ДиалогНаука

Реализация требований по защите информации в соответствии с ФЗ «О национальной платежной системы»

Свинцицкий Антон

Руководитель отдела консалтинга

ЗАО «ДиалогНаука»

ДиалОгНаука

Национальная платежная система

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.06.2011 N 161-ФЗ «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ»

ДиалОгНаука

Национальная платежная система. Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»

- **Целью** Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе» является законодательное закрепление понятия «платежная система», установление требований к организации и функционированию таких систем, а также надзору и контролю за их деятельностью.

- **Предметом** Закона являются деятельность и взаимодействие в рамках платежных систем организаций - операторов по переводу денежных средств, включая операторов услуг платежной инфраструктуры (операционных, клиринговых и расчетных центров).

ДиалОгНаука

Национальная платежная система. Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»

Глава 1. Общие положения

Глава 2. Порядок оказания платежных услуг, в том числе осуществления перевода денежных средств, и использования электронных средств платежа

Глава 3. Субъекты национальной платежной системы и требования к их деятельности

Глава 4. Требования к организации и функционированию платежных систем

Глава 5. Надзор и наблюдение в национальной платежной системе

Глава 6. Заключительные положения

ДиалОгНаука

Национальная платежная система. Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»

- Закон вводит новые правила осуществления расчетов, правила проведения расчетов электронными денежными средствами, а также вносит изменения в действующие правила.
- Положения Закона затрагивают деятельность многих участников безналичных расчетов: банков, небанковских кредитных организаций, платежных агентов, поставщиков, работающих с платежными агентами, и др.
- Закон будет вступать в силу поэтапно. Большая часть его положений вступит в силу через год после опубликования (30.09.2012), а некоторые нормы - через 18 месяцев (30.03.2013). В частности, нормы, предполагающие наиболее существенные изменения, вступят в силу не в сентябре, а несколько позже, поскольку многие из них требуют подготовки нормативных документов, технической и организационной подготовки для участников данной сферы деятельности.
- Закон представляет собой объемный нормативный акт, в котором условно можно выделить три основных направления регулирования: деятельность платежных систем, осуществление безналичных расчетов, эмиссия и использование электронных денежных средств.

Национальная платежная система. Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»

Закон впервые устанавливает, что не только Банки, но и все субъекты национальной платежной системы **обязаны гарантировать банковскую тайну** и **обеспечивать защиту информации** о применяемых способах обеспечения информационной безопасности, а также защиту персональных данных и другой информации, подлежащей обязательной защите в соответствии с законодательством РФ.

ДиалОгНаука

Национальная платежная система

ОСНОВНЫЕ ПОНЯТИЯ

Национальная платежная система

Национальная платежная система - это совокупность операторов по переводу денежных средств (в том числе электронных денег), банковских платежных агентов, платежных агентов, организаций федеральной почтовой связи.

