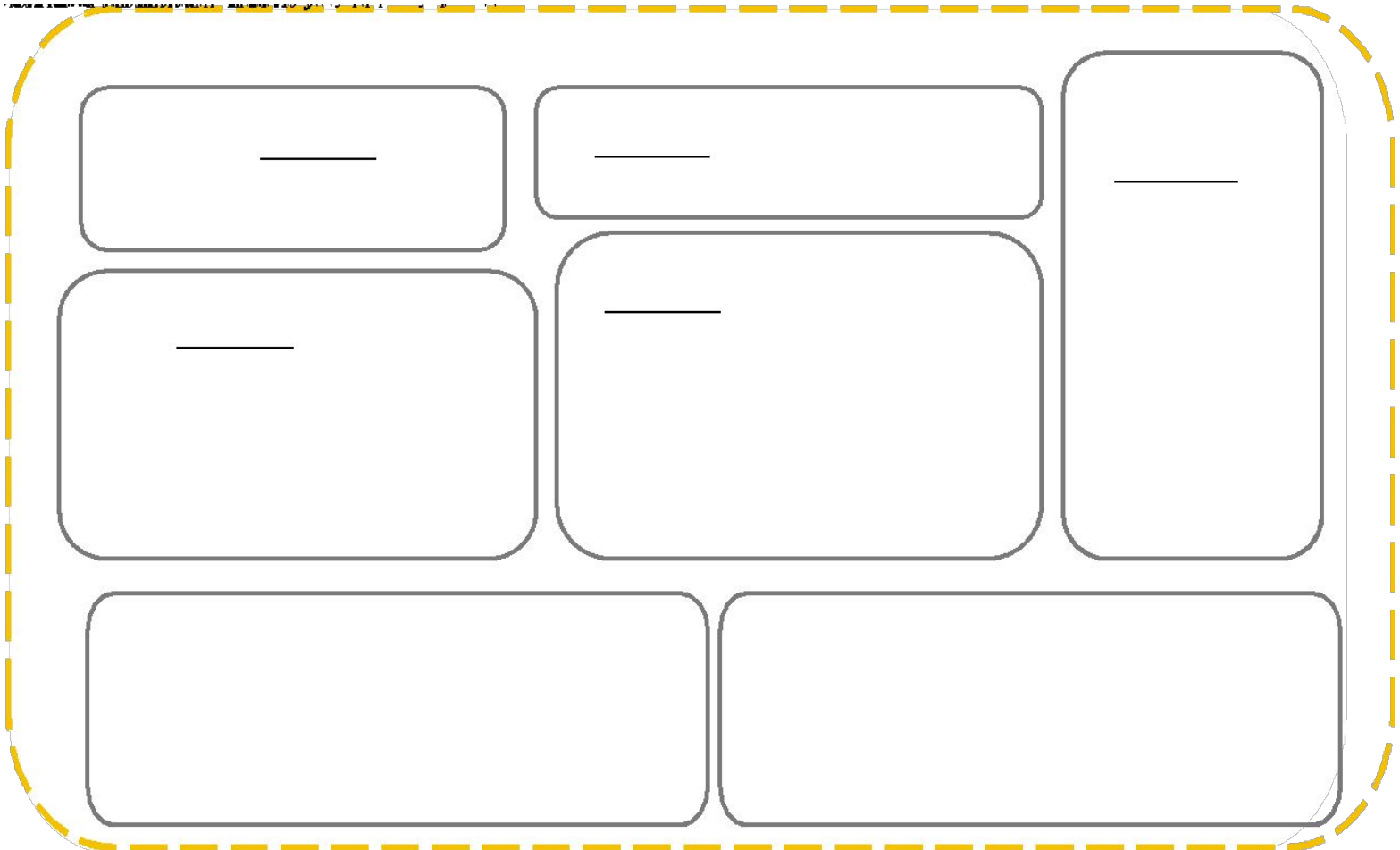
ПОЛОЖЕНИЕ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 № 381-П "О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ НАДЗОРА ЗА СОБЛЮДЕНИЕМ НЕ ЯВЛЯЮЩИМИСЯ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ ОПЕРАТОРАМИ ПЛАТЕЖНЫХ СИСТЕМ, ОПЕРАТОРАМИ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА ОТ 27 ИЮНЯ 2011 ГОДА N 161-ФЗ "О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ", ПРИНЯТЫХ В СООТВЕТСТВИЕ С НИМ НОРМАТИВНЫХ АКТОВ БАНКА РОССИИ

ПРЕДМЕТ ДОКУМЕНТА

- **Закреплено, как ЦБР надзирает за операторами услуг платежной инфраструктуры, не являющимися кредитными организациями.**
- **Банк России проводит**
  - **Дистанционный надзор (**оператору направляется запрос, указывается срок и время проведения проверки**),**
  - **Плановые инспекционные проверки (**не чаще 1 раза в 2 года**)**
  - **Внеплановые инспекционные проверки (**при нарушении бесперебойности функционирования значимой платежной системы, решение принимает Председатель Банка России.**)**
- **По результатам проверок составляется акт.**
- **К мерам принуждения относятся ограничение (приостановление) оказания операционных услуг, услуг платежного клиринга или исключение оператора платежной системы из реестра. Закреплен порядок их применения.**

Федеральный закон Российской Федерации от 27 июня 2011 г. **№ 161-ФЗ** "О национальной платежной системе"

Постановление Правительства Российской Федерации от 13 июня 2012 г. **№ 584** "Об утверждении Положения о защите информации в платежной системе

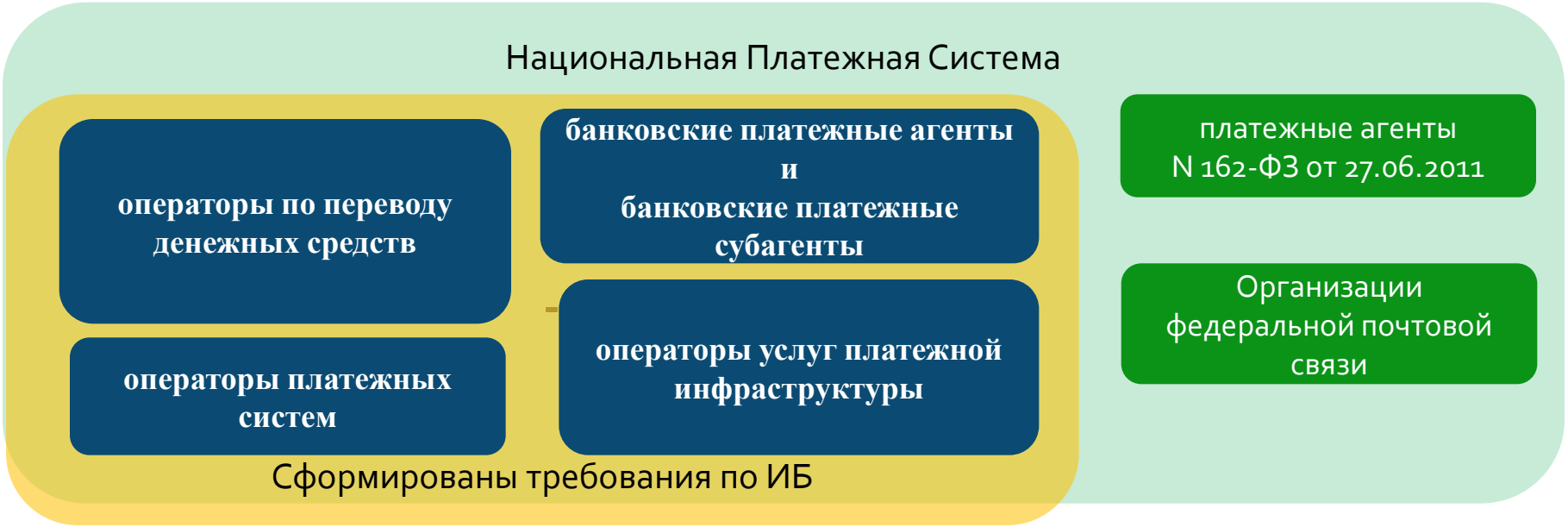


ПОЛОЖЕНИИ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 ГОДА № 382-П “О ТРЕБОВАНИЯХ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ И О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ БАНКОМ РОССИИ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ”

БАНК РОССИИ

ПРЕДМЕТ ДОКУМЕНТА

- **Положение устанавливает <u>требования</u>, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств (далее - требования к обеспечению защиты информации при осуществлении переводов денежных средств), а также устанавливает порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе**

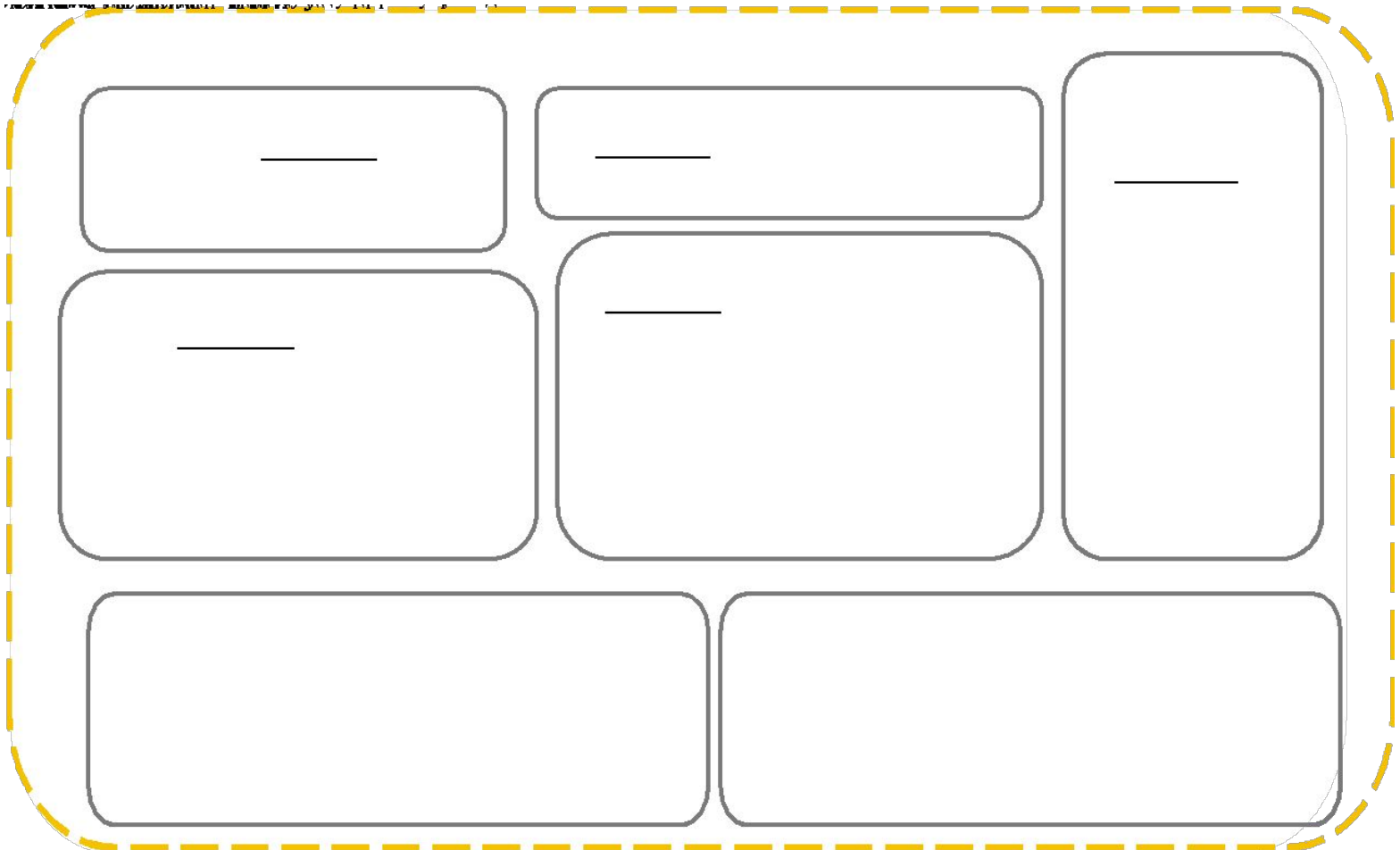


ПРЕДМЕТ ДОКУМЕНТА

- **Так, к защищаемым относятся сведения об остатках денежных средств на банковских счетах, а также электронных денег; о совершенных переводах денежных средств; о платежных клиринговых позициях. Речь идет и об информации, необходимой для удостоверения клиентами права распоряжения деньгами, а также ограниченного доступа, подлежащей обязательной защите и др.**
- **Приложение к документу содержит:**
  - Порядок проведения оценки соответствия и документирования ее результатов **(напоминает методику оценки соответствия СТО БР ИББС)**
  - Форма 1. Документирование результатов оценки соответствия
  - Форма 2. Документирование результатов вычислений обобщающих показателей выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств
  - Перечень требований к обеспечению защиты информации при осуществлении переводов денежных средств, выполнение которых проверяется при проведении оценки соответствия

Федеральный закон Российской Федерации от 27 июня 2011 г. **№ 161-ФЗ** "О национальной платежной системе"

Постановление Правительства Российской Федерации от 13 июня 2012 г. **№ 584** "Об утверждении Положения о защите информации в платежной системе



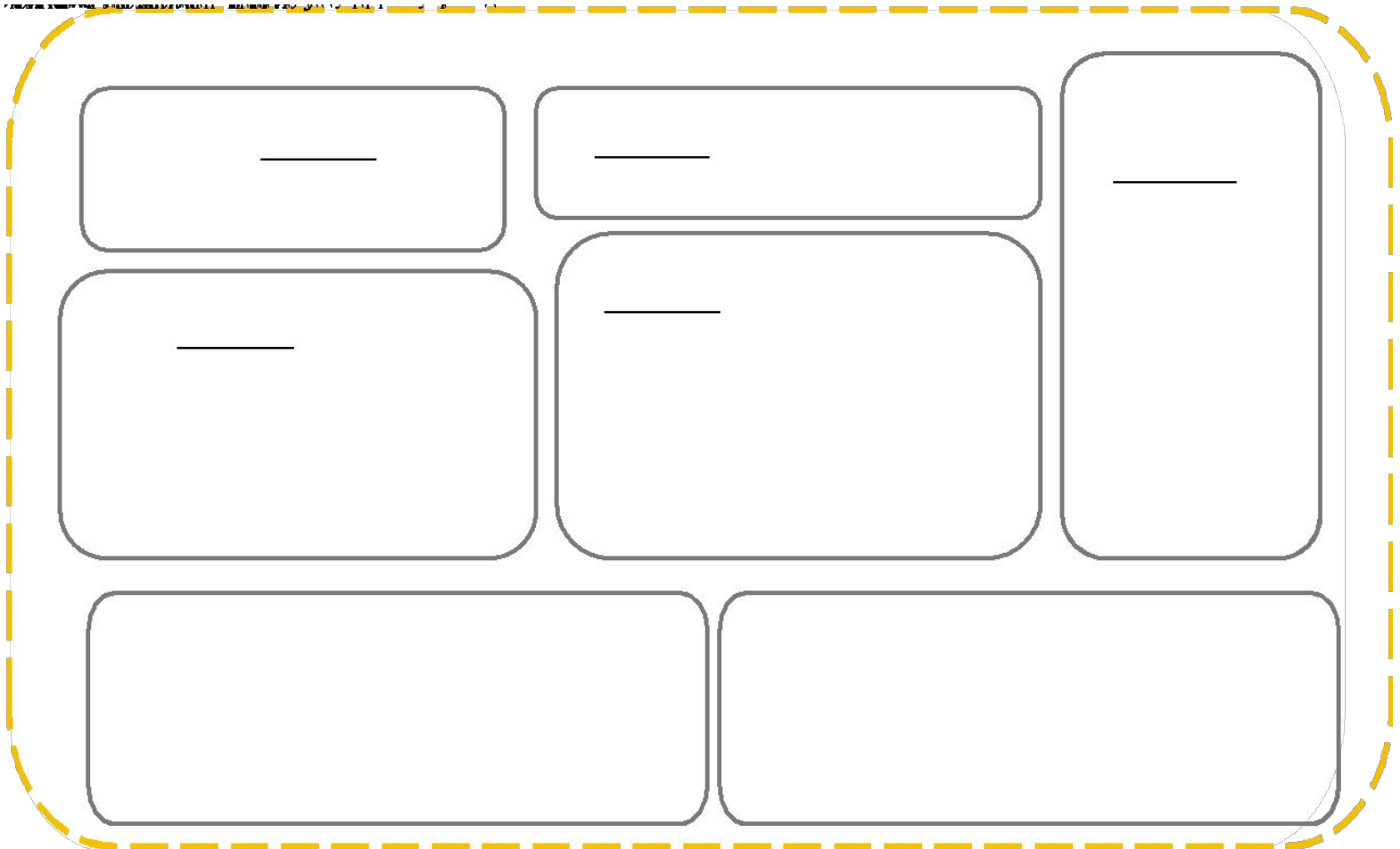
УКАЗАНИИ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 ГОДА №2831-У “ОБ ОТЧЕТНОСТИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ ОПЕРАТОРОВ ПЛАТЕЖНЫХ СИСТЕМ, ОПЕРАТОРОВ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ, ОПЕРАТОРОВ ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ”

ПРЕДМЕТ ДОКУМЕНТА

- ✔ Установлены формы отчетности по обеспечению защиты информации при осуществлении переводов денежных средств:
  - ✔ операторами платежных систем,
  - ✔ операторами услуг платежной инфраструктуры,
  - ✔ операторами по переводу денежных средств
- ✔ Определены сроки предоставления и методики составления.
- ✔ **Сведения о выполнении операторами требований к обеспечению защиты информации** подаются по форме 0403202.
- ✔ **Сведения о выявлении инцидентов, связанных с нарушением требований**, подаются по форме 0403203.

Федеральный закон Российской Федерации от 27 июня 2011 г. **№ 161-ФЗ** "О национальной платежной системе"

Постановление Правительства Российской Федерации от 13 июня 2012 г. **№ 584** "Об утверждении Положения о защите информации в платежной системе

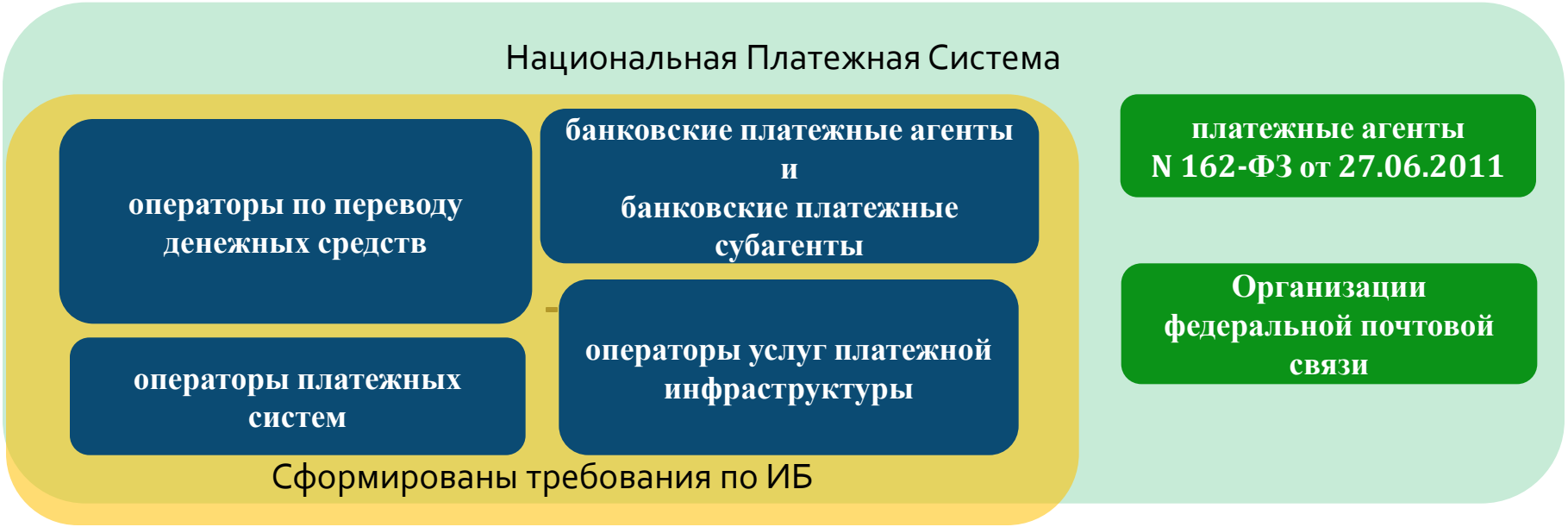


ПОЛОЖЕНИИ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 ГОДА № 382-П “О ТРЕБОВАНИЯХ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ И О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ БАНКОМ РОССИИ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ”

БАНК РОССИИ

ОБЩИЕ ПОЛОЖЕНИЯ

✔ **Положение устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств (далее - требования к обеспечению защиты информации при осуществлении переводов денежных средств), а также устанавливает порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе**



КОНТРОЛЬ И НАДЗОР

Субъекты НПС	Контроль и надзор
Оператор по переводу денежных средств	Банк России по 382-П
Операторы ПС	Банк России по 382-П
Операторы услуг платежной инфраструктуры	Банк России по 382-П
Банковские платежные агенты (субагенты)	Оператор ПС (с учетом операций, выполняемых агентами) по 382-П и Правилам ПС

Для проведения работ по обеспечению защиты информации при осуществлении переводов денежных средств операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры могут привлекать организации, имеющие лицензии на ТЗКИ и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.

