РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ.

ТРЕБОВАНИЯ ФЗ «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ» И ПОЛОЖЕНИЯ БАНКА РОССИИ 382-П.

КОНСАЛТИНГОВЫЕ УСЛУГИ ЗАО «ДИАЛОГНАУКА»

Антон Свинцицкий

Руководитель отдела консалтинга

ЗАО «ДиалогНаука»

ДиалОгНаука

О компании «ДиалогНаука

«ДиалогНаука» является членом:

- Межрегиональной общественно организации «Ассоциация защиты информации» (АЗИ),
- Ассоциации документальной электросвязи (АДЭ),
- НП «АБИСС» (Некоммерческого партнерства «Сообщество пользователей стандартов по информационной безопасности АБИСС»)
- Ассоциации предприятий компьютерных и информационных технологий (АП КИТ)
- Консорциума «Инфорус»
- Британского Института Стандартов (British Standards Institution Management Systems)

О компании «ДиалогНаука»

Компания «ДиалогНаука» предлагает комплексные решения по защите автоматизированных систем предприятий от возможных угроз информационной безопасности.

- Защита персональных данных
- Защита от спама и вирусов
- Защита интернет-порталов
- Защита от утечки информации
- Защита электронного документооборота
- Мониторинг информационной безопасности
- Анализ защищенности и выявление уязвимостей
- Защита ERP-систем
- Криптографическая защита информации на базе VPN
- Организация защищенного удаленного доступа

Структура законодательства РФ

Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»

Постановление Правительства РФ от 13.06.2012 N 584 «Об утверждении Положения о защите информации в платежной системе»

Документы Банка России

Положение о бесперебойности функционирования платежных систем и анализе рисков в платежных системах (утв. Банком России 31.05.2012 N 379-П)

Положение 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» (утв. Банком России 09.06.2012 N 382-П)

. . .

Указание Банка России от 09.06.2012 N 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» (Зарегистрировано в Минюсте России 14.06.2012 N 24573)

Национальная платежная система. Федеральный закон «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).

- **Положения Закона** затрагивают деятельность многих участников безналичных расчетов: банков, небанковских кредитных организаций, платежных агентов, поставщиков, работающих с платежными агентами, и др.

Закон 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.