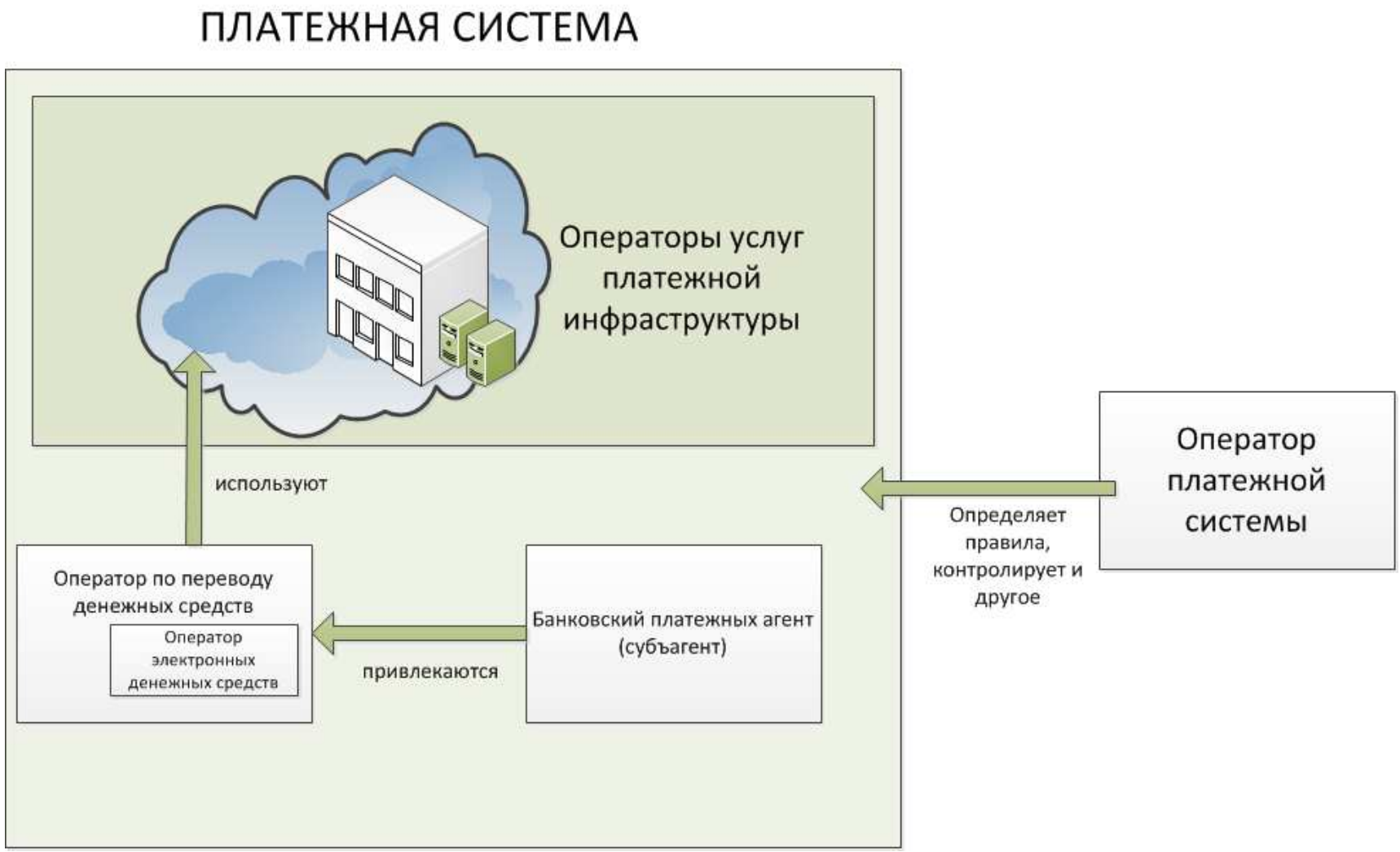
ДиалОгНаука

Национальная платежная система
Основные понятия

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.

Платежная система носит более локальный характер чем национальная платежная система.

Структура платежной системы



Операторы платежных систем

Банк России ведер реестр операторов платежных систем.

На текущий момент зарегистрировано 20 платежных систем.

При регистрации указываются также:

- Расчетный центр;
- Платежный клиринговый центр;
- Операционный центр.

Ссылка:
http://www.cbr.ru/today/Print.aspx?File=payment_system/rops/reestr.zip&pid=rops&sid=ITM_13528

Национальная платежная система
Основные понятия

Перевод денежных средств - действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика

Существует три вида платежной услуги:

- *услуга по переводу денежных средств,*
- *услуга почтового перевода,*
- *услуга по приему платежей.*

Национальная платежная система
Основные понятия

Характеристики перевода денежных средств:

- Безотзывность - характеристика перевода денежных средств, обозначающая отсутствие или прекращение возможности отзыва распоряжения об осуществлении перевода денежных средств в определенный момент времени;
- Безусловность - характеристика перевода денежных средств, обозначающая отсутствие условий или выполнение всех условий для осуществления перевода денежных средств в определенный момент времени;
- Окончательность - характеристика перевода денежных средств, обозначающая предоставление денежных средств получателю средств в определенный момент времени.

Оператор и правила платежной системы

- Оператор платежной системы обязан **контролировать** соблюдение установленных правил участниками платежной системы, а также операторами услуг платежной инфраструктуры.
- Правилами платежной системы будут **устанавливаться** требования к осуществлению перевода денежных средств, распределению рисков в платежной системе и т.д. Полный перечень вопросов, которые будут регулироваться данными правилами, приведен в ст. 20 Закона.
- Согласно Закону о платежной системе правила платежной системы являются договором присоединения. Участники платежной системы присоединяются к правилам платежной системы только путем **принятия их в целом**.
- Требования к правилам платежной системы **устанавливаются** непосредственно Законом. Банк России уполномочен определять особенности только для правил платежных систем, в рамках которых осуществляется перевод денежных средств по сделкам, совершенным на организованных торгах.

Обеспечение защиты информации в платежной системе

- 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
- 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.