АКТУАЛЬНОСТЬ ТРЕБОВАНИЙ ПО СУБ

Требования	№	Группы требований к обеспечению защиты инфомрации при осуществлении переводов ДС	Оператор ПС	Оператор по переводу ДС	Оператор по переводу электронных ДС	Операторы услуг платежной инфраструктуры	Банковский платежный агент
Требования показателя EV1	1	Защита информации при назначении и распределении ролей	-	+	+	+	+
	2	Защита информации на стадиях жизненного цикла объектов ИТ-инфраструктуры	-	+	+	+	+
	3	Защита информации при осуществлении доступа к объектам ИТ-инфраструктуры	-	+	+	+	+
	4	Защита информации от воздействия вредоносного кода	+	+	+	+	+
	5	Защита информации при использовании сети Интернет	-	+	+	+	+
	6	Защита информации с использованием СКЗИ	+	+	+	+	+
	7	Защита информации с использованием технологических мер защиты информации	+	+	+	+	+
	15*	Защита информации с применением банкоматов и платежных терминалов	-	+	+	+	-
Требования показателя EV2	8	Организация функционирования службы ИБ	-	+	+	+	-
	9	Повышение осведомленности в области обеспечения защиты информации	-	+	+	+	-
	10	Выявление и реагирование на инциденты	+	+	+	+	+
	11	Определение и реализация порядка обеспечения защиты информации	+	+	+	+	-
	12	Оценка выполнения требований к обеспечению защиты информации	+	+	+	+	-
	13	Информирование оператора ПС об обеспечении в ПС защиты информации	+	+	+	+	-
	14	Совершенствование защиты информации	+	+	+	+	-

к Положению Банка России
от 9 июня 2012 года N 382-П
"О требованиях к обеспечению защиты
информации при осуществлении
переводов денежных средств
и о порядке осуществления
Банком России контроля
за соблюдением требований
к обеспечению защиты
информации при осуществлении
переводов денежных средств"

ПЕРЕЧЕНЬ
ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ, ВЫПОЛНЕНИЕ КОТОРЫХ ПРОВЕРЯЕТСЯ ПРИ ПРОВЕДЕНИИ ОЦЕНКИ СООТВЕТСТВИЯ

N	Номер подпункта настоящего Положения	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств	Категории проверки требования
1	2	3	4
Требования к обеспечению защиты информации при осуществлении переводов денежных средств, оценки выполнения которых используются для вычисления обобщающего показателя EV1 ПС			
П.1	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по осуществлению доступа к защищаемой информации	Требование категории проверки 1
П.2	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по управлению криптографическими ключами	Требование категории проверки 1

ДОКУМЕНТИРОВАНИЯ ЕЕ РЕЗУЛЬТАТОВ

Требования категории проверки	Определение	Оценки
Требования категории проверки 1	требования реализуемые применение организационных мер защиты информации или использование технических средств защиты информации	0 0,25 0,5 0,75 1
Требования категории проверки 2	требования устанавливающие необходимость наличия документа	0 1
Требования категории проверки 3	требования устанавливающие необходимость выполнения	0 0,5 1

ТРЕБОВАНИЯ КАТЕГОРИИ ПРОВЕРКИ

Требование категории проверки 1	выполняется	выполняется почти в полном объеме	выполняется не в полном объеме	не выполняется
документировано	1	0,75	0,5	0,25
не документировано	0			

Требование категории проверки 2	
документировано	1
не документировано	0

Требование категории проверки 3	выполняется	выполняется частично	не выполняется
	1	0,5	0

ФОРМА 2. ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ ОЦЕНКИ СООТВЕТСТВИЯ

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

ОБОБЩАЮЩИЕ ПОКАЗАТЕЛИ

Требования показателя EV1	1	Защита информации при назначении и распределении ролей
	2	Защита информации на стадиях жизненного цикла объектов ИТ-инфраструктуры
	3	Защита информации при осуществлении доступа к объектам ИТ-инфраструктуры
	4	Защита информации от воздействия вредоносного кода
	5	Защита информации при использовании сети Интернет
	6	Защита информации с использованием СКЗИ
	7	Защита информации с использованием технологических мер защиты информации
	15*	Защита информации с применением банкоматов и платежных терминалов
Требования показателя EV2	8	Организация функционирования службы ИБ
	9	Повышение осведомленности в области обеспечения защиты информации
	10	Выявление и реагирование на инциденты
	11	Определение и реализация порядка обеспечения защиты информации
	12	Оценка выполнения требований к обеспечению защиты информации
	13	Информирование оператора ПС об обеспечении в ПС защиты информации
	14	Совершенствование защиты информации

- **EV1ПС – среднее арифметическое оценок выполнения указанных требований, умноженное на корректирующий коэффициент К1**
- **EV2ПС - среднее арифметическое оценок выполнения указанных требований, умноженное на корректирующий коэффициент К2**

КОРРЕКТИРУЮЩИЕ КОЭФФИЦИЕНТЫ

К1 принимается равным:

- **1 (если отсутствуют показатели в EV1ПС, требования которых полностью не выполняются)**
- **0,85 (если в EV1ПС меньше 11 требований которые полностью не выполняются)**
- **0,7 (если в EV1ПС ЧИСЛО требований которые полностью не выполняются больше или равно 11)**

К2:

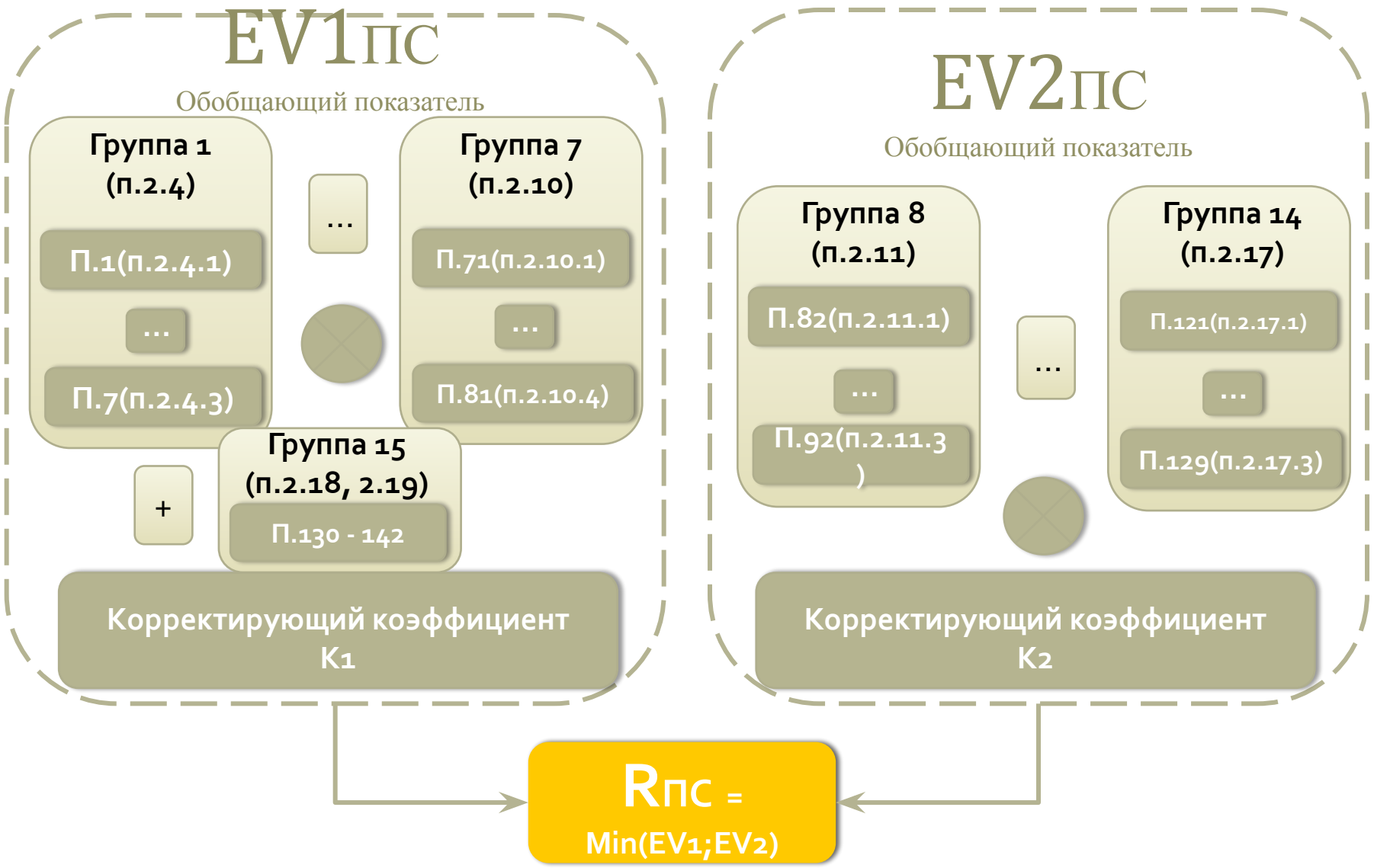
- **1 (если отсутствуют показатели в EV2ПС, требования которых полностью не выполняются)**
- **0,85 (если в EV2ПС меньше 6 требований которые полностью не выполняются)**
- **0,7 (если в EV2ПС число требований которые полностью не выполняются больше или равно 6)**

ИТОГОВЫЙ ПОКАЗАТЕЛЬ ОЦЕНКИ

$$R_{ПС} = Min(EV1;EV2)$$

$R_{ПС}$	Значение качественной оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств
Rпс>=0,85	"хорошая"
0,7<=Rпс<0,85	"удовлетворительная"
0,5<=Rпс<0,7	"сомнительная"
Rпс<0,5	"неудовлетворительная"

РАСЧЕТ ПОКАЗАТЕЛЕЙ



ФОРМА 2. ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ ВЫЧИСЛЕНИЙ ОБОБЩАЮЩИХ ПОКАЗАТЕЛЕЙ

Обобщающий показатель	Значение обобщающего показателя
1	2
EV1 ПС	
EV2 ПС	
R ПС	

КЛАССИЧЕСКИЕ ОШИБКИ/ПРОБЛЕМЫ ОЦЕНКИ СООТВЕТСТВИЯ ПО 382-П

- Недостаточное понимание аудитором платежного процесса
- Неверная интерпретация «шкалы» (требования категории проверки)
- Необоснованная пессимизация показателя
- Необоснованное завышение показателя
- Ошибки при сборе свидетельств
- Обоснование не соответствует выставленной оценке
- Терминологические проблемы (инцидент)

НЕДОСТАТОЧНОЕ ПОНИМАНИЕ АУДИТОРОМ ПЛАТЕЖНОГО ПРОЦЕССА

- **Платежные системы:**
  - Платежи РКЦ
  - SWIFT
  - Биржи
  - Банк-клиент
  - WU
  - И т.д
- **Платежные процессы:**
  - Бизнес
  - ИТ
  - ИБ

НЕВЕРНАЯ ИНТЕРПРЕТАЦИЯ «ШКАЛЫ»

Требование категории проверки 1	выполняется	выполняется почти в полном объеме	выполняется не в полном объеме	не выполняется
документировано	1	0,75	0,5	0,25
не документировано	0			

Требование категории проверки 2	
документировано	1
не документировано	0

Требование категории проверки 3	выполняется	выполняется частично	не выполняется
	1	0,5	0

НЕВЕРНАЯ ИНТЕРПРЕТАЦИЯ «ШКАЛЫ»

№ п/п	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
П.102	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают информирование службы информационной безопасности, в случае ее наличия, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	1	Имеется журнал инцидентов, считаем, что обновление производится Требование категории проверки 3
П.103	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	1	Имеется регламент реагирование на инциденты Требование категории проверки 1

НЕОБОСНОВАННОЕ ЗАВЫШЕНИЕ ПОКАЗАТЕЛЯ

№ п/п	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
П.102	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают информирование службы информационной безопасности, в случае ее наличия, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	1	Имеется журнал инцидентов, считаем, что обновление производится Требование категории проверки 3 На основании каких свидетельств сделан такой вывод?
П.103	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	1	Имеется регламент реагирование на инциденты Требование категории проверки 1 На основании каких свидетельств сделан такой вывод?

НЕОБОСНОВАННАЯ ПЕССИМИЗАЦИЯ ПОКАЗАТЕЛЯ

№ п/п	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
П.85	Служба информационной безопасности и служба информатизации (автоматизации) не должны иметь общего куратора.	0,5	ИБ имеет общего куратора с управлением мониторинга транзакций УМТ не является ИТ

ОШИБКИ ПРИ СБОРЕ СВИДЕТЕЛЬСТВ

1. **Запросили и проанализировали документы по ИБ**
2. **Опросили безопасников, кадровиков и руководство**
3. **Ничего не спрашиваем у бизнеса и\или ИТ**

Фантазируем при документировании результатов оценки

«ЭТАПНОСТЬ» ПРОВЕДЕНИЯ ОЦЕНКИ

1. **Анализ документов**
2. **Проведение интервью**
3. **Анализ свидетельств**
4. **Проведение итоговой оценки соответствия**

«ЭТАПНОСТЬ» ПРОВЕДЕНИЯ ОЦЕНКИ

1. Анализ документов
2. Проведение интервью
3. Анализ свидетельств
4. Проведение предварительной оценки соответствия
5. Сбор недостающих свидетельств
6. Анализ свидетельств
7. Проведение итоговой оценки соответствия

ВНЕДРЕНИЕ ТРЕБОВАНИЙ 382-П В ПРОЕКТНОМ РЕЖИМЕ

1. **План устранения несоответствий:**
   - Несоответствие из Формы 1
   - Мероприятие
   - Ответственный/Участники
   - Срок
   - Ресурсы
2. **Подготовка документов**
3. **Внедрение процессов (Система управления инцидентами)**

УКАЗАНИИ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 ГОДА №2831-У “ОБ ОТЧЕТНОСТИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ ОПЕРАТОРОВ ПЛАТЕЖНЫХ СИСТЕМ, ОПЕРАТОРОВ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ, ОПЕРАТОРОВ ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ”

БАНК РОССИИ

ПРЕДМЕТ ДОКУМЕНТА

- ✔ Установлены формы отчетности по обеспечению защиты информации при осуществлении переводов денежных средств:
  - ✔ операторами платежных систем,
  - ✔ операторами услуг платежной инфраструктуры,
  - ✔ операторами по переводу денежных средств
- ✔ Определены сроки предоставления и методики составления.
- ✔ **Сведения о выполнении операторами требований к обеспечению защиты информации** подаются по форме 0403202.
- ✔ **Сведения о выявлении инцидентов, связанных с нарушением требований**, подаются по форме 0403203.

Отчетность	Периодичность предоставления	Крайний срок
Сведения о выполнении требований к обеспечению защиты информации при осуществлении переводов денежных средств	Не реже одного раза в два года, а также по требованию Банка России Не позднее 30 рабочих дней со дня завершения оценки выполнения требований Положения N382-П	Первая оценка должна быть завершена не позднее 01.07.2014 Первый отчет должен быть предоставлен не позднее 11.08.2014
Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств	Ежемесячно, не позднее 10 рабочего дня месяца, следующего за отчетным	Выявление и регистрация инцидентов должны начаться с 01.07.2012 Первый отчет должен быть предоставлен не позднее 14.08.2012

ФОРМА 0403202

Сведения о выполнении операторами платежных систем, операторами услуг платежной инфраструктуры, операторами по переводу денежных средств требований к обеспечению защиты информации при осуществлении переводов денежных средств

по состоянию на "__" _____ ____ г.

Наименование _____

Почтовый адрес _____

Код формы по ОКУД 0403202

На нерегулярной основе

I	Вид деятельности	
II	Регистрационный номер оператора платежной системы	
III	Предоставление услуг платежной инфраструктуры	
IV	Участие в платежных системах	

Номер строки	Вид сведений	Содержание
1	2	3
Сведения о выполнении требований к обеспечению защиты информации при осуществлении переводов денежных средств		
1	Показатель EV1 ПС	
2	Показатель EV2 ПС	
3	Итоговый показатель R ПС	
Сведения об оценке выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств		
4	Проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств	

Руководитель
(заместитель руководителя) _____ _____
(личная подпись) (инициалы, фамилия)

М.П.

Исполнитель _____ _____
(личная подпись) (инициалы, фамилия)

Номер телефона:

ФОРМА 0403203

Сведения о выявлении инцидентов, связанных
с нарушением требований к обеспечению защиты информации
при осуществлении переводов денежных средств

по состоянию на "__" _____ ____ г.

Наименование _____
Почтовый адрес _____

Код формы по ОКУД 0403203

Месячная

Количество инцидентов (единицы) _____

Номер строки	Дата выявления инцидента	Наименование банковского платежного агента (субагента)	Код банковского платежного агента (субагента) по ОКПО	Регистрационные номера операторов платежных систем	Последствия инцидента	Объекты информационной инфраструктуры	Описание предпринятых действий по устранению последствий инцидента	Факт обращения в правоохранительные органы
1	2	3	4	5	6	7	8	9

Руководитель
(заместитель руководителя) _____ _____
(личная подпись) (инициалы, фамилия)

М.П.

Исполнитель _____ _____
(личная подпись) (инициалы, фамилия)

ПРОЕКТ ПОПРАВОК 2831-У

- ✔ Вместо одной отчетной таблицы по инцидентам , планируется две.:
  - ✔ Сведения об инцидентах отчетного периода
  - ✔ Сведения об инцидентах прошлых отчетных периодов

- ✔ Заполняются кодами на основе методики.

УПРАВЛЕНИЯ ИНЦИДЕНТАМИ? «СМЕНА» ФОРМЫ 203.

Раздел 3. Сведения об инцидентах отчетного периода

Номер строки	Тип инцидента	Даты выявления (возникновения) инцидента	Условия возникновения инцидента	Описание инцидента	Причина инцидента	Дополнительные сведения об инциденте	Регион возникновения инцидента	Нарушенное требование Положения Банка России № 382-П	Отношение к платежной системе	Последствия инцидента			Описание предпринятых действий по устранению последствий инцидента	Факт обращения в правоохранительные органы	Сведения о выявлении инцидента клиентом, банковским платежным агентом (субагентом), операционным центром, находящимся за пределами Российской Федерации	Код банковского платежного агента (субагента)	Дата завершения разбирательства по инциденту	Код инцидента
										Суммы переводов денежных средств	Нарушение сроков	Оценка убытка						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

Раздел 4. Сведения об инцидентах предыдущих отчетных периодов

Номер строки	Код инцидента	Тип инцидента	Даты завершения разбирательства по инциденту (возникновения инцидента)	Условия возникновения инцидента	Описание инцидента	Причина инцидента	Дополнительные сведения об инциденте	Регион возникновения инцидента	Нарушенное требование Положения Банка России № 382-П	Отношение к платежной системе	Последствия инцидента			Описание предпринятых действий по устранению последствий инцидента	Факт обращения в правоохранительные органы	Сведения о выявлении инцидента клиентом, банковским платежным агентом (субагентом), операционным центром, находящимся за пределами Российской Федерации	Код банковского платежного агента (субагента)
											Суммы переводов денежных средств	Нарушение сроков	Оценка убытка				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

УКАЗАНИИ БАНКА РОССИИ ОТ 5 ИЮНЯ 2013 ГОДА №3007-У
О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПОЛОЖЕНИЕ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 ГОДА № 382-П "О ТРЕБОВАНИЯХ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ И О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ БАНКОМ РОССИИ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ"

ВНЕСЕНИЕ ПОПРАВОК В 382-П

1. Исправлены незначительные ошибки
2. Внесены изменения в отдельные подпункты положения и Приложения 2
3. Добавлены новые требования (29.1–29.4, 106.1, 106.2, 113.1, 113.2)
4. Как отчитываться по проведенной оценке?
    1. 202-я форма
    2. Форма 1
    3. Сведения о сторонней организации

УКАЗАНИИ БАНКА РОССИИ ОТ 14 АВГУСТА 2014 ГОДА №3361-У "О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПОЛОЖЕНИЕ БАНКА РОССИИ ОТ 9 ИЮНЯ 2012 ГОДА № 382-П "О ТРЕБОВАНИЯХ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ И О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ БАНКОМ РОССИИ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ"

ВНЕСЕНИЕ ПОПРАВОК В 382-П

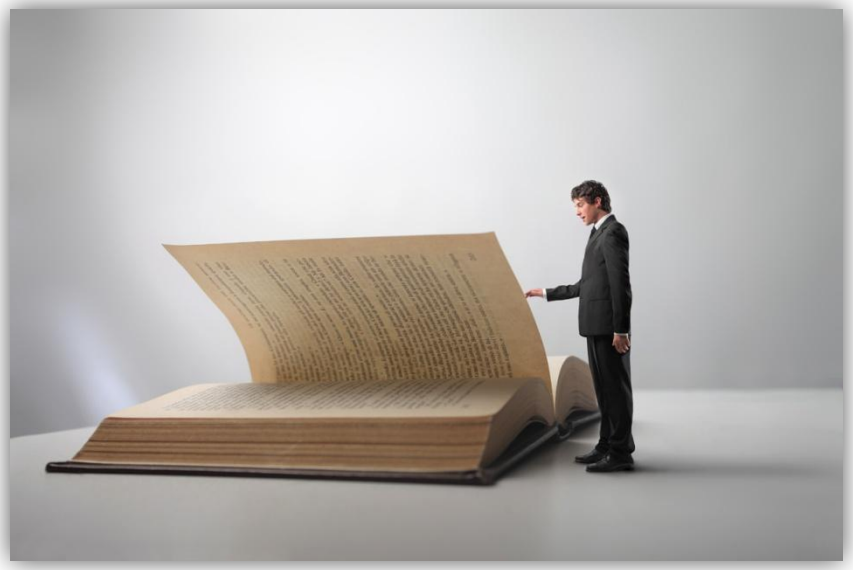
1. Исправлены незначительные ошибки
2. Определены требования для осуществления переводов с использованием систем Интернет-банкинга, мобильного банкинга, а также требования к использованию платежных карт, оснащенных микропроцессором
3. Добавлена новая группа требований к защите информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов
4. Определены факторы, которые должны учитываться при реализации требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе с учетом особенностей конструкции и места установки терминальных устройств дистанционного банковского обслуживания

Коллеги,
Большое спасибо за внимание и совместную работу!