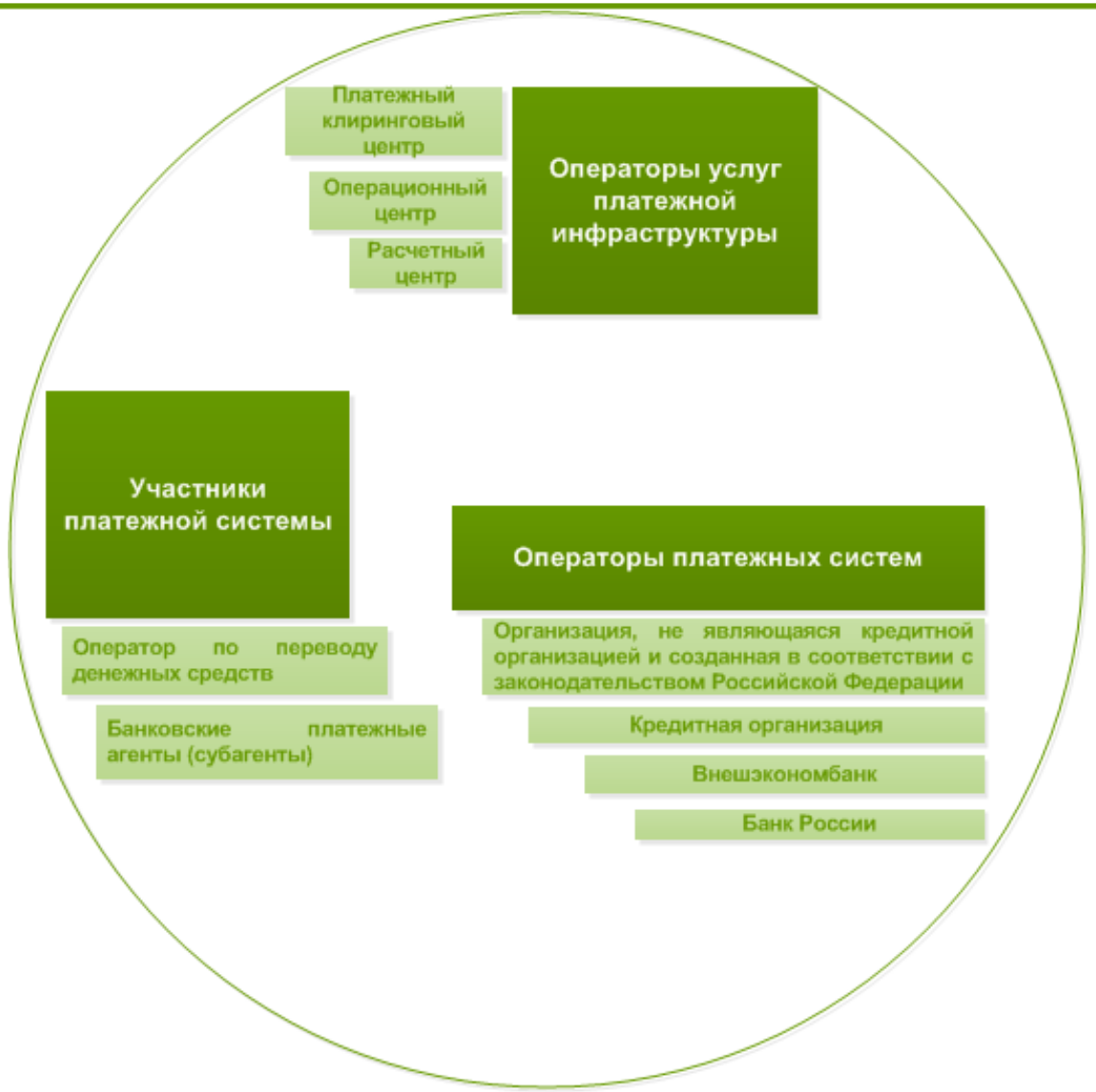
Национальная платежная система

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

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



Структура платежной системы

Оператор платежной системы

Определяет правила платежной системы

Платежная система

Оператор по переводу денежных средств

Оператор электронных денежных средств

Осуществляет перевод денежных средств

Банковский платежный агент

Банковский платежный субагент

Участники платежной системы

Операционный центр

Платежный клиринговый центр

Расчетный центр

Обеспечивает доступ к услугам по переводу денежных средств

Обеспечивает прием к исполнению распоряжений

Обеспечивает исполнение распоряжений

Операторы услуг платежной инфраструктуры

Центральный платежный клиринговый контрагент

Платежный клиринговый центр, выступающий плательщиком и получателем средств по переводам денежных средств

КЛИЕНТ

Операторы платежных систем

Банк России ведет реестр операторов платежных систем.

На текущий момент зарегистрировано 28 платежных систем (платежная система Мигом была исключена Приказом Банка России от19.03.2014 № ОД-335).

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

- 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.

Постановление Правительства Российской Федерации №584 от 13 июня 2012 года (вступило 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).

- 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**.

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).

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

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

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.

При проведении оценки соответствия используются три обобщающих показателя:

- обобщающий показатель **$EV1_{ПС}$** - 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 **$EV2_{ПС}$** - 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 **$R_{ПС}$** - характеризующий выполнение всех требований к обеспечению защиты информации при осуществлении переводов денежных средств (всего 129 показателей).

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

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

Итоговые значения

$R_{ПС} = Min \{EV1_{ПС} , EV2_{ПС} \}$ 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»**

Внесение изменений в 382-П

01.07.2013 в Минюсте зарегистрировано Указание Банка России от 05.06.2013 N 3007-У "О внесении изменений в Положение Банка России от 9 июня 2012 года N 382-П

Важно: провести оценку соответствия **в течение 6 месяцев со дня вступления Указания в силу (1.07.2013)** обязаны и организации, являющиеся на текущий момент операторами по переводу денежных средств, операторами платежной системы, операторами услуг платежной инфраструктуры.