ДиалОгНаука

Обеспечение защиты информации в платежной системе

- Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации, осуществляются ФСТЭК и ФСБ России, в пределах их полномочий и без права ознакомления с защищаемой информацией.

ДиалОгНаука

Национальная платежная система

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ №584

ДиалОгНаука

Требования по обеспечению информационной безопасности

Постановление Правительства Российской Федерации №584 от 13 июня 2012 года (вступает в силу 1.07.2012) устанавливает требования к «**правилам платежной системы**», в том числе по следующим направлениям:

- создание выделенного подразделения и(или) лица, ответственного за обеспечение ИБ;
- включение в должностные обязанности работников требований по обеспечению ИБ;
- осуществление мероприятий по определению угроз ИБ и анализу уязвимости информационных систем;
- проведение анализа рисков ИБ;
- необходимость применение средств защиты информации (СЗИ от НСД, защиты от вредоносного ПО, СКЗИ, СОВ, САЗ);
- управление инцидентами ИБ;
- проведение периодического контроля (1 раз в 2 года).

ДиалОгНаука

Требования по обеспечению информационной безопасности

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

ДиалогНаука

Национальная платежная система

ТРЕБОВАНИЯ БАНКА РОССИИ

Положение Банка России 382-П

Определяет необходимость защиты информации при осуществлении переводов денежных средств!

1. Устанавливает перечень защищаемой информации.
2. Устанавливает направления обеспечения информационной безопасности
3. Требования к контролю (проверка на месте и(или) запрос на предоставление информации)

Мера принуждения:

«ограничивает (приостанавливает) предписанием оказание операционных услуг, в том числе при привлечении операционного центра, находящегося за пределами Российской Федерации, и (или) услуг платежного клиринга»

Положение Банка России 382-П

Типы защищаемых информационных активов:

- информации об остатках денежных средств на банковских счетах;
- информации об остатках электронных денежных средств;
- информации о совершенных переводах денежных средств;
- требование об отнесении информации о совершенных переводах денежных средств к защищаемой информации;
- информации, содержащейся в оформленных в рамках применяемой формы безналичных расчетов;
- информации о платежных клиринговых позициях;
- информации, необходимой для удостоверения клиентами права распоряжения денежными средствами, в том числе данных держателей платежных карт;
- ключевой информации СКЗИ;;
- управляющая информация;
- информации ограниченного доступа (в том числе персональных данных).

ДиалогНаука

Положение Банка России 382-П
Направления обеспечения ИБ

Направление	Раздел СТО БР ИББС-1.0-2010
Распределение ролей	7.2
Обеспечение ИБ на жизненном цикле	7.3
Управление доступом	7.4
Антивирусная защита	7.5
Контроль использования Интернет	7.6
Использование СКЗИ	7.7
Обеспечение защиты информации при осуществлении переводов	7.8, 7.9
Организационная структура ИБ	8.2
Повышение осведомленности в вопросах ИБ	8.9
Управление инцидентами ИБ	8.10

ДиалогНаука

Положение Банка России 382-П
Направления обеспечения ИБ

Направление	Раздел СТО БР ИББС-1.0-2010
Определение и реализация порядка обеспечения защиты информации при осуществлении переводов	8.4 8.5 8.12
Оценка выполнения оператором платежной системы, оператором по переводу денежных средств	8.13 8.14
Доведение требований по обеспечение ИБ до оператора платежной системы	-
Совершенствование оператором платежной системы, оператором по переводу денежных средств	8.15 8.16 8.17 8.18

Положение Банка России 382-П
Направления обеспечения ИБ

Все требования разбиты на 3 основных класса:

1. Требования, необходимые к документированию в Организации.
2. Требования, необходимые к выполнению в Организации.
3. Требования, необходимые и к документированию, и к выполнению в Организации.

ДиалОгНаука

Пример описания требований

Требование	Реализация		Субъект платежной системы			
	Документирование	Выполнение	Оператор по переводу	Банковский платежный агент	Оператор платежной инфраструктуры	Оператор платежной системы
использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры	Да	Да	Да	Да	Да	Нет

ДиалОгНаука

Пример описания требований

Требование	Реализация		Субъект платежной системы			
	Документирование	Выполнение	Оператор по переводу	Банковский платежный агент	Оператор платежной инфраструктуры	Оператор платежной системы
определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок обращения с носителями криптографических ключей…	Да	-	Да	Да	Да	Нет

ДиалогНаука

Положение Банка России 382-П
Направления обеспечения ИБ

При проведении оценки соответствия используются три обобщающих показателя:

- обобщающий показатель $\mathbf{EV1_{ПС}}$ - характеризующий выполнение группы требований к обеспечению защиты информации при осуществлении переводов денежных средств, определенных в пунктах 2.4 - 2.10 Положения 382-П (с учетом корректирующего коэффициента k1);

- обобщающий показатель $\mathbf{EV2_{ПС}}$ - характеризующий выполнение группы требований к обеспечению защиты информации при осуществлении переводов денежных средств, определенных в пунктах 2.11 - 2.17 Положения 382-П (с учетом корректирующего коэффициента k2);

- итоговый показатель $\mathbf{R_{ПС}}$ - характеризующий выполнение всех требований к обеспечению защиты информации при осуществлении переводов денежных средств (всего 129 показателей).

Положение Банка России 382-П
Направления обеспечения ИБ

Итоговые значения

$$R_{ПС} = \text{Min}\{EV1_{ПС}, EV2_{ПС}\}$$ с учетом корректирующих коэффициентов

Уровни значения

Больше или равно 0,85	**«хорошо»**
От 0,7 до 0,85	**«удовлетворительно»**
От 0,5 до 0,7	**«сомнительная»**
Менее 0,5	**«неудовлетворительная»**

Положение Банка России 379-П

Определяет требования:

- К проведению анализа рисков информационной безопасности

(частично п.8.3-8.5 СТО БР ИББС-1.0-2010,
РС БР ИББС-2.2-2009).

- К обеспечению бесперебойного функционирования платежной системы

(частично п.8.11 СТО БР ИББС-1.0-2010)

Срок реализации требований для операторов платежных систем: 1 января 2013 года

Положение Банка России 379-П

Показатели БФПС:

- ✓ уровень бесперебойности оказания операционных услуг;
- ✓ уровень бесперебойности оказания услуг платежного клиринга;
- ✓ уровень бесперебойности оказания расчетных услуг.

Самое важное: оператор платежной системы должен определить метрики и методики оценки показателей БФПС.

Положение 380-П

- Устанавливает формы, способы и порядок осуществления Банком России наблюдение за деятельностью операторов по переводу денежных средств, операторов платежных систем, операторов услуг платежной инфраструктуры (наблюдаемых организаций), других субъектов НПС за оказываемыми ими услугами, а также за развитием платежных систем, платежной инфраструктуры.

ДиалогНаука

Положение 381-П

- Определяет порядок, формы и способы осуществления надзора за соблюдением требований ФЗ №161 не являющихся кредитными организациями операторами платежных систем, операторами услуг платежной инфраструктуры.
  - дистанционный надзор;
  - проведение инспекционных проверок
  - применение действий и мер принуждения

ДиалОгНаука

Указания №2831-У

- Отчетность по форме 0403202 (оценка выполнения требований 382-П);
  - Не позднее 30 дней после окончания оценки соответствия;
  - Отчетность в соответствии с 1375-У;
  - В электронном виде в соответствии с 1546-У;
  - С 1 июля 2013 года – только в электронном виде
- Отчетность по форме 0403203 (отчетность по инцидентам ИБ)
  - Ежемесячно не позднее 10 рабочего дня месяца;
  - По требованию ЦБ не позднее 10 рабочих дней со дня получения уведомления;
  - Отчетность в соответствии с 1375-У;
  - В электронном виде в соответствии с 1546-У;
  - С 1 июля 2013 года – только в электронном виде

ДиалогНаука

Указания №2831-У. Отчетность по инцидентам ИБ

Типы рассматриваемых инцидентов ИБ:

- ✓ воздействие вредоносного кода (нарушение доступности и целостности информационных активов);
- ✓ нарушение доступности и целостности предоставляемых услуг и сервисов на всех уровнях среды обработки (более 3 часов);
- ✓ нарушение конфиденциальности аутентификационной информации клиентов;
- ✓ компрометация ключевой информации;
- ✓ осуществление несанкционированного денежного перевода;

Указания №2831-У. Отчетность по инцидентам ИБ

1. Общее количество инцидентов за отчетный период.
2. Дата выявления инцидента ИБ.
3. Наименование БПА (субагента) и его код.
4. Последствия инцидента (в том числе и финансовые потери).
5. Объекты информационной инфраструктуры.
6. Описание предпринятых действий.
7. Факты обращения в правоохранительные органы.

ДиалогНаука

Спасибо за внимание!
Вопросы?

ЗАО «ДиалогНаука»
Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: svintsitskii@DialogNauka.ru