Web: http://www.tsarev.biz/
Twitter: http://twitter.com/TsarevEvgeny
Facebook: http://www.facebook.com/tsarev.biz
E-mail: TsarevEO@gmail.com
Tel: +7-926-104-70-58

Конец первого дня

ОЦЕНКА СООТВЕТСТВИЯ



Конец второго дня

ВНЕДРЕНИЕ

ВНЕДРЕНИЕ ТРЕБОВАНИЙ 382-П В ПРОЕКТНОМ РЕЖИМЕ

1. **План устранения несоответствий:**
   - Несоответствие из Формы 1
   - Мероприятие
   - Ответственный/Участники
   - Срок
   - Ресурсы
2. **Подготовка документов**
3. **Внедрение процессов (Система управления инцидентами)**

ПОДХОДЫ К РАЗРАБОТКЕ ДОКУМЕНТАЦИИ

Подход:

- **От плана устранения несоответствий**
- **От групп требований**
- **От систем попадающих в область работ**

ПРИМЕР ПЛАТЕЖНЫХ СИСТЕМ

Работа с Банком России:

- **КБР**
- **БЭСП**
- **SWIFT**
- **Telex**
- **Платежи РКЦ**
- **Биржи**

ДБО:

- **BSS**
- **Мобильный банкинг**

Внутренние системы банка:

- **АБС (Афина, Диасофт)**

Сторонние платежные системы:

- **Migom**
- **WU**

- **Позволяет создать единое понимание Scope**
- **В основном используется при сложной системе документации**

План устранения несоответствий

№	Название мероприятия	№ п/п по 382-П	Дни	Ответственный сотрудник	Сторонний исполнитель
20	Разработать требования к системе ДБО	28			
21	Включить в документацию требование по регистрации действий, связанных с назначением и распределением прав клиентов, предоставленных им в автоматизированных системах и программном обеспечении, при наличии технической возможности.	29			
22	Рекомендуется внедрить решение класса IDM.	31			
23	Использовать технические средства защиты информации от воздействия вредоносного кода различных производителей и осуществить их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении переводов денежных средств, при наличии технической возможности.	44			
24	Документально не регламентирована необходимость приостанавливать при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом	49			
25	Дополнить анкету клиента по ИБ рабочего места и памятку по обеспечению безопасности ДБО рекомендацией по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.	54			
26	Документировать процедуру учета и контроля состава установленного и(или) используемого на средствах вычислительной техники программного обеспечения.	71			
27	Дополнить существующую документацию формулировкой: Распоряжение клиента, распоряжение участника платежной системы и распоряжение платежного клирингового центра в электронном виде может быть удостоверено электронной подписью, а также в соответствии с пунктом 3 статьи 847 Гражданского кодекса Российской Федерации аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом.	74			

План устранения несоответствий

28	Необходимо добавить фразу и раскрыть ее содержание в разрабатываемой документации: «Сотрудники Управления информационных технологий осуществляют контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры. Контроли их деятельности осуществляет ОИБ»	76			
29	Разработать регламент работы с системой FRAUD-анализ, разработки ООО «БСС»	81, 101			
30	Выделить цели подразделения	82			
31	Разработать документ о назначении куратора и определении полномочий.	84			
32	Добавить правильную формулировку по полномочиям в положение об отделе. Создать/Найти планы внедрения СОИБ/Документы свидетельствующие о контроле обеспечения защиты информации при осуществлении переводов денежных средств	88			
35	Добавить формулировку по полномочиям в положение об отделе. Создать/Найти планы внедрения СОИБ/Документы свидетельствующие о контроле обеспечения защиты информации при осуществлении переводов денежных средств.	91, 92			
36	Подготовить документы по обучению сотрудников Банка (ЧП, Положение)	93, 94, 95			
37	Разработать перечень ПС участником, которых является Банк (оператор по переводу ДС). Отсутствую принятые правила ПС.	50, 98, 100, 108, 109, 115, 116, 117, 118, 119, 120			

План устранения несоответствий

38	Использовать системы сбора и корреляции событий. Закупка и внедрение SIEM.	101			
39	Разработать регламент содержащий процедуры выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	101			
40	Сделать дополнения в шаблон должностных инструкций с требованием информирования службы информационной безопасности, о выявлении инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	102			
41	Разработать регламент содержащий процедуры информирования службы ИБ об инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	102			
42	Сделать дополнения в шаблон должностных инструкций с требованием реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	103, 104			
43	Разработать регламент содержащий процедуры реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.	103, 104			
44	Разработать журнал инцидентов либо базу инцидентов. Заявки от пользователей должны фиксироваться. Реализуется функционалом SIEM.	103, 104, 112			
45	Добавить в должностные инструкции сотрудников ОИБ требование: Лицами, ответственным за выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств назначены сотрудники ОИБ	110			

ГРУППЫ ТРЕБОВАНИЙ

№	Группы требований к обеспечению защиты информации при осуществлении переводов ДС
1	Защита информации при назначении и распределении ролей
2	Защита информации на стадиях жизненного цикла объектов ИТ-инфраструктуры
3	Защита информации при осуществлении доступа к объектам ИТ-инфраструктуры
4	Защита информации от воздействия вредоносного кода
5	Защита информации при использовании сети Интернет
6	Защита информации с использованием СКЗИ
7	Защита информации с использованием технологических мер защиты информации
8	Организация функционирования службы ИБ
9	Повышение осведомленности в области обеспечения защиты информации
10	Выявление и реагирование на инциденты
11	Определение и реализация порядка обеспечения защиты информации
12	Оценка выполнения требований к обеспечению защиты информации
13	Информирование оператора ПС об обеспечении в ПС защиты информации
14	Совершенствование защиты информации

Позволяет:

- Определить последовательность внедрения
- Выбрать единую систему документации для всей группы требований

В основном используется в случае отсутствия документации

14. СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Терминология

Совершенствование (поддержка и улучшение) - проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения.

[адаптировано из ГОСТ Р ИСО/МЭК 27001]

Корректирующее действие (corrective action) - действие, предпринятое для устранения причины обнаруженного несоответствия или другой нежелательной ситуации.

Примечания

1 Несоответствие может иметь несколько причин.

2 Корректирующее действие предпринимают для предотвращения повторного возникновения события, а предупреждающее действие— для предотвращения возникновения события.

3 Следует различать термины коррекция и корректирующее действие.

[ГОСТ Р ИСО 9000-2008]

Терминология (продолжение)

Коррекция (correction) - действие, предпринятое для устранения обнаруженного несоответствия.

Примечания

1 Коррекция может осуществляться в сочетании с корректирующим действием.

2 Коррекция может включать в себя, например, переделку или снижение градации. [ГОСТ Р ИСО 9000-2008]

Предупреждающее действие (preventive) - действие, предпринятое для устранения причины потенциального несоответствия или другой потенциально нежелательной ситуации.

Примечания

1 Потенциальное несоответствие может иметь несколько причин.

2 Предупреждающее действие предпринимают для предотвращения возникновения события, а корректирующее действие — для предотвращения повторного возникновения события. [ГОСТ Р ИСО 9000-2008]

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.121 Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями требований к защите информации, определенных правилами платежной системы	ОПС ОПДС ОУПИ	СТО БР ИББС-1.0 П. 8.17.2, 8.18.1
П.122 Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе	ОПС ОПДС ОУПИ	СТО БР ИББС-1.0 П. 8.17.2, 8.18.1

Ссылки в последней графе относятся как к требованиям, связанным с причинами совершенствования, так и с результатами (принятием соответствующих решений).

Следствия

Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры **регламентируют пересмотр порядка обеспечения защиты информации.**

Пересмотр ограничен в рамках обязанностей, установленных оператором платежной системы.

Основания для пересмотра:

1 изменения требований к защите информации, определенных правилами платежной системы;

2 регулятивные изменения.

Соответственно, **субъекты НПС должны отслеживать эти изменения**. Для этого необходима организация соответствующей деятельности, начиная от выделения ролей в части отслеживания изменений, их анализа и реализации. Необходимо и создание некоторой информационной базы для фиксирования требований и результатов их реализации.

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.123 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения требований к защите информации, определенных правилами платежной системы	ОПДС ОУПИ	СТО БР ИББС-1.0 П. 8.17.2
П.124 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующих отношения в национальной платежной системе	ОПДС ОУПИ	СТО БР ИББС-1.0 П.8.18.1
П.125 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	СТО БР ИББС-1.0 П. 8.17.1, 8.18.1

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.126 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	СТО БР ИББС-1.0 П. 8.17.1, 8.18.1
П.127 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	СТО БР ИББС-1.0 П. 8.17.1, 8.18.1
П.128 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при проведении оценки соответствия	ОПДС ОУПИ	СТО БР ИББС-1.0 П. 8.17.1, 8.18.1

Следствия

Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры **регламентируют порядок принятия мер, направленных на совершенствование защиты информации**

Основания для совершенствования:

1 изменения требований к защите информации, определенных правилами платежной системы;

2 регулятивные изменения;

3 изменения порядка обеспечения защиты информации;

4 выявления угроз, рисков и уязвимостей;

5 выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации;

6 выявления недостатков при проведении оценки соответствия.

Обращает внимание «жесткий» набор оснований для совершенствования, а также то, что требования пункта 2.17.2 не распространяются на ОПС.

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.129 Принятие решений оператора по переводу денежных средств, оператора услуг платежной инфраструктуры по совершенствованию защиты информации при осуществлении переводов денежных средств согласуется со службой информационной безопасности	ОПДС ОУПИ	СТО БР ИББС-1.0 П. 8.17.4

Направления совершенствования по ГОСТ Р ИСО/МЭК 27001

Корректирующие действия

Организация должна проводить мероприятия по устранению причин несоответствий требованиям СМИБ с целью предупредить их повторное возникновение. Документированная процедура корректирующего действия должна устанавливать требования по:

a) выявлению несоответствий;

b) определению причин несоответствий;

c) оцениванию необходимости действий во избежание повторения несоответствий;

d) определению и реализации необходимых корректирующих действий;

e) ведению записей результатов предпринятых действий;

f) анализу предпринятого корректирующего действия.

Направления совершенствования по ГОСТ Р ИСО/МЭК 27001

Предупреждающие действия

Организация должна определять действия, необходимые для устранения причин потенциальных несоответствий требованиям СМИБ, с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия должны соответствовать последствиям потенциальных проблем. Документированная процедура предпринятого предупреждающего действия должна устанавливать требования по:

a) выявлению потенциальных несоответствий и их причин;

b) оцениванию необходимости действия с целью предупредить появление несоответствий;

c) определению и реализации необходимого предупреждающего действия;

d) записи результатов предпринятого действия;

e) анализу результатов предпринятого действия.

Направления совершенствования по СТО БР ИББС- 1.0

К **тактическим улучшениям** СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СОИБ организации БС РФ и не требующие пересмотра политики ИБ и частных политик ИБ организации БС РФ. Как правило, тактические улучшения СОИБ не требуют выполнения деятельности в рамках этапа «планирование» СМИБ.

К **стратегическим улучшениям** СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром политики ИБ и частных политик ИБ организации БС РФ, с последующим выполнением соответствующих тактических улучшений СОИБ. Стратегические улучшения СОИБ всегда требуют выполнения деятельности в рамках этапа «планирование» СМИБ.

Исходные данные для принятия решений **и решения** по тактическим и стратегическим улучшениям СОИБ **должны быть документально зафиксированы**.

Решения должны содержать либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо должны быть указаны направления улучшений СОИБ в виде корректирующих или превентивных действий.

Основания для совершенствования по СТО БР ИББС-1.0

- аудитов ИБ;
- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- анализа перечня защитных мер, возможных для применения;
- **стратегических улучшений СОИБ**;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций).

Примеры решений по тактическим улучшениям (СТО БР ИББС-1.0)

- пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;
- пересмотр процедур эксплуатации отдельных видов защитных мер;
- пересмотр процедур обнаружения и обработки инцидентов;
- уточнение описи информационных активов;
- пересмотр программы обучения и повышения осведомленности персонала;
- пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;
- пересмотр планов обработки рисков;
- вынесение санкций в отношении персонала;
- пересмотр процедур мониторинга СОИБ и контроля защитных мер;
- пересмотр программ аудитов;
- корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;
- ввод новых или замена используемых защитных мер.

Примеры решений по стратегическим улучшениям

- уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ или частных политик ИБ организации БС РФ;
- изменение в области действия СОИБ;
- уточнение описи типов информационных активов;
- пересмотр моделей угроз и нарушителей;
- изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

Кроме того выполнить ряд деятельностей:

- выработку планов тактических улучшений СОИБ;
- уточнение планов обработки рисков;
- уточнение программы внедрения защитных мер;
- уточнение процедур использования защитных мер.

Требования к совершенствованию защиты в PCI-DSS

В PCI-DSS требования к совершенствованию защиты также присутствуют, только не выделены в некий отдельный процесс, как это определяется для СМИБ.

При этом принятию действий также **предшествуют процессы проверки**, такие как: тестирование, сканирование, контроль, мониторинг.

Действия в рамках совершенствования формулируются, например, следующим образом «установка обновлений безопасности», «устранение выявленных уязвимостей» и др.

Пример требований из PCI-DSS

Требование PCI DSS	Проверочные процедуры
11.3 Следует проводить **внешний и внутренний тест на проникновение** не реже одного раза в год, а также **после любого значимого изменения или обновления инфраструктуры и приложений** (например, обновления операционной системы, добавления подсети, установки веб-сервера). Данные тесты на проникновение должны включать:	11.3.a Изучить результаты последнего теста на проникновение, убедиться в том, что тест на проникновение осуществляется не реже одного раза в год и после всех значительных изменений в инфраструктуре.
	11.3.b **Убедиться в том, что выявленные уязвимости были устранены и проведен повторный тест.**
	11.3.c Убедиться в том, что тест на проникновение был проведен квалифицированными сотрудниками компании либо квалифицированной третьей стороной, а также убедиться в их организационной независимости (если это возможно; при этом наличие статуса QSA или ASV не требуется).

Итого

По группе требований 14. Совершенствование защиты информации необходимо разработать:

- **регламент пересмотра порядка обеспечения защиты информации**
- **порядок принятия мер, направленных на совершенствование защиты информации**
- Рекомендуется учесть:
- **ГОСТ Р ИСО/МЭК 27001 (корректирующие, предупреждающие действия)**
- **СТО БР ИББС- 1.0 (тактические, стратегические улучшения, совершенствование СОИБ)**
- **PCI DSS (11.3)**

13. ИНФОРМИРОВАНИЕ ОПЕРАТОРА ПС ОБ ОБЕСПЕЧЕНИИ В ПС ЗАЩИТЫ ИНФОРМАЦИИ

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.114 Оператор платежной системы устанавливает требования к содержанию, форме и периодичности представления информации, направляемой операторами по переводу денежных средств и операторами услуг платежной инфраструктуры оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств	ОПС	Комплекс БР ИББС
П.115 Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанных в подпункте 2.16.1 пункта 2.16 настоящего Положения требований	ОПДС ОУПИ	Комплекс БР ИББС

Ссылки в последней графе не носят характер прямого соответствия. Такая информация как, например, информация о выявленных угрозах и уязвимостях в обеспечении защиты информации передается как правило внутри одной организации (от филиалов в головной офис).

СЛЕДСТВИЯ

- **оператор платежной системы устанавливает требования** к содержанию, форме и периодичности представления информации **от участников его ПС**;
- **оператор по переводу денежных средств и оператор услуг платежной инфраструктуры** обеспечивают выполнение указанных требований;
- **каждым оператором платежной системы могут быть установлены свои требования**, их объем и содержание будут различны.

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.116 Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о степени выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	Комплекс БР ИББС
П.117 Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.118 Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	
П.119 Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о результатах проведенных оценок соответствия	ОПДС ОУПИ	Комплекс БР ИББС
П.120 Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о выявленных угрозах и уязвимостях в обеспечении защиты информации	ОПДС ОУПИ	

РЕЗЮМЕ ПО П. 2.16 ПОЛОЖЕНИЯ

- **В большей части требования направлены на деятельность в рамках отдельных платежных систем, т. к. потребителями информации являются операторы платежных систем. В то же время оценка выполнения этих требований выдается и внешней (третьей) стороне, а именно – Банку России.**

- **Действия в рамках Положения № 382-П заканчиваются документированием результатов оценки и выходом на осуществление Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств. Данный порядок определен в главе 3 Положения**

Итого

По группе требований 13. Информирование оператора ПС об обеспечении в ПС защиты информации необходимо разработать:

Оператору платежной системы:

- **Требование к отчетности участников ПС (для Правил ПС)**
- **Регламент сбора отчетности**

Участникам ПС:

- **Регламент подготовки и отправки отчетности операторам ПС**

11. ОЦЕНКА ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.113 Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России	ОПДС ОПС ОУПИ	СТО БР ИББС-1.0
П.113.1 Организация, ставшая оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, должна провести первую оценку соответствия в течение шести месяцев после получения соответствующего статуса	ОПДС ОПС ОУПИ	Комплекс БР ИББС
П.113.2 Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры по результатам оценки соответствия в целях ее документального подтверждения формируют отчет, который утверждается исполнительными органами управления и хранится в порядке, установленном соответствующим оператором_ Отчет включает сведения о проведении оценки соответствия, в том числе: заполненную форму 1, установленную приложением 1 к настоящему Положению и содержащую оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств; заполненную форму 2, установленную приложением 1 к настоящему Положению и содержащую оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств; сроки проведения оценки соответствия; сведения о сторонней организации (наименование и местонахождение) в случае ее привлечения оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры для проведения оценки соответствия	ОПДС ОПС ОУПИ	Комплекс БР ИББС

СЛЕДСТВИЯ

- оценка должна осуществляться не реже одного раза в два года, а также по требованию Банка России;
- требования основной части пункта 2.15.3 и 2.15.4 Положения № 382-П также носят методический характер (не проверяются);
- необходимо провести оценку соответствия до начала 2014 года;
- оценка может осуществляться как самими субъектами НПС, так и с привлечением сторонних организаций.
- предоставить в ЦБ информацию:
  - заполненную форму 1;
  - заполненную форму 2;
  - сроки проведения оценки соответствия;
  - сведения о сторонней организации.

Итого

По группе требований 11. Оценка выполнения требований к обеспечению защиты информации необходимо разработать :

- **регламент проведения оценки соответствия**
- **план и программа оценок соответствия**
- Рекомендуется учесть:
- **СТО БР ИББС- 1.0 (план аудита/самооценки, программа аудитов/самооценок)**

10. ВЫЯВЛЕНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

ТЕРМИНОЛОГИЯ

Согласно 382-П в редакции после принятия 3007-У:

Инцидент, связанный с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств - событие, которое возникло вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств и (или) условия осуществления (требования к осуществлению) перевода денежных средств, связанные с обеспечением защиты информации при осуществлении переводов денежных средств, которое установлено оператором по переводу денежных средств и доведены им до клиента, и которое:

- **привело к несвоевременности** (к нарушению сроков, установленных законодательством Российской Федерации, правилами платежных систем и (или) договорами, заключаемыми клиентами, операторами по переводу денежных средств, операторами услуг платежной инфраструктуры, операторами платежных систем, банковскими платежными агентами (субагентами), участниками платежных систем) **осуществления переводов денежных средств**;
- привело или может привести к осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;
- привело к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях клиентов, распоряжениях участников платежной системы, распоряжениях клирингового центра.

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.97 Оператор платежной системы определяет требования к порядку, форме и срокам информирования оператора платежной системы, операторов по переводу денежных средств и операторов услуг платежной инфраструктуры о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПС	PCI DSS
П.98 Информирование оператора платежной системы о выявленных операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры, привлекаемыми для оказания услуг платежной инфраструктуры в платежной системе, инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, осуществляется ежемесячно	ОПДС ОУПИ	PCI DSS

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.99 Оператор платежной системы определяет требования к взаимодействию оператора платежной системы, операторов по переводу денежных средств и операторов услуг платежной инфраструктуры в случае выявления в платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПС	PCI DSS
П.100 Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанных в подпункте 2.13.1 пункта 2.13 настоящего Положения требований	ОПДС ОУПИ	PCI DSS

СЛЕДСТВИЯ

По поводу пункта 2.13.1 можно выделить главное:

- оператор платежной системы определяет требования и до того как он их определит, оператор по переводу денежных средств и оператор услуг платежной инфраструктуры, **являющиеся участниками данной платежной системы**, не смогут их выполнять, а следовательно не могут быть оценены по соответствующим требованиям оценки;
- оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение требований;
- информирование осуществляется ежемесячно;
- по видам инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, стоит ориентироваться на ***Указание №2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств***»

ИНЦИДЕНТЫ, ПОДЛЕЖАЩИЕ УВЕДОМЛЕНИЮ

- Воздействие программного кода, приводящее к нарушению штатного функционирования СВТ, результатом которого является нарушение предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств;
- Реализация воздействий на АС, ПО, СВТ, телекоммуникационное оборудование, эксплуатация которых обеспечивается оператором по переводу денежных средств, оператором услуг платежной инфраструктуры, банковским платежным агентом (субагентом), и используемых для осуществления переводов денежных средств (объекты информационной инфраструктуры), с целью создания условий невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств;
- Нарушение конфиденциальности информации, необходимой для удостоверения клиентами операторов по переводу денежных средств права распоряжения денежными средствами;
- Компрометация ключевой информации СКЗИ, используемых при осуществлении переводов денежных средств;

ИНЦИДЕНТЫ, ПОДЛЕЖАЩИЕ УВЕДОМЛЕНИЮ (ПРОДОЛЖЕНИЕ)

- Осуществление переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, вследствие нарушения конфиденциальности информации, необходимой для удостоверения клиентами операторов по переводу денежных средств права распоряжения денежными средствами или вследствие компрометации ключевой информации СКЗИ, используемых при осуществлении переводов денежных средств;
- Воздействие вредоносного кода, приводящее к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях клиентов, оформленных в рамках применяемой формы безналичных расчетов, распоряжениях участников платежной системы, распоряжениях платежного клирингового центра;
- Невозможность предоставления услуг по переводу денежных средств в платежной системе в течение трех часов и более.