Внесение изменений в 382-П

Основные изменения:

1. Регистрация действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения стала обязательной.
2. Определены требования к составу регистрируемой информации, действиями и срокам хранения информации.
3. Детализированы требования к документации на системы дистанционного банковского обслуживания, интернет-банкинг, мобильный банкинг и т.п. (в том числе регистрируемых БПА).
4. Уточнен порядок применения СКЗИ Российского производства.
5. Уточнения в части управления инцидентами информационной безопасности.
6. Требования к процессу оценки соответствия.

Внесение изменений в 382-П

Пример подхода к реализации нового требования (в части журналирования событий):

Рекомендуется разработать описание информационных систем, к которым предоставляется доступ клиентам, содержащее:

- описание архитектуры информационной системы;
- типы клиентских устройств;
- регистрация назначения и распределения прав клиентов и работников Банка:
  - роли;
  - регистрация событий (где, что, как долго хранится);
  - документ, описывающий формализованный процесс;
- регистрация всех действий клиентов:
  - состав регистрируемой информации;
  - регистрируемый идентификатор устройства клиента;
  - перечень действий клиентов;
  - срок хранения информации о действиях клиентов;
- правила формирования идентификатора;
- использование криптографии для защиты каналов связи и подтверждения электронных документов:
  - защита канала связи;
  - подтверждение электронных документов.

Отчетность. Оценка соответствия

УКАЗАНИЕ от 9 июня 2012 г. N 2831-У устанавливает формы и порядок отчетности по оценке соответствия и по инцидентам информационной безопасности

Отчетность по форме **0403202** (оценка соответствия):

Субъекты:

операторы платежной системы,

операторы услуг платежной инфраструктуры,

операторы по переводу денежных средств

Срок: не позднее 30 дней

Отчетность. Инциденты

Отчетность по форме **0403203** (инциденты):

Субъекты:

Операторы услуг платежной инфраструктуры

Операторы по переводу денежных средств

Срок: Не позднее 10 рабочих дней

Важно! С 28 января 2014 года новые требования к отчетности по инцидентам (УКАЗАНИЕ от 21 июня 2013 г. N 3024-У)

Отчетность. Инциденты

Отчетность по форме **0403203** (инциденты):

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.

Типы инцидентов:

- ✓ 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;