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.101 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.102 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают информирование службы информационной безопасности, в случае ее наличия, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

ТРЕБОВАНИЯ ПОЛОЖЕНИЯ №382-П (ПРОДОЛЖЕНИЕ)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.103 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.104 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

СЛЕДСТВИЯ

Следствия по пункту 2.13.2

Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают классические процедуры:

- **Выявление инцидентов (организационными и техническими мерами);**
- **Информирование службы ИБ (при наличии);**
- **Реагирование;**
- **Осуществление анализа причин выявленных инцидентов.**

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.105 Оператор платежной системы обеспечивает учет и доступность для операторов по переводу денежных средств, являющихся участниками платежной системы, и операторов услуг платежной инфраструктуры, привлекаемых для оказания услуг платежной инфраструктуры в платежной системе, информации о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПС	
П.106 Оператор платежной системы обеспечивает учет и доступность для операторов по переводу денежных средств, являющихся участниками платежной системы, и операторов услуг платежной инфраструктуры, привлекаемых для оказания услуг платежной инфраструктуры в платежной системе, информации о методиках анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПС	

СЛЕДСТВИЯ

Следствия по пункту 2.13.3

Оператор платежной системы обеспечивает для участников своей ПС (!!!!) классические процедуры информирования:

- **о выявленных инцидентах;**
- **о методиках анализа и реагирования.**

РЯД АНАЛОГИЧНЫХ ТРЕБОВАНИЙ СТО БР ИББС-1.0

8.2.2. **Служба ИБ** (уполномоченное лицо) должна быть наделена следующими минимальными полномочиями:

…

- участвовать в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД, например, нарушивших требования инструкций, руководств и т. п. по обеспечению ИБ организации БС РФ;

8.10.1. В организации БС РФ должны быть документы, регламентирующие **процедуры обработки инцидентов**, включающие:

- процедуры обнаружения инцидентов ИБ;
- процедуры информирования об инцидентах;
- процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ;
- процедуры реагирования на инцидент;
- процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости с участием внешних экспертов в области ИБ).

8.10.2. В организации БС РФ рекомендуется сформировать и поддерживать в актуальном состоянии **централизованную базу данных инцидентов ИБ**. Должны быть документально определены процедуры по хранению информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ.

РЯД АНАЛОГИЧНЫХ ТРЕБОВАНИЙ СТО БР ИББС-1.0 (ПРОДОЛЖЕНИЕ)

8.10.3. Должны быть документально определены порядки действий работников организации БС РФ при обнаружении **нетипичных событий, связанных с ИБ,** и информировании о данных событиях. Работники организации должны быть осведомлены об указанных порядках.

8.10.4. **Процедуры расследования инцидентов ИБ** должны учитывать действующее законодательство Российской Федерации, положения нормативных актов Банка России, а также внутренних документов организации БС РФ в области ИБ.

8.10.5. В организациях БС РФ должны приниматься и выполняться документально оформленные **решения** по всем выявленным **инцидентам ИБ.**

8.10.6. В организации БС РФ должны быть документально **определены роли** по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ и назначены ответственные за выполнение указанных ролей.

ОТДЕЛЬНЫЕ ТРЕБОВАНИЯ И ПРОВЕРОЧНЫЕ ПРОЦЕДУРЫ PCI DSS В ЧАСТИ ИНЦИДЕНТОВ

Требование PCI DSS	Проверочные процедуры
12.5.3 Разработка, документирование и распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций.	**12.5.3** Убедиться в том, что определена ответственность за разработку, документирование и распространение процедур реагирования на инциденты и процедур эскалации.
12.9 Должен быть внедрен план реагирования на инциденты. Компания должна быть готова немедленно отреагировать на нарушение в работе системы.	**12.9** Изучить план реагирования на инциденты, выполнить следующие проверки:
12.9.1 Следует разработать план реагирования на инциденты, применяемый в случае компрометации системы. План должен содержать, как минимум: - роли, обязанности и схемы оповещения в случае компрометации, включая, как минимум, оповещение международных платежных систем; - процедуры реагирования на определенные инциденты; - процедуры восстановления и обеспечения непрерывности бизнеса; - процессы резервного копирования данных; анализ требований законодательства об оповещении о фактах компрометации; - охват всех критичных системных компонентов; - ссылки или включение процедур реагирования на инциденты международных платежных систем.	**12.9.1.a** Убедиться, что план реагирования на инциденты включает в себя: - роли, обязанности и схемы оповещения в случае компрометации, включая, как минимум, оповещение международных платежных систем; - процедуры реагирования на определенные инциденты; - процедуры восстановления и обеспечения непрерывности бизнеса; - процессы резервного копирования данных; - анализ требований законодательства об оповещении о фактах компрометации; - охват всех критичных системных компонентов; - ссылки или включение процедур реагирования на инциденты международных платежных систем. **12.9.1.b** Изучить документацию по последнему инциденту или оповещению безопасности и убедиться в соблюдении документированного плана реагирования на инциденты и соответствующих процедур.

ОТДЕЛЬНЫЕ ТРЕБОВАНИЯ И ПРОВЕРОЧНЫЕ ПРОЦЕДУРЫ PCI DSS В ЧАСТИ ИНЦИДЕНТОВ (ПРОДОЛЖЕНИЕ)

Требование PCI DSS	Проверочные процедуры
12.9.2 План должен тестироваться не реже одного раза в год.	**12.9.2** Убедиться в том, что план реагирования на инциденты тестируется не реже одного раза в год.
12.9.5 План должен включать в себя процедуры реагирования на сигналы тревоги систем обнаружения и предупреждения вторжений, а также систем мониторинга целостности файлов.	**12.9.5** Убедиться в том, что план реагирования на инциденты включает в себя процедуры реагирования на сигналы тревоги систем безопасности, в том числе обнаружение неавторизованных беспроводных точек доступа.
12.9.6 Должен быть разработан процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.	**12.9.6** Убедиться в том, что налажен процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.
A.1.4 Убедиться в наличии процессов, позволяющих провести расследование инцидентов каждого клиента.	**A.1.4** Убедиться в наличии у хостинг-провайдера политик, описывающих правила проведения расследования в случае компрометации данных клиентов.

ОБЩИЙ ПОДХОД

Структурному подходу к менеджменту инцидентов ИБ призван послужить стандарт ГОСТ Р ИСО/МЭК ТО 18044. При этом отметим, что ГОСТ Р ИСО/МЭК ТО 18044 2007 содержит аутентичный текст ISO/IEC TR 18044:2004, но сейчас вышел заменяющий его ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management.

Однако с точки зрения охвата лучшего опыта и практики организации и реализации работ рекомендации ГОСТ Р ИСО/МЭК ТО 18044 устарели. Заменивший ISO/IEC TR 18044 международный стандарт ISO/IEC 27035, принятый в 2011 году, в предельно лаконичном виде определяет, что должно быть сделано и почему.

Положения ISO/IEC 27035 тесно взаимосвязаны с соответствующими международными стандартами 27-го комплекса, в первую очередь с ISO/IEC 27001, дополняя их специфичными материалами, касающимися организации и реализации задач по менеджменту инцидентов ИБ.

ИНФОРМАЦИОННО-СПРАВОЧНАЯ БАЗА

Для поддержки практических работ в ISO/IEC 27035 включены следующие информационно-справочные приложения, занимающие практически половину всего объема документа из более чем 100 страниц:

- **примерный подход к классификации и категоризации событий и инцидентов информационной безопасности;**
- **примеры образцов инцидентов информационной безопасности и их причин;**
- **примеры электронных форм и отчетов о событиях, инцидентах и недостатках информационной безопасности;**
- **таблица перекрестных ссылок ИСО/МЭК 27001/27002 и ИСО/МЭК 27035;**
- **правовые и нормативные аспекты.**

ПРАВОВАЯ ФУНКЦИЯ МЕНЕДЖМЕНТА ИНЦИДЕНТОВ В НПС

Правовые и нормативные вопросы в ISO/IEC 27035 рассмотрены в самом общем плане, т.к. законодательство во многих странах имеет фундаментальные различия. Применительно к субъектам НПС в последние годы наработан ряд практик, нашедших отражение в соответствующих документах. В их числе можно выделить:

- **документ АРБ и партнерства НПС: «Методические Рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента»**
- **рекомендации частной компании – Group-IB – участвующей в расследованиях компьютерных преступлений, осуществляемых по линии Управления «К» МВД, нашедших, например, отражение в документе: Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания.**

Несмотря на то, что оба документа «заточены» под ДБО (резонансная тематика), они применимы и для других ситуаций, где имеется связь «электронные данные – средства обработки».

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ, ПОДГОТОВЛЕННЫЕ АРБ И ПАРТНЕРСТВОМ НПС

К исх. А-02/1А-424, НПС-02/1-89
от 20.07.2012

Утверждены
Рабочей группой Ассоциации российских банков
и НП «Национальный платежный совет»
по предотвращению мошенничества в платежных системах
(Протокол № 1 от 19 июля 2012 г.)

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента

Настоящие рекомендации разработаны Рабочей группой Ассоциации российских банков и НП «Национальный платежный совет» по предотвращению мошенничества в платежных системах (далее – Рабочая группа) с учетом Письма Бюро

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ, ПОДГОТОВЛЕННЫЕ АРБ И ПАРТНЕРСТВОМ НПС (ПРОДОЛЖЕНИЕ)

Методические рекомендации, подготовленные АРБ и партнерством НПС, отражают практику инициирования и участия в расследованиях организаций БС РФ по фактам хищений денежных средств со счетов клиентов: физических и юридических лиц.

Документ содержит ряд типовых форм, предназначенных для использования клиентами и банками на тех или иных фазах расследований.

В силу достаточной важности данной темы, а также учитывая практический характер данных рекомендаций, в составе материалов курса содержится полный текст документа в версии, направленной в Банк России, для рассмотрения и согласования и придания ему нормативной силы для взаимоотношений участников рынка и государственных организаций.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ, ПОДГОТОВЛЕННЫЕ АРБ И ПАРТНЕРСТВОМ НПС (ПРОДОЛЖЕНИЕ)

Председателю
Центрального банка
Российской Федерации
Игнатьеву С.М.

О применении рекомендаций о действиях в связи с совершением мошенничества в системах ДБО

Уважаемый Сергей Михайлович!

Совместной Рабочей группой Ассоциации российских банков (АРБ) и Некоммерческого партнерства «Национальный платежный совет» (НП «НПС») по предотвращению мошенничества в платежных системах (далее – Рабочая группа) при участии представителей Департамента регулирования расчетов Банка России с учетом письма Бюро специальных технических мероприятий МВД России (далее – БСТМ МВД России) от 17 января 2012 г. № 10/257 разработаны «Методические рекомендации о необходимых действиях в связи с совершением хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента» (далее – Рекомендации) (прилагаются).

Рекомендации разработаны Рабочей группой с целью разъяснения порядка действий в связи с совершением хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства (персональный компьютер, iPad, ноутбук и т.п.) клиента (далее – ДБО).

В целях оперативного принятия процессуальных решений по фактам совершения хищения денежных средств в системах ДБО кредитными организациями и операторами платежных систем Рекомендации содержат порядок сбора и хранения необходимой доказательной базы по фактам хищений, систему сбора и регулярного обновления контактной информации для оперативной связи с ответственными сотрудниками банков, а также рекомендации о порядке действий клиента (пострадавшего), банка плательщика и банка получателя, направленных на предотвращение мошенничества в системах ДБО и порядке их действий в случае выявления хищения денежных средств в системах ДБО. В Рекомендациях также содержатся примерные формы документов, подлежащих направлению участниками правоотношений в банки и правоохранительные органы в случае несанкционированного списания денежных средств со счета клиента.

Принимая во внимание важность оперативного решения проблем, связанных с совершением мошеннических действий в системах ДБО, АРБ и НП «НПС» просят Вас рассмотреть вопрос об издании адресованного кредитным организациям совместного документа (проект прилагается), подписанного руководством Банка России, АРБ и НП «НПС» и согласованного с БСТМ МВД России, ФСБ России и ФСТЭК России.

Приложение на 39 листах:

1. Проект совместного письма Банка России, АРБ и НП «НПС» о применении кредитными организациями и операторами платежных систем «Методических рекомендаций о необходимых действиях в связи с совершением хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента» на 2 листах;

2. «Методические рекомендации о необходимых действиях в связи с совершением хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента» на 37 листе.

С уважением,

Президент	**Президент**
Ассоциации российских банков	**Некоммерческого партнерства**
	«Национальный платежный совет»
Г.А.Тосунян	**А.В.Емелин**
Исх. № А-02/1А-424	Исх. № НПС-02/1-89
от 20.07.2012	от 20.07.2012
Исп. Т.Н.Аитов	Исп. Н.В.Крючкова
тел. (495) 691-80-98	тел. (499) 678-25-62

ЧАСТНАЯ МЕТОДИКА

ИНСТРУКЦИЯ

по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания

Документ подготовлен компанией «Группа информационной безопасности» (Group-IB)

Итого

По группе требований 10. Выявление и реагирование на инциденты необходимо разработать :

- **Частная политика по инцидентам ИБ**
- **Регламент управления инцидентами ИБ (выявление, реагирование, информирование оператора ПС, анализ причин)**
- **Должностные инструкции**

Оператору ПС:

- **Регламент управления инцидентами ИБ (учет и доступность для участников ПС, методиках анализа и реагирования на инциденты)**

При наличии SIEM:

- **Регламент работы с SIEM**
- **Инструкции для администраторов и пользователей**

Итого

Рекомендуется учесть:

- **ГОСТ Р ИСО/МЭК ТО 18044**
- **ISO/IEC 27035**
- **СТО БР ИББС- 1.0 (управление инцидентами ИБ)**
- **Методические Рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента**
- **Рекомендации Group-IB**
- **Драфт РС по инцидентам СТО БР ИББС**

9. ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

ОСВЕДОМЛЕННОСТЬ

- **Осведомленность – частный случай обучения**
- **Цель материалов по осведомлению – привлечение внимания персонала к проблемам безопасности**
- **Материалы по осведомлению предназначены для того, чтобы руководители и персонал организации могли распознавать проблемы информационной безопасности и правильно реагировать на них**

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.93 Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.94 Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников в области обеспечения защиты информации по порядку использования технических средств защиты информации	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0

В требованиях 382-П везде фигурирует **только осведомленность**, что исходя из предметов получаемого знания не совсем верно. Например, в СТО БР ИББС-1.0 при получении новой роли должно быть организовано **обучение** или инструктаж.

Требования Положения №382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.95 Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.96 Оператор по переводу денежных средств обеспечивает доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению	ОПДС	

Требования Положения № 382-П и СТО БР ИББС 1.0 (общность и различия)

8.9.1. Должна быть организована документально оформленная и утвержденная руководством работа с персоналом организации БС РФ в направлении повышения осведомленности и обучения в области ИБ.....

8.9.2. В планах обучения и повышения осведомленности должны быть установлены требования к периодичности ....

8.9.3. Программы обучения и повышения осведомленности должны включать информацию:

– ....;

– **по применяемым в организации БС РФ защитным мерам**;

– **по правильному использованию защитных мер в соответствии с внутренними документами организации БС РФ**;

– .....

8.9.4. В организации БС РФ должен быть определен перечень документов, являющихся свидетельством выполнения программ обучения и повышения осведомленности в области ИБ.....

8.9.5. **Для работника, получившего новую роль, должно быть организовано обучение или инструктаж в области ИБ, соответствующее полученной роли**.

8.9.6. В организации БС РФ должны быть документально определены роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ .....

АНАЛОГИЧНЫЕ ТРЕБОВАНИЯ PCI DSS

Требование 12: Разработать и поддерживать политику информационной безопасности для всего персонала организации

Строгая политика безопасности задает атмосферу безопасности для всей компании и информирует персонал организации о том, что от них требуется. Все сотрудники должны быть осведомлены о критичности данных и своих обязанностях по их защите. В контексте данного требования термином «персонал» обозначаются постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на объекте компании или так или иначе имеющие доступ к среде данных о держателях карт.

Требования

12.6 Должна быть внедрена официальная программа повышения осведомленности персонала компании о вопросах безопасности, чтобы донести до них важность обеспечения безопасности данных о держателях карт.

12.6.1 Обучение персонала организации должно проводиться при приеме их на работу, продвижении по службе, а также не реже одного раза в год.

Примечание: Методики обучения могут варьироваться в зависимости от обязанностей персонала и уровня доступа к данным о держателях карт.

12.6.2 Персонал организации должен не реже одного раза в год подтверждать свое знание и понимание политики и процедур информационной безопасности организации.

Централизованная модель управления программой повышения уровня осведомленности

Практики повышения уровня осведомленности

- проведение инструктажей
- формирование информационного фонда документов
- обеспечение средствами связи
- проведение рабочих собраний и совещаний
- обеспечение средствами наглядной агитации
- организация кабинетов обучения
- обеспечение средствами контроля и сигнализации
- оказание консультаций
- практические тренировки

План программы повышения уровня осведомленности

- персонал, ответственный за разработку программы
- затрагиваемые национальные политики и политики организации
- цели программы
- целевая аудитория
- темы занятий и обучающие материалы
- периодичность повторных занятий

Примеры общих мероприятий по программе повышения уровня осведомленности

- просмотр видеофильмов и видеороликов
- проведение демонстрационных занятий
- семинары по вопросам информационной безопасности
- дни безопасности ИТ или подобные события
- рассылка электронных писем

Итого

По группе требований 9. Повышение осведомленности в области обеспечения защиты информации необходимо разработать:

- **частная политика повышения осведомленности/обучения**
- **план повышения осведомленности/обучения**
- **программа повышения осведомленности/обучения**
- **журнал повышения осведомленности/обучения**
- Рекомендуется учесть:
- **СТО БР ИББС- 1.0 (Обучение)**
- **PCI DSS (п.12)**

7. ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЧЕСКИХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

ОСНОВНЫЕ ТЕРМИНЫ

3.27. Банковский технологический процесс: Технологический процесс, реализующий операции по изменению и (или) определению состояния активов организации банковской системы Российской Федерации, используемых при функционировании или необходимых для реализации банковских услуг.

Примечания.

1. Операции над активами организации банковской системы Российской Федерации могут выполняться

вручную или быть автоматизированными, например, с помощью автоматизированных банковских систем.

2. В зависимости от вида деятельности выделяют: банковский платежный технологический процесс, банковский информационный технологический процесс и др.

ОСНОВНЫЕ ТЕРМИНЫ

3.28. Банковский платежный технологический процесс: часть банковского технологического процесса, реализующая банковские операции над информационными активами организации банковской системы Российской Федерации, связанные с перемещением денежных средств с одного счета на другой и (или) контролем данных операций.

3.29. Банковский информационный технологический процесс: Часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования организации банковской системы Российской Федерации и не являющихся платежной информацией.

Примечания.

1. Платежная информация — информация, содержащаяся в документах, на основании которой совершаются операции, связанные с перемещением денежных средств с одного счета на другой.

2. Неплатежная информация, необходимая для функционирования организации банковской системы Российской Федерации, может включать в себя, например, данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию.

Основные термины (продолжение)

организационные меры безопасности (operational controls) - Меры безопасности информационной системы, которые, главным образом, реализуются и выполняются операторами, а не системами.

Примечание Меры безопасности — меры защиты и контрмеры.

[ГОСТ Р ИСО/МЭК ТО 19791, пункт 3.4]

организационные меры обеспечения информационной безопасности; организационные меры обеспечения ИБ - Меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

[ГОСТ Р 53114, пункт 3.6.4]

технические меры безопасности (technical controls) - Меры безопасности информационной системы, которые реализуются и выполняются самой информационной системой через механизмы, содержащиеся в аппаратных, программных или программно-аппаратных компонентах системы.

[ГОСТ Р ИСО/МЭК ТО 19791-2008, пункт 3.16]

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.71 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают учет и контроль состава установленного и (или) используемого на средствах вычислительной техники программного обеспечения	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.72 Оператор платежной системы определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств	ОПС	
П.73 Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанного в подпункте 2.10.2 пункта 2.10 настоящего Положения порядка	ОПДС ОУПИ	

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.74 Распоряжение клиента, распоряжение участника платежной системы и распоряжение платежного клирингового центра в электронном виде может быть удостоверено электронной подписью, а также в соответствии с пунктом 3 статьи 847 Гражданского кодекса Российской Федерации аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом	ОПДС БПА (БПСА) ОУПИ	

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Гражданский кодекс

Статья 847. Удостоверение права распоряжения денежными средствами, находящимися на счете

1. Права лиц, осуществляющих от имени клиента распоряжения о перечислении и выдаче средств со счета, удостоверяются клиентом путем представления банку документов, предусмотренных законом, установленными в соответствии с ним банковскими правилами и договором банковского счета.

2. Клиент может дать распоряжение банку о списании денежных средств со счета по требованию третьих лиц, в том числе связанному с исполнением клиентом своих обязательств перед этими лицами. Банк принимает эти распоряжения при условии указания в них в письменной форме необходимых данных, позволяющих при предъявлении соответствующего требования идентифицировать лицо, имеющее право на его предъявление.

3. Договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи (пункт 2 статьи 160), кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом.

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Гражданский кодекс

Статья 160. Письменная форма сделки

1. Сделка в письменной форме должна быть совершена путем составления документа, выражающего ее содержание и подписанного лицом или лицами, совершающими сделку, или должным образом уполномоченными ими лицами.

Двусторонние (многосторонние) сделки могут совершаться способами, установленными пунктами 2 и 3 статьи 434 настоящего Кодекса.

Законом, иными правовыми актами и соглашением сторон могут устанавливаться дополнительные требования, которым должна соответствовать форма сделки (совершение на бланке определенной формы, скрепление печатью и т.п.), и предусматриваться последствия несоблюдения этих требований. Если такие последствия не предусмотрены, применяются последствия несоблюдения простой письменной формы сделки (пункт 1 статьи 162).

2. Использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронной подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

(*имеются ввиду 62-ФЗ и 149-ФЗ*)

3. Если гражданин вследствие физического недостатка, болезни или …

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.7.5 При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.76 При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.77 При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают аутентификацию входных электронных сообщений	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.78 При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.79 При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают восстановление информации об остатках денежных средств на банковских счетах, информации об остатках электронных денежных средств и данных держателей платежных карт в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.80 При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчетов в платежной системе	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.81 При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации	ОПДС БПА (БПСА) ОУПИ	

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Возможные технические решения

Общая схема работы

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

Рутокен PINPad

Поддерживает работу с Рутокен ЭЦП

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

«SafeTouch» от компании «SafeTech»

На базе Vasco Digipass 920

MAC-токены (Message Authentication Code)

Назначение: формирование кода подтверждения документа в автономном, внешнем по отношению к компьютеру, устройстве.

Способы ввода информации в устройство:

- ручной (с клавиатуры);
- оптический (фотоэлементы);
- акустический;
- «проводной» (USB).

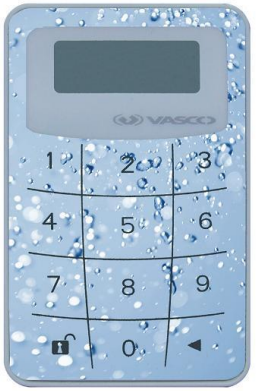
MAC-токены

Общее описание алгоритма применения:

1. В устройство вводятся ключевые реквизиты документа
2. Устройство вычисляет код подтверждения как криптографическую функцию от введенных данных и «секрета» (ключа), зашитого в устройство на этапе производства
3. Пользователь вводит код подтверждения в компьютер для передачи на сервер вместе с документом
4. Сервер верифицирует код подтверждения (симметричный алгоритм)

ЗИ с использованием взаимоувязанной совокупности организационных мер ЗИ и технических средств ЗИ, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (технологические меры ЗИ)

MAC-токены, варианты исполнения



Итого

По группе требований 7. Защита информации с использованием технологических мер защиты информации необходимо разработать:

- **Перечень разрешенного ПО**
- **Порядок использования технических и организационных мер защиты информации в платежном процессе (привязка к защите электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации)**
- **Процедуры восстановления информации об остатках денежных средств на банковских счетах, информации об остатках электронных денежных средств и данных держателей платежных карт**
- **Регламент работы с системой мониторинга транзакций**
- **Инструкции для администраторов и пользователей**
- Рекомендуется учесть:
- **СТО БР ИББС- 1.0 (банковские технологические процессы)**

6. ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СКЗИ

ОСНОВНЫЕ ТЕРМИНЫ

Электронная подпись: информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [ФЗ от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»]

Сертификат ключа проверки электронной подписи: электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. [ФЗ от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»]

Квалифицированный сертификат ключа проверки электронной подписи: сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. [ФЗ от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»]

Нормативная база применения криптосредств в РФ

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (Приказ ФСБ России № 149/54-144 от 21.02.2008)
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСБ России № 149/6/6-622 от 21.02.2008)
- Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) (Приказ ФСБ России № 66 от 9.02.2005)
- Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами (Постановление Правительства РФ № 957 от 29.12.2007)
- Приказ ФАПСИ
- Приказ ФСБ №66

Требования 382-П в части защиты информации при использовании СКЗИ

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.58 Работы по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с Федеральным законом от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи", Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года N 66 и технической документацией на СКЗИ	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.59 В случае если оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

Следствия

Из приведенного фрагмента требований вытекают следующие выводы:

1) Работы по обеспечению защиты информации с помощью СКЗИ должны проводиться в соответствии с профильными законами и нормативными актами соответствующего регулятора;

2) Какие из требований указанных законов и нормативных актов относятся к конкретным субъектам НПС зависит от деятельности субъектов;

3) Подтверждается необходимость сертификации СКЗИ;

4) Никаких «аномалий» в части требований нет, что обосновано и предсказуемо.

Федеральный закон от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи»

Принят Государственной Думой 25 марта 2011 года

Одобрен Советом Федерации 30 марта 2011 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Статья 20. Вступление в силу настоящего Федерального закона

1. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

2. Федеральный закон от 10 января 2002 года №1-ФЗ "Об электронной цифровой подписи" (Собрание законодательства Российской Федерации, 2002, №2, ст. 127) признать утратившим силу с 1 июля 2013 года.

Федеральный закон от 6 апреля 2011 г. №63-ФЗ»Об электронной подписи»

Статья 2. Основные понятия, используемые в Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

3) квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

Федеральный закон от 6 апреля 2011 г. №63-ФЗ»Об электронной подписи»

Основные понятия, используемые в Федеральном законе (продолжение)

4) владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

5) ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

8) аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

Федеральный закон от 6 апреля 2011 г. №63-ФЗ»Об электронной подписи»

Основные понятия, используемые в Федеральном законе (продолжение)

9) средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

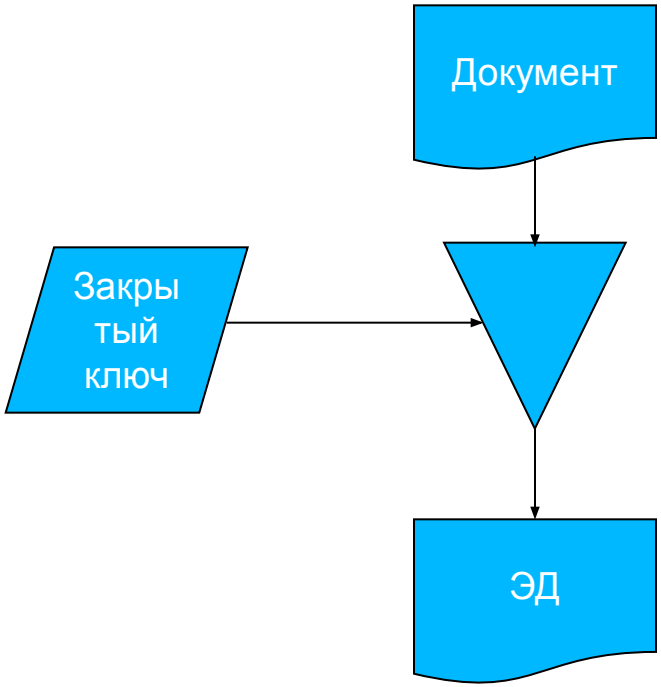
10) средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

11) участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

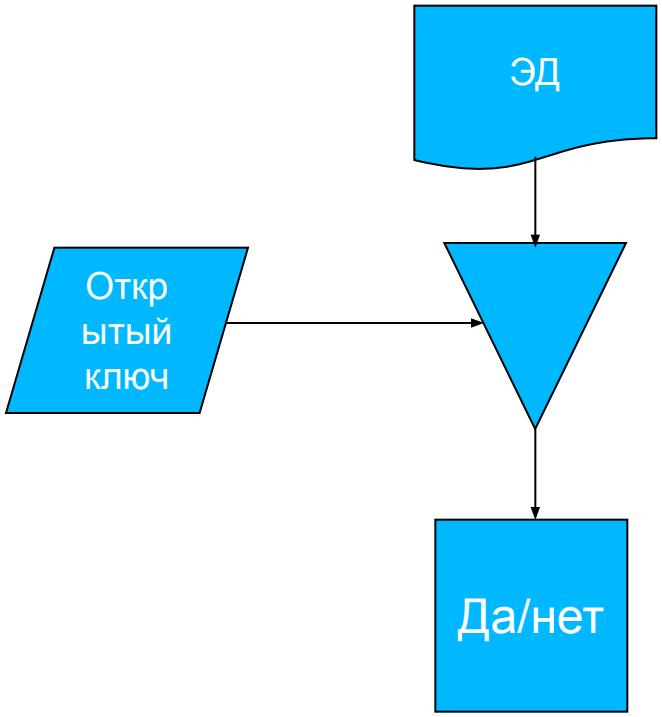
12) корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

13) информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Формирование электронной подписи



Проверка электронной подписи



Федеральный закон от 6 апреля 2011 г. №63-ФЗ»Об электронной подписи»

Статья 3. Правовое регулирование отношений в области использования электронных подписей

1. Отношения в области использования электронных подписей регулируются настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также соглашениями между участниками электронного взаимодействия. Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Виды электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, порядок их использования, а также требования об обеспечении совместимости средств электронных подписей при организации электронного взаимодействия указанных органов между собой устанавливает Правительство Российской Федерации.

Федеральный закон от 6 апреля 2011 г. №63-ФЗ»Об электронной подписи»

Статья 4. Принципы использования электронной подписи

Принципами использования электронной подписи являются:

1) право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Федеральный закон от 6 апреля 2011 г. №63-ФЗ»Об электронной подписи»

Статья 5. Виды электронных подписей

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

2. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

3. Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

……..(см. учебное пособие)

Федеральный закон от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» (основное содержание)

Статья 6. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью
Статья 7. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами
Статья 8. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи
Статья 9. Использование простой электронной подписи
Статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей
Статья 11. Признание квалифицированной электронной подписи
Статья 12. Средства электронной подписи
Статья 13. Удостоверяющий центр
Статья 14. Сертификат ключа проверки электронной подписи
Статья 15. Аккредитованный удостоверяющий центр
Статья 16. Аккредитация удостоверяющего центра
Статья 17. Квалифицированный сертификат
Статья 18. Выдача квалифицированного сертификата
Статья 19. Заключительные положения
Статья 20. Вступление в силу настоящего Федерального закона

«Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

Положение ПКЗ-2005 введено в действие приказом ФСБ РФ от 09.02.2005 № 66. Оно пришло на смену ранее действовавшего положения ПКЗ-99, приведя его в соответствие с изменившейся законодательной базой.

Структура:

1 Общие положения
2 Порядок разработки СКЗИ
3 Порядок производства СКЗИ
4 Порядок реализации (распространения) СКЗИ
5 Порядок эксплуатации СКЗИ

«Положение ПКЗ-2005»

Область действия:

«1. Положение регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

2. Шифровальные (криптографические) средства защиты информации конфиденциального характера в настоящем Положении именуются СКЗИ. К СКЗИ относятся:

а) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

….. (см. учебное пособие)

«Положение ПКЗ-2005»

Область действия:

…3. Настоящим Положением необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;

при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации (далее – государственные органы);

……. (см. учебное пособие)

«Положение ПКЗ-2005»

Область действия:

…4. Требования Положения ПКЗ 2005 носят рекомендательный характер при разработке, производстве, реализации и эксплуатации:

- средств криптографической защиты информации, доступ к которой ограничивается по решению обладателя, пользователя (потребителя) данной информации, собственника (владельца) информационных ресурсов (информационных систем) или уполномоченных ими лиц, не являющихся государственными органами или организациями, выполняющими государственные заказы;
- средств криптографической защиты информации открытых и общедоступных государственных информационных ресурсов Российской Федерации;
- средств электронной цифровой подписи, предназначаемых для использования в электронном документообороте, информация которого не относится к информации конфиденциального характера;

…….. (см. учебное пособие)

«Положение ПКЗ-2005»

Положение определяет необходимые процедуры, связанные с контролем государства за разработкой, производством, реализацией и эксплуатацией средств криптографической защиты информации конфиденциального характера. Оно определяет:

- участников каждого этапа жизненного цикла СКЗИ и их ответственность;
- последовательность действий по контролю за СКЗИ на всех этапах жизненного цикла;
- содержание документов, необходимых для контроля СКЗИ (например, ТЗ (ТТЗ), правила пользования).

Наиболее подробно регламентирована разработка СКЗИ. Описан порядок разработки (НИР, ОКР), требования к ТТЗ и его согласование, порядок организации исследований и их экспертизы.

«Положение ПКЗ-2005»

По поводу использования криптоалгоритмов:

«27. При разработке СКЗИ рекомендуется использовать криптографические алгоритмы, утвержденные в качестве национальных стандартов или определенные перечнями, утверждаемыми в порядке, установленном Постановлением Правительства Российской Федерации от 23 сентября 2002 года N 691) »

В РФ в настоящее время действуют следующие стандарты на криптографическую технику:

- ГОСТ 28147–89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
- ГОСТ Р 34.10–2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
- ГОСТ Р 34.11–94 Информационная технология. Криптографическая защита информации. Функция хэширования.
- ГОСТ Р ИСО/МЭК 10116-93 Информационная технология. Режимы работы для алгоритма n-разрядного блочного шифрования.

«Положение ПКЗ-2005»

Порядок эксплуатации СКЗИ

46. СКЗИ эксплуатируются в соответствии с правилами пользования ими. Все изменения условий использования СКЗИ, указанных в правилах пользования ими, должны согласовываться с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

В случае планирования размещения СКЗИ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, технические средства, входящие в состав СКЗИ, должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации.

47. СКЗИ, находящиеся в эксплуатации, должны подвергаться контрольным тематическим исследованиям, конкретные сроки проведения которых определяются заказчиком СКЗИ по согласованию с разработчиком СКЗИ, специализированной организацией и ФСБ России.

……. (см. учебное пособие)

«Положение ПКЗ-2005»

Порядок эксплуатации СКЗИ

50. Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, а также условий производства ключевых документов, осуществляется в соответствии с требованиями Федерального закона от 8 августа 2001 года N 134-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)".

51. Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

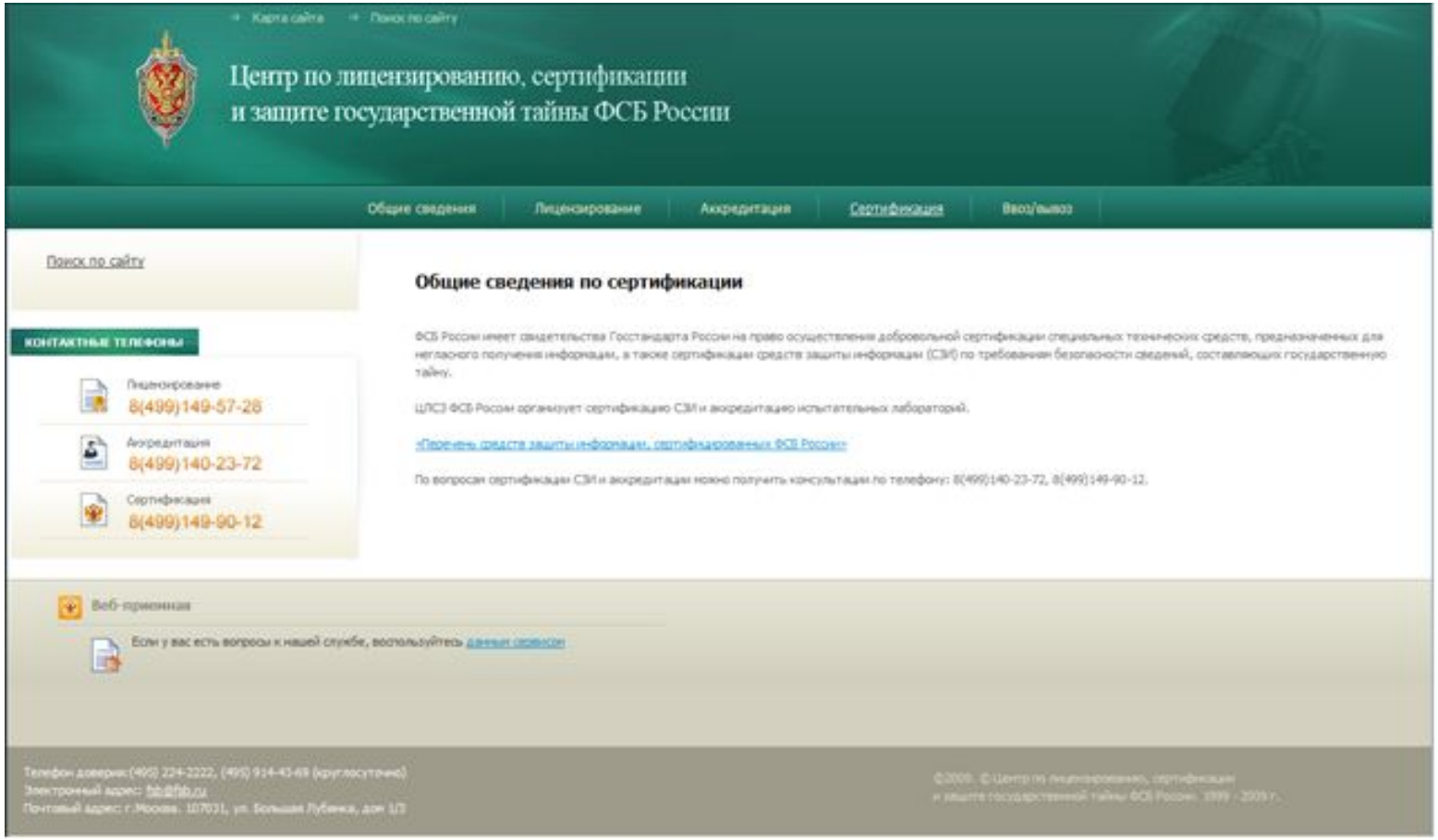
- обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
- собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
- ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

….. (см. учебное пособие)

Ссылки

Реестр УЦ и ПО ЭЦП, сертифицированных ФСБ:

http://clsz.fsb.ru/certification.htm



Выписка из перечня средств защиты информации, сертифицированных ФСБ России

Выписка из перечня средств защиты информации, сертифицированных ФСБ России
(по состоянию на 20 сентября 2012 года)

Рег. номер сертификата соответствия	Срок действия сертификата соответствия	Условное наименование (индекс)	Выполняемая функция	Изготовитель
СФ/СЗИ-0001	18.08.2011 01.07.2016	Техническое средство защиты информации от перехвата электромагнитных сигналов «Программно-аппаратный комплекс защиты объектов информационных технологий от разведки ПЭМИ «ЛГШ-504»	соответствует требованиям ФСБ России к программно-аппаратным комплексам средств активной защиты оборудования информационных технологий от разведки побочных электромагнитных излучений и наводок и может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну, при условии выполнения требований руководства по эксплуатации ДИФШ.468781.035РЭ и рекомендаций по размещению СЗИ на объекте электронной вычислительной техники	Заявитель ООО «Ленспецпроизводство», 190000, Санкт-Петербург, пер. Гривцова, д. 1/64 Литер А
СФ/СЗИ-0002	19.08.2011 19.08.2016	Техническое средство в защищенном исполнении «Аппарат телефонный специальный СТА-2ПМТд»	соответствует требованиям ФСБ России по защите информации от утечки по техническим каналам при эксплуатации аналоговых телефонных аппаратов, предназначенных для эксплуатации в выделенных помещениях I, II и III категории органов государственной власти Российской Федерации и может использоваться для обработки информации, содержащей сведения, составляющие государственную тайну, при условии выполнения требований руководства по эксплуатации ДКИС.468626.009 и предписания на эксплуатацию	Заявитель ОАО «Псковский завод Автоматических телефонных станций - Т», 180004, г. Псков, ул. Яна Фабрициуса д. 10

Требования 382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.60 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые допускают встраивание СКЗИ в технологические процессы осуществления переводов денежных средств, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.61 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

Требования 382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.62 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые поддерживают непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

Требования 382-П (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.63 В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления переводов денежных средств	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.64 В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок эксплуатации СКЗИ	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.65 В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

Защита информации при использовании СКЗИ

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.66 В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.67 В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок снятия с эксплуатации СКЗИ	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.68 В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок управления ключевой системой	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.69 В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

Требования 382-П (продолжение)

Требования основной части 382-П	Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
2.9.4. Криптографические ключи изготавливаются клиентом (самостоятельно), оператором услуг платежной инфраструктуры и (или) оператором по переводу денежных средств. Безопасность процессов изготовления криптографических ключей СКЗИ обеспечивается комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.	-	Клиент ОПДС/ОУПИ	СТО БР ИББС-1.0
2.9.5. Оператор платежной системы определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации.	П.70 Оператор платежной системы определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации	ОПС	СТО БР ИББС-1.0

«Аналогичные требования СТО БР ИББС-1.0»

7.7. Общие требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации

7.7.1. Средства криптографической защиты информации, или шифровальные (криптографические) средства (далее – СКЗИ), предназначены для защиты информации при ее обработке, хранении и передаче по каналам связи.

Необходимость использования СКЗИ определяется организацией БС РФ самостоятельно, если иное не предусмотрено законодательством РФ.

Применение СКЗИ в организации БС РФ должно проводиться в соответствии с моделью угроз ИБ и моделью нарушителя ИБ, принятыми организацией БС РФ. Рекомендуется утвердить частную политику ИБ, касающуюся применения СКЗИ в организации БС РФ.

СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2.

Работы по обеспечению с помощью СКЗИ безопасности информации проводятся в соответствии с действующими в настоящее время нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России.

«Аналогичные требования СТО БР ИББС-1.0» (продолжение)

7.7.2. Для обеспечения безопасности необходимо использовать СКЗИ, которые:

допускают встраивание в технологические процессы обработки электронных сообщений, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;

сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России.

7.7.3. Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ должны осуществляться в соответствии с эксплуатационной и технической документацией к этим средствам.

7.7.4. При применении СКЗИ должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющую собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

7.7.5. ИБ процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

«Аналогичные требования СТО БР ИББС-1.0» (продолжение)

7.7.6. Для повышения уровня безопасности при эксплуатации СКЗИ и их ключевых систем рекомендуется реализовать процедуры мониторинга, регистрирующего все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и все инциденты ИБ.

7.7.7. Порядок применения СКЗИ определяется руководством организации БС РФ на основании указанных выше в данном разделе документов и должен включать:

порядок ввода в действие, включая процедуры встраивания СКЗИ в АБС;

порядок эксплуатации;

порядок восстановления работоспособности в аварийных случаях;

порядок внесения изменений;

порядок снятия с эксплуатации;

порядок управления ключевой системой;

порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей.

7.7.8. Криптографические ключи могут изготавливаться организациями БС РФ и (или) клиентом организации БС РФ самостоятельно. Отношения, возникающие между организациями БС РФ и их клиентами, регулируются заключаемыми договорами.

Итого

По группе требований 6. Защита информации с использованием СКЗИ необходимо разработать:

- **Частная политика использования СКЗИ**
- **Регламенты и процедуры управления ключевой информацией**
- **Документация под лицензии ФСБ**
- **Журнал СКЗИ**

Для Оператора ПС:

- **Правила ПС (в части требований по использованию СКЗИ)**

Рекомендуется учесть:

- **СТО БР ИББС- 1.0 (в части требований по использованию СКЗИ)**
- **ПКЗ-2005**

5. ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ

ОСНОВНЫЕ ТЕРМИНЫ

Информационно-телекоммуникационная сеть: Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. [ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 г № 149-ФЗ]

Сеть связи: Технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи. [ФЗ “О связи” от 7 июля 2003 г. № 126-ФЗ]

Управление сетью связи: Совокупность организационно-технических мероприятий, направленных на обеспечение функционирования сети связи, в том числе регулирование трафика. [ФЗ “О связи” от 7 июля 2003 г. № 126-ФЗ]

Корпоративная информационная система: информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц. [ФЗ от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»]

ОСНОВНЫЕ ТЕРМИНЫ

Информационная система общего пользования: информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано. [ФЗ от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»]

Сетевая атака: Действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы.

Примечание - Сетевой протокол — совокупность семантических и синтаксических правил, определяющих взаимодействие программ управления сетью, находящейся в одной ЭВМ, с одноименными программами, находящимися в другой ЭВМ. [ГОСТ Р 53114-2008, пункт 3.3.7]

Сеть (network): Совокупность систем связи и систем обработки информации, которая может использоваться несколькими пользователями. [ГОСТ Р ИСО/ТО 13569-2007, пункт 3.48]

Сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими

Гарантии по обеспечению ИБ при использовании сети Интернет никаким органом не предоставляются.

Требования 382-П в части защиты информации при использовании Интернет

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.52 При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения доступа к содержанию защищаемой информации, передаваемой по сети Интернет	ОПДС БПА (БПСА) ОУПИ	
П.53 При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием сети Интернет	ОПДС БПА (БПСА) ОУПИ	

Требования 382-П в части защиты информации при использовании Интернет (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.54 При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения	ОПДС БПА (БПСА) ОУПИ	
П.55 При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают снижение тяжести последствий от воздействий на объекты информационной инфраструктуры с целью создания условий для невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств	ОПДС БПА (БПСА) ОУПИ	

Требования 382-П в части защиты информации при использовании Интернет (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.56 При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет	ОПДС БПА (БПСА) ОУПИ	
П.57 Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от несанкционированного доступа путем использования ложных(фальсифицированных) ресурсов сети Интернет	ОПДС	

КОММЕНТАРИИ

Каждый из дефисов требований подпункта 2.8.1 несет определённую смысловую нагрузку.

Первый дефис может означать, в том числе, использование безопасных протоколов передачи данных транспортного и прикладного уровней (SSL/TLS, HTTS и т.п.), а также использования средств организации VPN и иных технологий обеспечения конфиденциальности связи.

Второй дефис может означать, в том числе, соответствующую многоуровневую эшелонированную защиту периметра при использовании сети Интернет.

Третий дефис требует регулярного анализа уязвимостей, что может быть организовано различными методами. От поиска известных уязвимостей имеющимися на рынке сканерами (чаще используется для общесистемного ПО и типовых продуктов), до специализированного анализа в соответствующих центрах.

Четвертый дефис требует наличия резервных центров или альтернативных каналов обслуживания клиентов или иных решений реагирования на атаки типа DDoS.

Пятый дефис определяет необходимость наличия межсетевых экранов на границе с сетью Интернет.

Требований подпункта 2.8.2 явно адресованы «фишинговым» атакам, основанным на введении в заблуждение пользователей услуг путем их перенаправления на фальшивые ресурсы и последующего получения их чувствительных данных.

Аналогичные требования из PCI DSS

Просканированы должны быть все внешние (доступные из Интернета) IP-адреса, согласно документу Процедуры сканирования PCI DSS.

Все системы должны быть защищены от неавторизованного доступа из сети Интернет, будь то системы электронной коммерции, удаленный доступ сотрудников, доступ к корпоративной почте или выделенные соединения.

Зачастую кажущиеся малозначимыми каналы связи с внешней средой могут представлять собой незащищенные пути доступа к ключевым системам. Межсетевые экраны – основные механизмы обеспечения безопасности любой компьютерной сети.

1.1 Должны быть разработаны стандарты конфигурации межсетевых экранов и маршрутизаторов, которые должны включать в себя:

…

1.1.3 Требования к межсетевому экранированию каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью компании.

Аналогичные требования из PCI DSS (продолжение)

1.3 Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом среды данных о держателях карт.

1.3.1 Необходимо внедрить DMZ, чтобы ограничить входящий и исходящий трафик только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным сервисам, протоколам и портам.

1.3.2 Необходимо ограничить входящие Интернет-соединения только адресами, находящимися в DMZ.

1.3.3 Должны быть запрещены любые прямые входящие или исходящие соединения между сетью Интернет и средой данных о держателях карт.

1.3.4 Необходимо запретить соединения с внутренними адресами от источника из сети Интернет к адресам, расположенным в DMZ.

1.3.5 Необходимо запретить неавторизованный исходящий трафик из среды данных о держателях карт в сеть Интернет.

1.3.6 Необходимо включить динамическую пакетную фильтрацию с запоминанием состояния (разрешение прохождения пакетов только для установленных соединений).

Аналогичные требования из PCI DSS (продолжение)

1.3.7 Необходимо размещать системные компоненты (например, базы данных), в которых хранятся данные о держателях карт, во внутреннем сегменте сети, отделенном от DMZ и иных недоверенных сетей.

1.3.8 Должно быть запрещено раскрытие частных IP-адресов и данных о маршрутах третьим сторонам, не имеющим авторизованного доступа.

Примечание: правила сокрытия IP-адресации могут включать (но не ограничиваются):

- технология NAT;
- расположение серверов, содержащих данные о держателях карт за прокси-серверами/межсетевыми экранами или кэшами содержимого;
- удаление или фильтрация объявлений маршрутов для частных сетей, требующих зарегистрированной адресации;
- внутреннее использование адресного пространства RFC1918 вместо зарегистрированных адресов.

1.4 Должны быть установлены персональные межсетевые экраны на все мобильные и принадлежащие сотрудникам компьютеры (например, ноутбуки), имеющие прямой доступ в сеть Интернет и используемые для доступа к сети организации.

Итого

По группе требований 5. Защита информации при использовании сети Интернет необходимо разработать:

- **Частная политика использования сети Интернет**
- **Регламент работы с сетью Интернет (предоставления доступа, использование технических средств, на основе заявок)**
- **Инструкции администраторов СЗИ и СКЗИ**
- **Памятка для сотрудника по работе с Интернет**

Рекомендуется учесть:

- **СТО БР ИББС- 1.0 (работа с сетью Интернет)**

4. ЗАЩИТА ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО КОДА

ОСНОВНЫЕ ТЕРМИНЫ

Стандартизированных терминов из области антивирусной защиты не много. Причиной тому является не столь охотное участие производителей данных средств в формализации своих продуктов.

Ниже приведённые термины сформулированы преимущественно потребителями таких средств для использования данных понятий в своей производственной деятельности.

(Компьютерный) вирус: Вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы [ГОСТ Р 51275-2006, пункт 3.10]

(Компьютерный) вирус (en Computer virus): Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

Примечание - дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению [Р 50.1.056-2005, статья 3.2.13]

ОБЩИЙ КОММЕНТАРИЙ

Положение № 382-П включает не столь внушительную, но чрезвычайно важную группу требований по защите от вредоносных программ (на западный манер именуются как «вредоносный код» - «malicious code», в то время как в том же PCI DSS во второй его редакции используется понятие «Malicious software», включающее вирусы, черви и трояны (viruses, worms, and Trojans)).

Вредоносные программы являются повседневной головной болью участников платежных технологий (как поставщиков услуг, так и их пользователей). Фактически налажена криминальная индустрия торговли уязвимостями общесистемного и прикладного программного обеспечения, под которые разрабатываются крайне результативные для злоумышленников стратегии нападений с использованием вредоносных программ. В последние годы это также затронуло и веб-сайты поставщиков платежных услуг, через *перехваты управления на ложные сайты или веб-инъекции страниц организаций*.

НОВЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ ФСТЭК РОССИИ

Об утверждении Требований к средствам антивирусной защиты от 30 июля 2012 г. № 240/24/3095

Требования к средствам антивирусной защиты применяются к программным средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом.

Для дифференциации требований к функциям безопасности средств антивирусной защиты установлено шесть классов защиты средств антивирусной защиты. Самый низкий класс – шестой, самый высокий – первый.

Средства антивирусной защиты, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов.

Средства антивирусной защиты, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса.

Средства антивирусной защиты, соответствующие 4 классу защиты, применяются в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса.

Средства антивирусной защиты, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

ТИПЫ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

тип «А» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для **централизованного администрирования** средствами антивирусной защиты, установленными на компонентах информационных систем (серверах, автоматизированных рабочих местах);

тип «Б» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на **серверах** информационных систем;

тип «В» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на **автоматизированных рабочих местах** информационных систем;

тип «Г» – средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения **на автономных автоматизированных рабочих местах**.

Средства антивирусной защиты типа «А» не применяются в информационных системах самостоятельно и предназначены для использования только совместно со средствами антивирусной защиты типов «Б» и (или) «В».

Защита информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.40 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают использование технических средств защиты информации от воздействия вредоносного кода на средствах вычислительной техники, включая банкоматы и платежные терминалы, при наличии технической возможности	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-10
П.41 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регулярное обновление версий технических средств защиты информации от воздействия вредоносного кода и баз данных, используемых в работе технических средств защиты информации от воздействия вредоносного кода и содержащих описание вредоносных кодов и способы их обезвреживания	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-10
П.42 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают функционирование технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме, при наличии технической возможности	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-10

КОММЕНТАРИЙ

Подпункт требований 2.7.1 определяет технический и организационный контекст применения антивирусных средств.

Смысл которого следующий: антивирусные средства должны надлежащим образом обслуживаться для того, чтобы оставаться эффективными.

Именно это и есть содержание 3-х требований по проверке.

Защита информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.43 Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода	ОПДС	
П.44 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении переводов денежных средств, при наличии технической возможности	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-10

КОММЕНТАРИЙ

Для проверки соответствия требованиям подпункта 2.7.2 предусмотрено одно требование (43) Приложения 2 к Положению № 382-П второй категории проверки (наличие или отсутствие документа).

Таким документом и являются рекомендации для клиентов по защите информации от воздействия вредоносного кода.

Для проверки соответствия требованиям подпунктов 2.7.3 предусмотрено одно требование (44) Приложения 2 к Положению № 382-П третьей категории проверки (деятельность).

Во многих ситуация использование антивирусных средств от нескольких производителей повышает их совокупную эффективность. Каждое последующее средство антивирусной защиты повышает на несколько процентов долю выявляемых вирусных атак. Однако 100% достичь практически не возможно.

Даже эвристические методы анализа пропускаю некоторые атаки. При этом в условиях постоянно выявляемых дефектов ПО остается высоким риск успешной атаки злоумышленника при использовании им сведений об уязвимостях, на которые ещё нет реакции производителя. Если организация с большой долей вероятности будет или уже была объектом атаки, то необходимы изменения в архитектуре ИТ наряду с использованием более чем одного антивирусного средства.

Защита информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.45 При наличии технической возможности оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-10
П.46 При наличии технической возможности оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выполнение проверки на отсутствие вредоносного кода средств вычислительной техники, включая банкоматы и платежные терминалы, выполняемой после установки или изменения программного обеспечения	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-10

Комментарии

Опять же выполнение пункта 2.7.4 «При наличии технической возможности».

Для сравнения требование СТО БР ИББС-1.0:

7.5.6. Должны быть документально определены и выполняться процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка. Результаты установки, изменения программного обеспечения и антивирусной проверки должны документироваться.

Защита информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.47 В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, банковский платежный агент (субагент), оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода	ОПДС БПА (БПСА) ОПС ОУПИ	СТО БР ИББС-10
П.48 В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, банковский платежный агент (субагент), оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на устранение последствий воздействия вредоносного кода	ОПДС БПА (БПСА) ОПС ОУПИ	СТО БР ИББС-10

Защита информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.49 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор платежной системы, оператор услуг платежной инфраструктуры приостанавливают при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом	ОПДС БПА (БПСА) ОПС ОУПИ	СТО БР ИББС-10
П.50 В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают информирование оператора платежной системы	ОПДС ОУПИ	
П.51 В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор платежной системы обеспечивает информирование операторов услуг платежной инфраструктуры и участников платежной системы	ОПС	

Комментарии

Для сравнения аналогичное требование СТО БР ИББС-1.0:

7.5.7. Должны быть документально определены процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать:

- необходимые меры по отражению и устранению последствий вирусной атаки;
- порядок официального информирования руководства;
- порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки).

PCI DSS. Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение

Большинство видов вредоносного программного обеспечения **проникают в сеть через электронную почту сотрудников, сеть Интернет, съемные носители или мобильные устройства в результате использования системных уязвимостей**.

Антивирусное программное обеспечение должно быть установлено на всех подверженных воздействию вирусов системах, чтобы защитить их от вредоносного кода.

Требование PCI DSS	Проверочные процедуры
5.1 Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах).	5.1 Для нескольких системных компонентов, включая все типы операционных систем, подверженных воздействию вирусов, проверить, что используется антивирусная защита (если подходящая антивирусная технология существует).
5.1.1 Антивирусное программное обеспечение должно обеспечивать защиту от всех известных видов вредоносного программного обеспечения.	5.1.1 Для нескольких системных компонентов проверить, что антивирусное программное обеспечение обеспечивает защиту от всех известных форм вредоносного программного обеспечения, включая шпионские и рекламные программы.

PSI DSS. Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение (продолжение)

Требование PCI DSS	Проверочные процедуры
5.2 Антивирусные механизмы должны быть актуальными, постоянно включенными и должны вести журналы протоколирования событий.	5.2 Проверить, что антивирусные механизмы актуальны, постоянно включены и ведут журналы протоколирования событий, а именно: 5.2.a Изучить политику и убедиться, что она регламентирует регулярное обновление антивирусного программного обеспечения и антивирусных баз. 5.2.b Убедиться, что в установочном образе используемых систем включено автоматическое обновление и регулярное сканирование. 5.2.c Для нескольких системных компонентов, включая все типы операционных систем, подверженных воздействию вирусов, проверить, что автоматическое обновление антивирусного программного обеспечения и периодические проверки включены 5.2.d Для нескольких системных компонентов проверить, что включено протоколирование событий антивирусного программного обеспечения и журналы протоколирования сохраняются в соответствии с требованием 10.7 PCI DSS.

НОВЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ ФСТЭК РОССИИ

Об утверждении Требований к средствам антивирусной защиты от 30 июля 2012 г. № 240/24/3095

Требования к средствам антивирусной защиты применяются к программным средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом.

Для дифференциации требований к функциям безопасности средств антивирусной защиты установлено шесть классов защиты средств антивирусной защиты. Самый низкий класс – шестой, самый высокий – первый.

Средства антивирусной защиты, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов.

Средства антивирусной защиты, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса.

Средства антивирусной защиты, соответствующие 4 классу защиты, применяются в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса.

Средства антивирусной защиты, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Итого

По группе требований 4. Защита информации от воздействия вредоносного кода необходимо разработать:

- **Частная политика антивирусной защиты**
- **Регламенты и процедуры управления АВЗ**
- **Инструкция администратора и пользователя**
- **Памятка клиента**
- **Логи**

Рекомендуется учесть:

- **СТО БР ИББС- 1.0 (АВЗ)**
- **PCI DSS (п.5)**

3. ЗАЩИТА ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ДОСТУПА К ОБЪЕКТАМ ИТ-ИНФРАСТРУКТУРЫ

Отдельные термины по теме

Термин из СТО БР ИББС-1.0

Информационная инфраструктура: Система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия.

Примечание.

Информационная инфраструктура:

- включает совокупность информационных центров, банков данных и знаний, систем связи;
- обеспечивает доступ потребителей к информационным ресурсам.

Экстракт понятия из 382-П

Объекты информационной инфраструктуры - автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, эксплуатация которых обеспечивается оператором по переводу денежных средств, оператором услуг платежной инфраструктуры, банковским платежным агентом (субагентом), и используемые для осуществления переводов денежных средств.

Термин из ИСО/МЭК 12207:2008

Жизненный цикл (life cycle) - Развитие системы, продукта, услуги, проекта или иной созданной руками человека сущности от замысла до снятия с эксплуатации.

ЗИ на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.8 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	СТО БР ИББС-1.0
П.9 Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают участие службы информационной безопасности в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.10 Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0

Следствия

Из приведенного фрагмента требований вытекают следующие выводы:

1) в ТЗ на создание (модернизацию) объектов информационной инфраструктуры, используемых при осуществлении переводов денежных средств (а это неопределенный состав из **автоматизированных систем, программного обеспечения, средства вычислительной техники, телекоммуникационного оборудования**) следует включить требования к обеспечению ЗИ;

2) Служба информационной безопасности должна участвовать в разработке и согласовании технических заданий;

3) Служба информационной безопасности должна обеспечивать контроль создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий.

Т.е. какая-либо методология реализации отсутствует - по сути субъекты НПС сами определяют состав объектов инфраструктуры, обеспечивают включение требований к ним в части ЗИ, а также контроль их реализации.

При таком подходе большая вероятность, что состав объектов и требований будет минимальным.

ЗИ на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.11 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают наличие эксплуатационной документации на используемые технические средства защиты информации	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.12 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.13 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

ЗИ на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.14 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

ЗИ на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.15 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают реализацию запрета несанкционированного копирования защищаемой информации	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.16 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают защиту резервных копий защищаемой информации	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

ЗИ на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.17 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, правилами платежной системы и (или) договорами, заключенными оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором платежной системы, оператором услуг платежной инфраструктуры	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.18 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

Следствия

Из приведенных требований вытекают следующие выводы:

1) Пункты требований задают по большому счету только ряд ключевых точек (этапов ЖЦ) и некоторые требования в рамках этих этапов;

2) Состав требований не выглядит исчерпывающим;

3) Средства достижения целей (выполнения требований) не даны, даны лишь некоторые направления.

Сопоставимые требования СТО БР ИББС-1.0

7.3.2. Разработка технических заданий и приемка АБС должны осуществляться по согласованию и при участии подразделения (лиц) в организации БС РФ, ответственного за обеспечение ИБ.
7.3.3. Ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации АБС должны осуществляться под контролем подразделения (лиц) в организации, ответственного за обеспечение ИБ.
7.3.5. Разрабатываемые АБС и (или) их компоненты должны быть снабжены документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации БС РФ. Приобретаемые организацией БС РФ готовые АБС и (или) их компоненты рекомендуется снабжать указанной документацией.
Также документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты должна содержать описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки.
7.3.7. На стадии тестирования должны обеспечиваться анонимность данных и проверка адекватности разграничения доступа.
7.3.8. На стадии эксплуатации АБС должны быть документально определены и выполняться процедуры контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер. Результаты выполнения контроля должны документироваться.
7.3.11. На стадии снятия с эксплуатации должны быть документально определены и выполняться процедуры, обеспечивающие удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС и с внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами. Результаты выполнения процедур должны документироваться.

382-П / СТО БР ИББС-1.0 / PCI DSS

Сопоставимость требований 382-П и СТО БР ИББС-1.0 вполне объяснима. Этапы ЖЦ во многом совпадают для разных объектов информационной инфраструктуры. В стандарте сделан акцент на ЖЦ АБС, в 382-П неопределенный круг объектов, но в него входят и системы.

Уместно также рассмотреть описание информационной инфраструктуры на которую распространяются требования стандарта PCI DSS.

Стоит заметить, что при проведении аудита на соответствие PCI DSS описание информационной инфраструктуры лежит помимо субъекта оценки еще и на аудиторах.

При реализации же требований 382-П это ложиться целиком на субъекты НПС.

С этого и нужно начинать реализацию требований 382-П – определить активы и описать инфраструктуру.

Выписка из недавнего Письма ЦБ РФ от 6 марта 2012 г. N 08-17/950 по вопросам кредитных организаций - членов ассоциации "Россия"

4. Являются ли эмитенты и эквайреры - члены международных платежных систем операторами по переводу денежных средств, или к ним применимо другое понятие, используемое в Законе о НПС?
Все ли операции по банковским картам попадают под понятие "перевод денежных средств"?
Возможно ли рассматривать системы дистанционного банковского обслуживания (ДБО), а именно системы "Клиент-банк", "Интернет-банкинг", "Мобильный банкинг", с использованием которых клиенты кредитной организации могут передавать в кредитную организацию распоряжения о проведении операций по счетам, в качестве электронного средства платежа (корпоративного электронного средства платежа).
Исходя из пунктов 2, 12 статьи 3 Закона о НПС, оператором по переводу денежных средств является организация, осуществляющая в соответствии с законодательством Российской Федерации перевод денежных средств, то есть действия в рамках применяемых форм безналичных расчетов по предоставлению получателю денежных средств плательщика.
Учитывая изложенное, кредитные организации, являющиеся эмитентами или эквайрерами, при совершении операций с использованием банковских карт являются операторами по переводу денежных средств.
Из содержания указанных норм также следует, что операции, совершаемые с использованием банковских карт, являются операциями по переводу денежных средств, за исключением операций, предусмотренных частью 4 статьи 5 Закона о НПС.
В отношении систем дистанционного банковского обслуживания отмечаем, что, исходя из совокупности норм Закона о НПС, системы дистанционного банковского обслуживания, позволяющие составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств, являются электронными средствами платежа. При этом корпоративное электронное средство платежа является одним из видов электронных средств платежа (часть 7 статьи 10, пункт 2 части 4 статьи 12 Закона о НПС), с использованием которого клиенты - юридические лица или индивидуальные предприниматели могут совершать только переводы электронных денежных средств.

Основные термины

Криптографическое средство защиты информации - средство защиты информации, реализующее алгоритмы криптографического преобразования информации [ГОСТ Р 50922].

Защита информации от несанкционированного воздействия - защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [ГОСТ Р 50922].

защита информации от несанкционированного доступа - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

Примечание — Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо [ГОСТ Р 50922].