Опыт проведения оценки соответствия

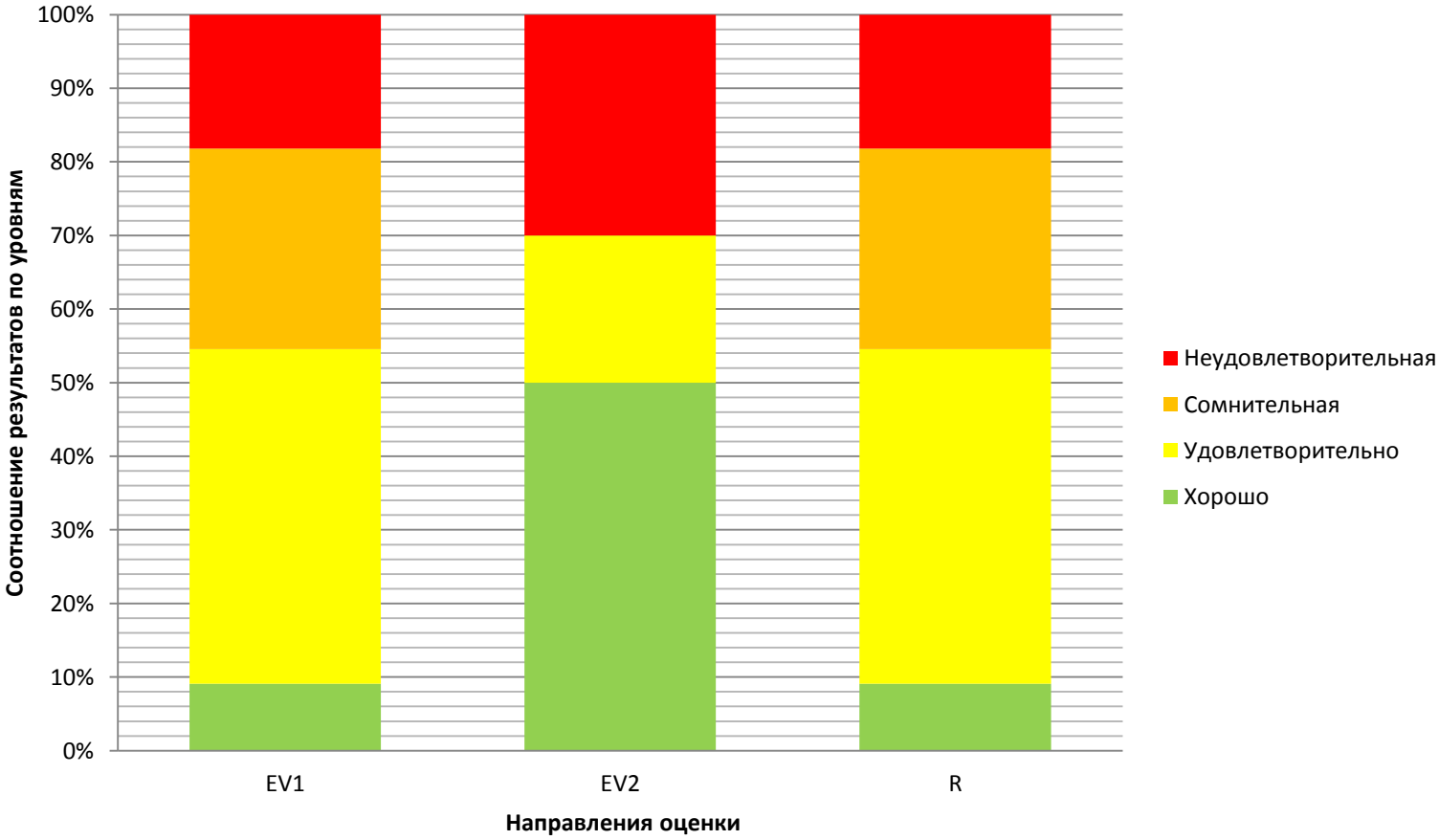
В 2013 году компанией ЗАО «ДиалогНаука» было реализовано более 10 проектов по оценке соответствия Банков требованиям Положения Банка России №382-П.

Средняя продолжительность оценки соответствия: 40 рабочих дней.

Состав рабочей группы: 2-3 аудитора.

Опыт проведения оценки соответствия

Обобщенные результаты:



Опыт проведения оценки соответствия

Основные недостатки:

1. Несогласованность документов ОПДС и документов ОПС (в том числе в части информирования об инцидентах информационной безопасности).
2. Невыполнение требований по регистрации событий в информационных системах ОПДС.
3. Отсутствие ответственных за обеспечение информационной безопасности в филиалах ОПДС.
4. Отсутствие описания области применения требований Положения Банка России 382-П (описание объектов инфраструктуры, регистрация лиц и т.п.).
5. Тестирование на реальных данных.
6. Отсутствие документов, регламентирующих жизненных цикл информационных систем (технические задания, ввод и вывод информационных систем).
7. Отсутствие документов, регламентирующих вопросы обеспечения информационной безопасности банкоматов.
8. Работа с персоналом по вопросам обеспечения информационной безопасности.
9. Не выполняется проверка выполнения требований по обеспечению защиты информации при осуществлении переводов денежных средств при присоединении к платежным системам.
10. И другие.

Что мы можем предложить?

1. **Проведение оценки соответствия** требованиям 382-П и разработка рекомендаций по совершенствованию СОИБ Оператора

2. **Приведение СОИБ** Оператора в соответствие требованиям 382-П (в том числе проведение работ по оценке рисков информационной безопасности)

3. **Внедрение СЗИ** в соответствии с рекомендациями и требованиями 382-П

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