Терминология (продолжение)

Идентификация - действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов [Р 50.1.053].

Аутентификация - обеспечение однозначного соответствия заявленного идентификатора объекту [ГОСТ Р ИСО/МЭК ТО 13335-4].

Санкционирование доступа; авторизация - предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ [Р 50.1.056].

Требования 382-П в части защиты информации при осуществлении доступа

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.19 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают учет объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматов и платежных терминалов	ОПДС БПА (БПСА) ОУПИ	
П.20 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение некриптографических средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия	ОПДС БПА (БПСА) ОУПИ	

Следствия

Необходимо обеспечить учет объектов информационной инфраструктуры (идентификация активов).

1) Обеспечить применение некриптографических средств защиты информации от НСД).
2) Средств защиты информации от НСД могут пройти оценку соответствия.

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.21 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выполнение процедур идентификации, аутентификации, авторизации своих работников при осуществлении доступа к защищаемой информации	ОПДС БПА (БПСА) ОУПИ	
П.22 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают идентификацию, аутентификацию, авторизацию участников платежной системы при осуществлении переводов денежных средств	ОПДС БПА (БПСА) ОУПИ	

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.23 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают определение порядка использования информации, необходимой для выполнения аутентификации	ОПДС БПА (БПСА) ОУПИ	
П.24 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию действий при осуществлении доступа своих работников к защищаемой информации	ОПДС БПА (БПСА) ОУПИ	

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.25 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию действий, связанных с назначением и распределением прав доступа к защищаемой информации	ОПДС БПА (БПСА) ОУПИ	
П.26 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают выполнение процедур идентификации, аутентификации, авторизации лиц, осуществляющих доступ к программному обеспечению банкоматов и платежных терминалов	ОПДС БПА (БПСА)	

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.27 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают выполнение процедур идентификации и контроль деятельности лиц, осуществляющих техническое обслуживание банкоматов и платежных терминалов	ОПДС БПА (БПСА)	
П.28 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию действий клиентов, выполняемую с использованием программного обеспечения и автоматизированных систем, при наличии технической возможности	ОПДС БПА (БПСА)	

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.29 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию действий, связанных с назначением и распределением прав клиентов, предоставленных им в автоматизированных системах и программном обеспечении, при наличии технической возможности	ОПДС БПА (БПСА)	
П.30 При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств обеспечивает регистрацию действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов	ОПДС	

ЗАМЕЧАНИЕ

Для проверки соответствия требованиям подпункта 2.6.3 предусмотрено 10 требований (21-30) Приложения 2 к Положению № 382–П. Преимущественно первой категории проверки за исключением требования 23 – оно ориентировано на проверку наличия в организации соответствующего внутреннего документа.

Множество требований подпункта 2.6.3 по-разному распространяется на тех или иных участников НПС.

ТАКИМ ОБРАЗОМ

ОПДС, БПА (БПСА), ОУПИ при осуществлении доступа к защищаемой информации обеспечивают:

1) выполнение процедур идентификации, аутентификации, авторизации своих работников при осуществлении доступа к защищаемой информации;
2) идентификацию, аутентификацию, авторизацию участников платежной системы при осуществлении переводов денежных средств;
3) определение порядка использования информации, необходимой для выполнения аутентификации;
4) регистрацию действий при осуществлении доступа своих работников к защищаемой информации;
5) регистрацию действий клиентов, связанных с назначением и распределением прав доступа к защищаемой информации.

Таким образом (продолжение)

ОПДС, БПА (БПСА) при осуществлении доступа к защищаемой информации обеспечивают:

1) выполнение процедур идентификации, аутентификации, авторизации лиц, осуществляющих доступ к программному обеспечению банкоматов и платежных терминалов;
2) выполнение процедур идентификации и контроль деятельности лиц, осуществляющих техническое обслуживание банкоматов и платежных терминалов;
3) регистрацию действий клиентов, выполняемых с использованием программного обеспечения, входящего в состав объектов информационной инфраструктуры и используемого для осуществления переводов денежных средств (далее - программное обеспечение), и автоматизированных систем, входящих в состав объектов информационной инфраструктуры и используемых для осуществления переводов денежных средств (далее - автоматизированные системы), при наличии технической возможности;
4) регистрацию действий, связанных с назначением и распределением прав клиентов, предоставленных им в автоматизированных системах и программном обеспечении, при наличии технической возможности.

ОПДС при осуществлении доступа к защищаемой информации обеспечивает:

1) регистрацию действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов.

РЕКОМЕНДАЦИИ СТАНДАРТОВ

В части блока требований безопасности по идентификации и контроля доступа лиц сервисных и обслуживающих подразделений и организаций, а так же доступа клиентов к платежным услугам с использованием платёжных карт при осуществлении операций через банкоматы или на объектах розничной сети, в ГОСТ Р ИСО/ТО 13569 (гармонизированном международном стандарте) даются следующие рекомендации.

Для предупреждения потерь из-за перехвата личных идентификационных номеров несанкционированными лицами, с личными идентификационными номерами следует обращаться в соответствии со стандартом ИСО 9564-(1–4) или ИСО 10202-(1–8).

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.31 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета несанкционированного расширения прав доступа к защищаемой информации	ОПДС БПА (БПСА) ОУПИ	
П.32 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации	ОПДС БПА (БПСА) ОУПИ	

АНАЛОГИЧНЫЕ ПРИНЦИПЫ В ГОСТ Р ИСО/ТО 13569

Принцип необходимого знания (need to know): Концепция безопасности, ограничивающая доступ к информации и ресурсам обработки информации в объеме, необходимом для выполнения обязанностей данного лица.

Двойной контроль (dual control): Процесс использования двух или более отдельных логических объектов (обычно людей), которые действуют совместно для обеспечения защиты важных функций или информации.

П р и м е ч а н и я:

1. Оба логических объекта несут равную ответственность за обеспечение физической защиты материалов, задействованных в уязвимых операциях. Ни один человек в отдельности не может получить доступ к материалам (например, криптографическому ключу) или использовать их.

2. При ручном формировании, передачи, загрузки, хранения и извлечения ключей и сертификатов двойной контроль требует раздельного знания ключа логическими объектами.

3. Когда бы ни требовался двойной контроль, следует позаботиться о том, чтобы обеспечить независимость лиц друг от друга.

Разделенное знание (split knowledge): Разделение критичной информации на множество частей таким образом, чтобы требовалось наличие минимального числа частей, перед выполнением какого-либо действия.

П р и м е ч а н и е . Разделенное знание часто используется для осуществления двойного контроля.»

Аналогичные требования стандарта СТО БР ИББС-1.0

7.1.4. При распределении прав доступа работников и клиентов к информационным активам организации БС РФ следует руководствоваться принципами:

- "знать своего клиента";
- "знать своего служащего";
- "необходимо знать",

а также рекомендуется использовать принцип "двойное управление".

"**Знать своего клиента**" (Know your Customer): принцип, используемый регулирующими органами для выражения отношения к финансовым организациям с точки зрения знания деятельности их клиентов.

"**Знать своего служащего**" (Know your Employee): принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких, как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью.

"**Необходимо знать**" (Need to Know): принцип, ограничивающий полномочия по доступу к информации и ресурсам по обработке информации на уровне минимально необходимых для выполнения определенных обязанностей.

"**Двойное управление**" (Dual Control): принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий дублирования (алгоритмического, временного, ресурсного или иного) действий до завершения определенных транзакций.

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.33 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры принимают и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для контроля физического доступа к объектам информационной инфраструктуры (за исключением банкоматов, платежных терминалов и электронных средств платежа), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, а также доступа в здания и помещения, в которых они размещаются	ОПДС БПА (БПСА) ОУПИ	

Защита информации при осуществлении доступа к объектам информационной инфраструктуры, включая требования к защите информации от несанкционированного доступа

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.34 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры принимают и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для предотвращения физического воздействия на средства вычислительной техники и телекоммуникационное оборудование, сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа	ОПДС БПА (БПСА) ОУПИ	
П.35 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры принимают и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для регистрации доступа к банкоматам, в том числе с использованием систем видеонаблюдения	ОПДС БПА (БПСА) ОУПИ	

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.36 В случае принятия оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором услуг платежной инфраструктуры решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, указанных в подпункте 2.6.5 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение указанных организационных мер защиты информации и (или) использование указанных технических средств защиты информации	ОПДС БПА (БПСА) ОУПИ	

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Подпункт 2.6.7 сформулирован как мера реагирования на одну из самых распространённых угроз российским клиентам услуг доступа к счетам с использованием платежных карт. Причина тому банальна: тотальное использование более дешевой в эксплуатации магнитной полосы на карте, а не чипа.

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.37 Оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают контроль отсутствия размещения на платежных терминалах и банкоматах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств	ОПДС БПА (БПСА)	

КОММЕНТАРИИ

Речь в подпункте 2.6.7, по всей видимости, идет об анти-скимминговом оборудовании. Это не дешевое удовольствие.

Реализация этого требования может быть как косвенным (непрерывное видеонаблюдение с возможностью оперативного выезда на место) образом, так и непосредственной установкой специализированного устройства на карто-приемник банкомата или платежного терминала.

Другим средством противодействия этой угрозе есть запрет использования магнитной полосы. В Европе подобным образом снизили на 90% количество воровства с карточных счетов с использованием скиммеров.

Требования 382-П в части защиты информации при осуществлении доступа (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.38 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на предотвращение хищений носителей защищаемой информации	ОПДС БПА (БПСА) ОУПИ	
П.39 Оператор по переводу денежных средств обеспечивает возможность приостановления (блокирования) клиентом приема к исполнению распоряжений об осуществлении переводов денежных средств от имени указанного клиента	ОПДС	

Итого

По группе требований 3. Защита информации при осуществлении доступа к объектам ИТ-инфраструктуры необходимо разработать:

- **Частная политика доступа к ИТ-объектам (помещения, оборудование, ПО)**
- **Частная политика ЖЦ АБС**
- **Регламенты и процедуры осуществления доступа**
- **Заявки на доступ**
- **Логи**

Рекомендуется учесть:

- **СТО БР ИББС- 1.0 (доступ к объектам среды)**
- **ГОСТ Р ИСО/ТО 13569**
- **ИСО/МЭК 12207:2008**

1. ЗАЩИТА ИНФОРМАЦИИ ПРИ НАЗНАЧЕНИИ И РАСПРЕДЕЛЕНИИ РОЛЕЙ

ОСНОВНЫЕ ТЕРМИНЫ

Роль: Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

Примечания.

1. К субъектам относятся лица из числа руководителей организации, ее персонала, клиентов или инициируемые от их имени процессы по выполнению действий над объектами.

2. Объектами могут быть аппаратное средство, программное средство, программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия.

Еще одно определение роли звучит как совокупность функций субъекта (субъектов), для выполнения которых необходим совокупный (по функциям) набор полномочий. Таким образом, роль можно рассматривать как некоторую совокупность полномочий, предоставленных одному или нескольким субъектам.

Субъект: лицо из числа персонала организации (работник организации), или лицо, не являющиеся работником организации, но которому предоставляются полномочия по доступу и (или) использованию информационных активов организации.

Функция: вид работ, выполняемых или планируемых к выполнению субъектом с осуществлением доступа и (или) с использованием информационных активов организации.

Операция: отдельное действие, выполняемое или планируемое к выполнению в рамках функции над информационным активом путем использования объекта среды.

ОСНОВНЫЕ ТЕРМИНЫ

Полномочие: совокупность трех составляющих:

- **информационный актив организации (тип информационных активов);**
- **объект среды информационной инфраструктуры организации (тип объектов среды);**
- **операция, выполняемая или планируемая к выполнению над информационным активом путем использования объекта среды (типовая операция, выполняемая или планируемая к выполнению над типом информационных активов путем использования типов объектов среды).**

Перечни операций, выполняемых или планируемых к выполнению над информационными активами путем использования объектов среды определяются в зависимости от рассматриваемого объекта среды, его расположения в рамках иерархии информационной инфраструктуры организации.

Ограничение: запрет, реализующий принцип разделения полномочий и определяющий:

- **совокупность полномочий, недопустимых для включения в одну роль. Недопустимым является включение в одну роль всех полномочий, принадлежащих какому-либо ограничению;**
- **совокупность ролей, недопустимых для назначения одному субъекту. Недопустимым является назначение одному субъекту всех ролей, принадлежащих какому-либо ограничению.**

Ролевые требования имеют отношение к организационным аспектам безопасности, что дает от 80 до 90% в общий вклад в систему обеспечения информационной безопасности организации.

Положение № 382-П определяет достаточно лаконичный, но крайне важный для практики состав требований из 3-х пунктов, применяемых для защиты информации при назначении и распределении ролей лиц, связанных с осуществлением переводов денежных средств.

Защита информации при назначении и распределении функциональных обязанностей и прав лиц, связанных с осуществлением переводов денежных средств

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.1 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по осуществлению доступа к защищаемой информации	ОПДС БПА (БПСА) ОУПИ	
П.2 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по управлению криптографическими ключами	ОПДС БПА (БПСА) ОУПИ	
П.3 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по управлению криптографическими ключами	ОПДС БПА (БПСА) ОУПИ	
П.4 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию своих работников, обладающих правами по формированию электронных сообщений	ОПДС БПА (БПСА) ОУПИ	

КОММЕНТАРИИ К ПОДПУНКТУ 2.4.1

Это наиболее «тяжелый» с точки зрения реализации пункт требований из группы требований к ролям, имеющий далеко идущие последствия.

Здесь мы видим комбинированный подход из следующих основных двух подходов к идентификации ролей безопасности:

- **первый подход: идентифицируются функциональные роли персонала организации и применительно к ним устанавливаются ограничения по операциям с информационными активами или компонентами информационной инфраструктуры организации;**
- **второй подход: каждое из требований безопасности, предполагающее реализацию некоторой деятельности, идентифицируется как функция для которой выделяется соответствующая роль безопасности, которая в последующем включается в должностные обязанности персонала.**

Как мы видим, в подпункте 2.4.1 присутствуют оба подхода.

Защита информации при назначении и распределении функциональных обязанностей и прав лиц, связанных с осуществлением переводов денежных средств

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.5 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с созданием (модернизацией) объекта информационной инфраструктуры и эксплуатацией объекта информационной инфраструктуры	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0
П.6 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и эксплуатацией объекта информационной инфраструктуры в части его технического обслуживания и ремонта	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

Это давно устоявшаяся общемировая практика, что уже давно применяется в ряде российских компаний. Например, перед проведением сервисных работ на оборудовании хранилища (архива) данных компании все рабочие данные с него удаляются (перемещаются), а по завершении обслуживания возвращаются обратно.

Защита информации при назначении и распределении функциональных обязанностей и прав лиц, связанных с осуществлением переводов денежных средств

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.7 Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль и регистрацию действий лиц, которым назначены роли, определенные в подпункте 2.4.1 пункта 2.4 настоящего Положения	ОПДС БПА (БПСА) ОУПИ	СТО БР ИББС-1.0

В соответствии с данным подпунктом требований субъект НПС должен организовать достаточно мощную систему регистрации, основное назначение которой – обеспечить условия для всестороннего и глубоко разбора любой нештатной ситуации с однозначной идентификацией всех вовлеченных лиц из персонала субъекта НПС.

ОБЩИЙ КОНТЕКСТ ГРУППЫ ТРЕБОВАНИЙ П. 2.4

Группа требований, применяемых для защиты информации при назначении и распределении ролей лиц, связанных с осуществлением переводов денежных средств, предполагает наличия следующего:

- **реестра защищаемой информации;**
- **инициирования и ведения базы данных персонала, имеющего доступ к защищаемой информации (техническая и процедурная компоненты этой деятельности), роли по управлению криптографическими ключами и других лиц, оказывающих воздействие на объекты информационной инфраструктуры;**
- **внутренних регламентов по поставке и сервисному обслуживанию оборудования и систем;**
- **мощной системы регистрации действий лиц, имеющих доступ к защищаемой информации, ответственных за управление ключами, а также иных лиц, оказывающих воздействие на объекты информационной инфраструктуры.**

При реализации данной группы требований, могут быть использованы следующие общие подходы, нашедшие отражение в соответствующих стандартах.

Пример ролей в структуре организации (ГОСТ Р ИСО/ТО 13569)

Функциональные должности (не связанные с непосредственным обеспечением ИБ):

- Совет директоров
- Комитет по аудиту
- Комитет по менеджменту риска
- Правовая функция
- Должностные лица
- Управляющие делами
- Сотрудники
- Сотрудники (персонал), не относящиеся к организации

Состав типовых обязанностей в тексте учебного пособия

Должности, связанные с безопасностью:

- Руководитель службы обеспечения информационной безопасности
- Ответственный за информационную безопасность
- Администраторы обеспечения безопасности

ФУНКЦИОНАЛЬНЫЕ РОЛИ И ОПЕРАЦИИ В ОРГАНИЗАЦИИ ДЛЯ ЦЕЛЕЙ ДЛЯ УПРАВЛЕНИЯ ДОСТУПОМ

Функциональные роли:

- Администратор;
- Старший менеджер отдела 1;
- Менеджер отдела 1;
- Старший менеджер отдела 2;
- Менеджер отдела 2;
- Старший менеджер процессинга;
- Менеджер процессинга;
- Контролер процессинга;
- Регистратор входящих документов;
- Пользователь расчетной системы;
- Менеджер корпоративной информации;
- Пользователь системы делопроизводства ….
- …..

Пример

Функциональные роли и операции в организации для целей для управления доступом (продолжение)

Операции (по просмотру, добавлению, редактированию, удалению), устанавливаемые индивидуально для каждой функциональной роли:

- Сформировать ежемесячную отчётность
- Ежедневная отчётность по резервам
- Сформировать требования оплаты услуг
- Настройка контрольной функции
- Виды контроля
- Протоколы контроля
- Запуск контроля
- Закрытие форм
- Операционный день
- Контрольная процедура
- Загрузка данных
- ……..

Пример

Роли информационной безопасности в СТО БР ИББС-1.0

В состав ролей, связанных с непосредственным обеспечением информационной безопасности, включаются:

- **роли ИБ для системы информационной безопасности** (СИБ) организации;
- **роли ИБ для СМИБ** организации.

Область выделения и назначения ролей ИБ определяется как организация в целом. При этом, для организаций имеющих сеть филиалов роль ИБ может быть назначена работникам нескольких филиалов в соответствии с закрепленным в организации распределением обязанностей и ответственности.

Состав ролей ИБ для **реализации требований Положения Банка России № 382-П вытекает из 14 областей требований**, подлежащих проверке, аналогичных требованиям к СИБ и СМИБ СТО БР ИББС 1.0.

Контроль выделения и назначения ролей ИБ

Контроль выделения и назначения ролей ИБ осуществляется на основе требований раздела 9 СТО БР ИББС-1.0. Основными формами проведения контроля являются:

- **проверка со стороны службы ИБ организации**;
- **самооценка ИБ**;
- **внешний аудит ИБ**;
- **анализ функционирования СОИБ** (в том числе со стороны руководства организации).

Основными целями проведения контроля выделения и назначения ролей ИБ являются:

- **контроль полноты выделения** и назначения ролей ИБ;
- **контроль выполнения** ролей ИБ;
- **контроль соответствия** состава выделенных ролей требованиям комплекса БР ИББС.

Пример распределения функций между ролями, связанными с проведением самооценок ИБ

Функции по проведению самооценки ИБ	Роли по проведению самооценки ИБ		
	Роль ответствен-ного за самооценку ИБ	Роль руководи-теля проверяю-щей группы	Роль члена проверяю-щей группы
Анализ документов, содержащих дополнительные свидетельства самооценки ИБ.	-	-	+
Анализ необходимой документации, регламентирующей обеспечение ИБ в проверяемых подразделениях организации БС РФ для определения соответствия положений, отраженных в документации, требованиям СТО БР ИББС-1.0.	-	-	+
Взаимодействие с руководителями проверяемых подразделений для содействия самооценке ИБ.	-	+	-
…	•	•	•
Информирование проверяемых подразделений организации БС РФ о порядке рассмотрения замечаний по проведению самооценки или заключению по результатам самооценки ИБ.	-	+	-

Итого

По группе требований 1. Защита информации при назначении и распределении ролей необходимо разработать:

- **Частная политика управления ролями (распределение ролей)**
- **Матрица доступа**
- **Ролевая модель**
- **Регламенты и процедуры распределения ролей**
- **Заявки на доступ**
- **Логи**

Рекомендуется учесть:

- **СТО БР ИББС- 1.0 (роли)**
- **ГОСТ Р ИСО/ТО 13569**

8. ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ СЛУЖБЫ ИБ

ИСТОЧНИКИ ТРЕБОВАНИЙ К НАЛИЧИЮ СЛУЖБЫ

Требования к организации и функционированию службы информационной безопасности определены следующими документами:

- **ПП 584;**
- **Положением Банка России № 382-П.**

ПП 584 определены следующие требования в части службы информационной безопасности:

«4. Правила платежной системы должны предусматривать в том числе следующие требования к защите информации:

а) создание и организация функционирования структурного подразделения по защите информации (службы информационной безопасности) или назначение должностного лица (работника), ответственного за организацию защиты информации;…»

Таким образом, в ПП 584 речь идет только о субъектах НПС, подпадающих под необходимость разработки «Правил платежной системы» (операторы платежных систем), но не затрагивает явным образом иных субъектов НПС (операторов по переводу денежных средств, агентов и т.д.).

ДРУГИЕ ТРЕБОВАНИЯ ПП 584 К ПЕРСОНАЛУ

ПП 584 содержит еще одно положение в части требований к персоналу, устанавливаемое оператором платежных систем в Правилах, а именно:

«б) включение в должностные обязанности работников, участвующих в обработке информации, обязанности по выполнению требований к защите информации;..»

Опять же для иных субъектов НПС, подобных требований ПП 584 не содержит.

Положение Банка России №382-П в части службы информационной безопасности устанавливает более развернутые требования, однако в части обязательности «*..включения в должностные обязанности работников, участвующих в обработке информации, обязанности по выполнению требований к защите информации..*» аналогичных норм не устанавливает, но рассматривает подобные задачи на платформе «*определения лиц, ответственных за ……*». Ролевой принцип.

Требования Положения № 382-П к организации и функционированию службы информационной безопасности имеют более широкую сферу применения нежели подобные требования ПП 584, однако также имеют некоторые ограничения. Они не распространяются на банковских платежных агентов (субагентов), являющихся индивидуальными предпринимателями.

***Выполнение всех требований относится только к операторам по переводу денежных средств, операторов платежных систем, а также операторам услуг платежной инфраструктуры и банковским платежным агентам (субагентам), являющимся юридическими лицами*.**

ТРЕБОВАНИЯ 382-П, СУБЪЕКТЫ, ПОДОБНЫЕ ТРЕБ. В ДР. СТАНДАРТАХ

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.82 Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают формирование службы информационной безопасности, а также определяют во внутренних документах цели и задачи деятельности этой службы	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.83 Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры предоставляют полномочия и выделяют ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.84 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры назначают куратора службы информационной безопасности из состава своего органа управления и определяют его полномочия	ОПДС ОУПИ	СТО БР ИББС-1.0
П.85 Служба информационной безопасности и служба информатизации (автоматизации) не должны иметь общего куратора	ОПДС ОУПИ	СТО БР ИББС-1.0

ТРЕБОВАНИЯ 382-П, СУБЪЕКТЫ, НАЛИЧИЕ ПОДОБНЫХ ТРЕБОВАНИЙ В ДРУГИХ СТАНДАРТАХ

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.86 Оператор по переводу денежных средств, имеющий филиалы, обеспечивает формирование служб информационной безопасности в указанных филиалах, определяет для них необходимые полномочия и выделяет необходимые ресурсы	ОПДС	СТО БР ИББС-1.0
П.87 Оператор по переводу денежных средств, имеющий филиалы, обеспечивает взаимодействие и координацию работ служб информационной безопасности	ОПДС	СТО БР ИББС-1.0

Организация и функционирование службы информационной безопасности

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.88 Служба ИБ осуществляет планирование и контроль обеспечения ЗИ при осуществлении переводов денежных средств, для чего наделяется полномочиями осуществлять контроль (мониторинг) выполнения порядка обеспечения ЗИ при осуществлении переводов денежных средств	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.89 Служба ИБ осуществляет планирование и контроль обеспечения ЗИ при осуществлении переводов денежных средств, для чего наделяется полномочиями определять требования к техническим средствам ЗИ и организационным мерам ЗИ	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.90 Служба ИБ осуществляет планирование и контроль обеспечения ЗИ при осуществлении переводов денежных средств, для чего наделяется полномочиями контролировать выполнение работниками требований к обеспечению ЗИ при осуществлении переводов денежных средств	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.91 Служба ИБ осуществляет планирование и контроль обеспечения ЗИ при осуществлении переводов денежных средств, для чего наделяется полномочиями участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению ЗИ при осуществлении переводов денежных средств, и предлагать применение дисциплинарных взыскании, а также направлять предложения по совершенствованию ЗИ	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0
П.92 Служба ИБ осуществляет планирование и контроль обеспечения ЗИ при осуществлении переводов денежных средств, для чего наделяется полномочиями участвовать в действиях, связанных с выполнением требований к обеспечению ЗИ при осуществлении переводов денежных средств, применяемых при восстановлении предоставления услуг платежной системы после сбоев и отказов в работе объектов информационной инфраструктуры	ОПДС БПА (БПСА) ЮЛ ОУПИ	СТО БР ИББС-1.0

ЗАДАЧИ

- Разработка и совершенствование единой политики (концепции) обеспечения безопасности информации в организации;
- Определение требований к системе защиты информации, обращающейся в организации;
- Организация мероприятий и координация работ всех подразделений организации по защите информации на всех этапах технологических циклов обработки информации, в соответствии с единой политикой информационной безопасности;
- Контроль и оценка эффективности принятых мер по защите информации в организации;
- Предотвращение возможности нарушений политики информационной безопасности организации, либо устранение последствий этих нарушений.

Полномочия

- Организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации
- Разрабатывать и вносить предложения по изменению политик ИБ организации;
- Организовывать изменение существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации;
- Определять требования к мерам обеспечения ИБ организации;
- контролировать работников организации в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам;

Полномочия

- осуществлять мониторинг событий, связанных с обеспечением ИБ;
- участвовать в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД, например, нарушивших требования инструкций, руководств и т.п. по обеспечению ИБ организации;
- участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий;
- участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации.

Функции

- Организация и координация действий подразделений организации в решении вопросов защиты информации.
- Экспертиза договоров организации со сторонними организациями по вопросам обеспечения безопасности банковской информации при осуществлении информационного взаимодействия с контрагентами.
- Экспертиза технических заданий, проектов, решений при их внедрении в организации, с точки зрения обеспечения защиты информации.
- Участие в работе комиссии по пересмотру перечня сведений организации, подлежащих защите.
- Согласование технических порядков по технологиям, связанным с обработкой информации на всех технологических циклах.
- Участие в проектировании, приёмке, сдаче в промышленную эксплуатацию программных средств и автоматизированных систем с точки зрения защиты информации, оказание консультативной поддержки, согласование.

Функции

- Контроль за соблюдением работниками организации правил работы в локальной сети.
- Контроль за соблюдением требований технических указаний и сертификатов на приобретённые программные и аппаратные средства защиты информации. Организация и контроль за разрешительной системой допуска работников к работе с защищаемой информацией.
- Осуществление контроля за генерацией сменяемых элементов криптографической и специальной защиты (ключей шифрования, электронно-цифровых подписей, паролей и др.), участие в разработке и согласование схем доставки сменяемых элементов криптографической и специальной защиты пользователям АИС организации.
- Участие в проведении аттестации автоматизированных рабочих мест по обработке и передаче информации, подлежащей защите с точки зрения необходимости и достаточности реализованных средств защиты информации.

Функции

- Контроль за работой администраторов подсистем информационной системы организации с точки зрения обеспечения последними мер по защите информации, обращающейся в подсистеме, администрирование которой они осуществляют. Определение достаточности реализованных мер обеспечения информационной безопасности, участие в разработке и согласование порядков и положений по обеспечению информационной безопасности в отдельных подсистемах организации.
- Проведение служебных расследований по фактам сбоев в работе информационных систем организации, повлекших за собой нарушение установленного порядка защиты информации.
- Проведение периодических проверок знания и выполнения работниками организации предписаний и инструкций по вопросам обеспечения защиты информации.
- Оказание консультационных услуг работникам организации в решении вопросов защиты информации при работе в информационных системах организации.

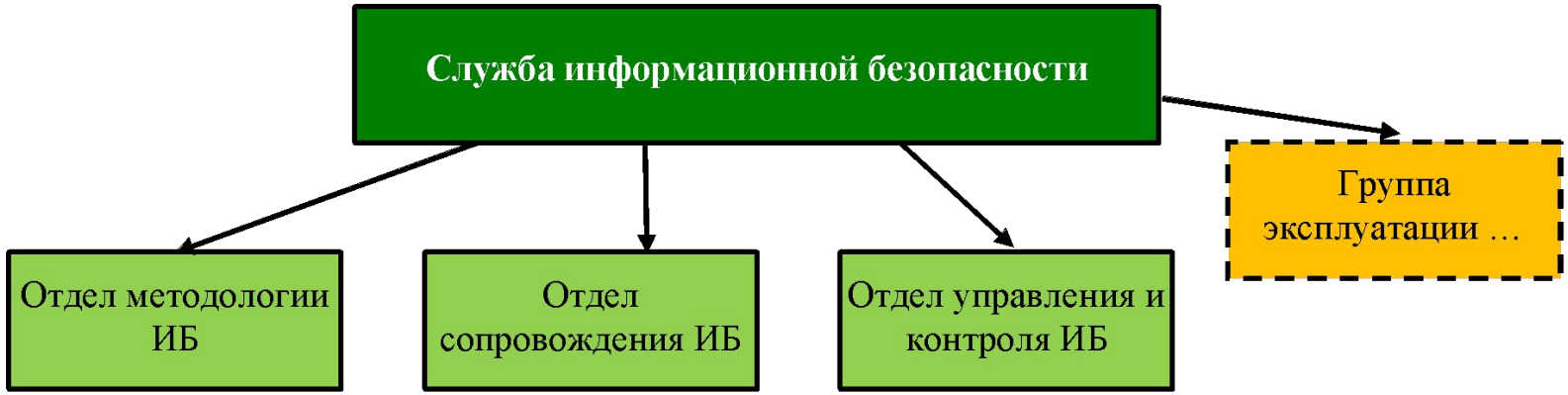
ПРИЧАСТНЫЕ СТОРОНЫ

В процессе обеспечения информационной безопасности организации участвует не только подразделение информационной безопасности, но и другие подразделения:

- Подразделение информационных технологий;
- Юридическая служба;
- Служба риск – менеджмента;
- И др.

Наиболее эффективным способом разграничения полномочий и ответственности является способ, когда порядок разграничения полномочий и ответственности обсуждается на совещании коллегиального органа по обеспечению информационной безопасности и закрепляется протоколом этого совещания.

ВОЗМОЖНАЯ СТРУКТУРА СЛУЖБЫ



В состав службы информационной безопасности могут входить:

- отдел методологии информационной безопасности;
- отдел сопровождения информационной безопасности;
- отдел управления и контроля информационной безопасности, включающий группу по управлению инцидентами ИБ.

По решению руководства оператора в соответствии с объемом практических задач в составе службы информационной безопасности могут быть образованы подразделения (группа, сектор), отвечающее за эксплуатацию специфичных объектов, таких как удостоверяющий центр и др.

Итого

По группе требований 8. Организация функционирования службы ИБ необходимо разработать:

- **Положение об отделе ИБ**
- **Приказы (назначения)**
- **Должностные инструкции**

Рекомендуется учесть:

- **ПП-584**
- **СТО БР ИББС 1.0 (служба ИБ)**

11. ОПРЕДЕЛЕНИЕ И РЕАЛИЗАЦИЯ ПОРЯДКА ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ПС

Применительно к порядку обеспечения защиты информации в платежной системе существуют требования как в ПП 584, так и в Положении Банка России № 382-П.

Требования ПП 584 сформулированы следующим образом:

«7. Операторы и агенты утверждают локальные правовые акты, устанавливающие порядок реализации требований к защите информации.»

Положение Банка России № 382-П определяет требования к порядку обеспечения защиты информации в п.п. 2.2 и 2.14. В п.2.14 в развернутом виде.

ТРЕБОВАНИЯ ПОЛОЖЕНИЯ БАНКА РОССИИ № 382-П

В пункте 2.2 определено, что среди прочих требований Положение устанавливаются «*требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;*», непосредственно сами требования сформулированы в п.2.14.

ТРЕБОВАНИЯ ПОЛОЖЕНИЯ БАНКА РОССИИ № 382-П К СЛУЖБЕ ИБ

Требования основной части 382-П	Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
2.14.1. Документы, составляющие порядок обеспечения защиты информации при осуществлении переводов денежных средств, определяют: - состав и порядок применения организационных мер защиты информации; - состав и порядок использования технических средств защиты информации, включая информацию о конфигурации технических средств защиты информации, определяющую параметры их работы; - порядок регистрации и хранения информации на бумажных носителях и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации.	-		

СЛЕДСТВИЯ

Из приведенного фрагмента вытекают следующие выводы:

1) порядок обеспечения защиты информации при осуществлении переводов денежных средств – это комплекс документов;

2) данный комплекс документов должен включать как регламенты и положения (организационные меры защиты), так и инструкции и руководства (для технических средств), а также журналы и «логии», отражающие факт регистрации значимых для целей защиты информации действий и событий.

Таким образом, «порядок обеспечения защиты информации при осуществлении переводов денежных средств» это практически все то, что в документе Банка России РС БР ИББС–2.0 обозначается как «Документация в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС–1.0». За тем исключением, что явно не указаны документы «верхнего уровня», а также с той поправкой, что рассмотрению подлежит только одно их направлений деятельности организации (оператора или агента) - сфера «осуществления переводов денежных средств». В пределах этой же области и будет осуществлять последующие надзор и контроль в соответствии с требованиями Положения Банка России № 382-П.

ТРЕБОВАНИЯ ПОЛОЖЕНИЯ БАНКА РОССИИ № 382-П К СЛУЖБЕ ИБ (ПРОДОЛЖЕНИЕ)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.107 Оператор платежной системы устанавливает распределение обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств путем: самостоятельного определения оператором платежной системы порядка обеспечения защиты информации при осуществлении переводов денежных средств; распределения обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы; передачи функций по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств оператором платежной системы, не являющимся кредитной организацией, расчетному центру	ОПС	

Требования Положения Банка России № 382-П к Службе ИБ (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.108 Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают определение порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках распределения обязанностей, установленных оператором платежной системы	ОПС ОПДС ОУПИ	

Рассмотрены полномочия и обязанности «**оператора платежной системы**» в части решений об исполнении порядка.

Требования Положения Банка России № 382-П к Службе ИБ (продолжение)

Требования основной части 382-П	Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
2.14.2. Для определения порядка обеспечения защиты информации при осуществлении переводов денежных средств оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры в рамках обязанностей, установленных оператором платежной системы, могут использовать: - положения национальных стандартов по защите информации, стандартов организаций, в том числе стандартов Банка России, рекомендаций в области стандартизации, в том числе рекомендаций Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании; - положения документов, определяемых международными платежными системами; - результаты анализа рисков при обеспечении защиты информации при осуществлении переводов денежных средств на основе моделей угроз и нарушителей безопасности информации, определенных в национальных стандартах по защите информации, стандартах организаций, в том числе стандартах Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании, или на основе моделей угроз и нарушителей безопасности информации, определенных оператором платежной системы, оператором по переводу денежных средств, оператором услуг платежной инфраструктуры.	-	ОПС ОПДС ОУПИ	СТО БР ИББС-1.0

СЛЕДСТВИЯ

Могут использоваться указанные источники при разработке документов, составляющих «порядок обеспечения защиты информации при осуществлении переводов денежных средств» с учетом решений, принятых оператором платежной системы.

При этом, по всей видимости, надо понимать, что если КО как «оператор по переводу денежных средств» не имеет своего «оператора платежной системы», то тогда она действует самостоятельно. Ясных указаний про это нет.

Требования Положения Банка России № 382-П к Службе ИБ (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.109 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	
П.110 Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают назначение лиц, ответственных за выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств	ОПДС ОУПИ	

Требования Положения Банка России № 382-П к Службе ИБ (продолжение)

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.111 Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) применения организационных мер защиты информации	ОПДС ОУПИ	СТО БР ИББС-1.0
П.112 Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) использования технических средств защиты информации	ОПДС ОУПИ	СТО БР ИББС-1.0

СЛЕДСТВИЯ

Значимым из этого фрагмента выводом является то, что служба информационной безопасности может не быть ответственной за реализацию порядка (что абсолютно понятно для большинства случае), но контролировать его исполнение она обязана.

ВЫВОДЫ

Таким образом, наиболее рациональным шагом как «операторов», так и «агентов» является следование рекомендациям документа Банка России РС БР ИББС–2.0, в т.ч. и в части областей, явно не затрагиваемых требованиями Положения Банка России № 382-П.

В рамках проверочных мероприятий могут возникнуть ситуации, касающиеся вопросов правомочности или же полноты тех или иных норм в срезе защиты информации при осуществлении переводов денежных средств.

Ответы на это могут быть найдены как в документах «верхнего уровня» или же в документах, регламентирующих единых порядок действий в пределах всей организации или группы юридических лиц.

Итого

По группе требований 11. Определение и реализация порядка обеспечения защиты информации в ПС необходимо разработать:

Оператор ПС:

- **Регламент взаимодействия в ПС**
- **Раздел по ЗИ в правилах ПС**

Участник ПС:

- **Регламент предоставления отчетности оператору ПС**
- **Должностные инструкции ИБ**
- **Положение об отделе ИБ**

15. ЗАЩИТА ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ С ПРИМЕНЕНИЕМ БАНКОМАТОВ И ПЛАТЕЖНЫХ ТЕРМИНАЛОВ

Данная группа требований определена Указанием Банка России от 14 августа 2014 год № 3361-У и вступает в силу с 17 марта 2015 года.

В данном разделе используется термин ТУ ДБО (терминальные устройства дистанционного банковского обслуживания) к которым относятся банкоматы и платежные терминалы, используемые при осуществлении переводов денежных средств.

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.130 Оператор по переводу денежных средств обеспечивает проведение классификации ТУ ДБО, с учетом следующего: • возможностей несанкционированного получения информации, необходимой для осуществления переводов денежных средств; • возможностей осуществления воздействия, приводящего к сбоям, отказам, повреждению ТУ ДБО; • особенностей конструкции ТУ ДБО; • места установки ТУ ДБО	ОПДС	
П.131 Оператор по переводу денежных средств фиксирует во внутренних документах результаты классификации ТУ ДБО и проводит пересмотр результатов классификации ТУ ДБО при изменении факторов, влияющих на классификацию ТУ ДБО	ОПДС	
П.132 Оператор по переводу денежных средств учитывает результаты классификации ТУ ДБО при выборе организационных мер защиты информации, технических средств защиты информации, а также функциональных и конструктивных особенностей ТУ ДБО, связанных с обеспечением защиты информации при осуществлении переводов денежных средств	ОПДС	

Необходимость проведения классификации ТУ ДБО и использование ее результатов для определения организационных и технических мер защиты информации

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.133 Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости установки на (в) ТУ ДБО технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного оборудования	ОПДС	
П.134 Оператор по переводу денежных средств обеспечивает контроль состава объектов информационной инфраструктуры в сегментах информационно-телекоммуникационных сетей, в составе которых присутствуют ТУ ДБО, за исключением случая использования услуг радиотелефонной подвижной связи	ОПДС	

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.135 Оператор по переводу денежных средств обеспечивает размещение на лицевой панели ТУ ДБО или в непосредственной близости от ТУ ДБО сведений, включающих: • наименование оператора по переводу денежных средств, которому принадлежит ТУ ДБО на правах собственности, аренды, лизинга; • идентификатор ТУ ДБО; • телефонный номер (телефонные номера), адреса электронной почты, предназначенные для связи клиентов, использующих данное ТУ ДБО, с оператором по переводу денежных средств, банковским платежным агентом (субагентом) по вопросам, связанным с использованием данного ТУ ДБО; • порядок действий клиента в случае возникновения подозрения о нарушении порядка штатного функционирования ТУ ДБО, а также в случае выявления признаков событий, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО	ОПДС	
П.136 Оператор по переводу денежных средств определяет во внутренних документах порядок работы с заявлениями клиентов о выявленных событиях, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО, и обеспечивает выполнение указанного порядка	ОПДС	

Формирование инструкций для клиентов в случае нарушения штатного режима функционирования при осуществлении переводов денежных средств с применением

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.137 Оператор по переводу денежных средств определяет порядок настройки программного обеспечения, средств вычислительной техники в составе ТУ ДБО, включая информацию о конфигурации, определяющей параметры работы технических средств защиты информации, и обеспечивает выполнение указанного порядка	ОПДС	

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.138 Оператор по переводу денежных средств обеспечивает периодический контроль состояния ТУ ДБО с целью выявления событий, влияющих на обеспечение защиты информации при осуществлении переводов денежных средств. К таким событиям, в том числе, относятся: несанкционированное внесение изменений в программное обеспечение ТУ ДБО, включая внедрение вредоносного кода; несанкционированное внесение изменений в аппаратное обеспечение ТУ ДБО (установка несанкционированного оборудования на (в) ТУ ДБО), включая несанкционированное использование коммуникационных портов; сбои и отказы в работе технических средств защиты информации, устройств приема платежных карт (при наличии данных устройств), устройств приема наличных денежных средств (при наличии данных устройств), устройств выдачи наличных денежных средств (при наличии данных устройств)	ОПДС	
П.139 В случае выявления вышеуказанных событий, оператор по переводу денежных средств обеспечивает приведение ТУ ДБО в такое состояние, при котором обслуживание клиентов невозможно, до минимизации возможности наступления негативных последствий выявленных событий или устранения несанкционированных изменений в программном и аппаратном обеспечении ТУ ДБО	ОПДС	

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.140 Оператор по переводу денежных средств определяет во внутренних документах и обеспечивает выполнение порядка проведения контроля, включая его периодичность, в зависимости от: • использования систем удаленного мониторинга состояния ТУ ДБО, применения технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного на (в) ТУ ДБО оборудования; • результатов классификации ТУ ДБО.	ОПДС	

Определение порядка и сроков проведения контроля состояния ТУ ДБО

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.141 Оператор по переводу денежных средств определяет требования к обеспечению привлеченными к деятельности по оказанию услуг по переводу денежных средств банковскими платежными агентами (субагентами) защиты информации при использовании ТУ ДБО	ОПДС	

Требования Положения №382-П

Требования приложения 382-П	Субъекты	Подобные требования в других стандартах
П.142 Оператор по переводу денежных средств осуществляет переводы денежных средств с применением расчетных (дебетовых), кредитных карт: оснащенных микропроцессором, оснащенных микропроцессором и магнитной полосой, выданных (эмитированных) кредитными организациями на территории Российской Федерации, срок действия которых начинается после 1 июля 2015 года; оснащенных магнитной полосой и (или) микропроцессором, выданных (эмитированных) кредитными организациями на территории Российской Федерации, срок действия которых начинается до 1 июля 2015 года	ОПДС	

Устанавливает требования к расчетным и кредитным картам, применяемым для перевода денежных средств

Итого

По группе требований 15. Защита информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов необходимо разработать:

- **Акт классификации ТУ ДБО**
- **Порядок использования ТУ ДБО**
- **Инструкции для администраторов и пользователей**

Коллеги,
Большое спасибо за внимание и совместную работу!

Web: http://www.tsarev.biz/
Twitter: http://twitter.com/TsarevEvgeny
Facebook: http://www.facebook.com/tsarev.biz
E-mail: TsarevEO@gmail.com
Tel: +7-926-104-70-58