

ТЕХНИЧЕСКАЯ ОРГАНИЗАЦИЯ ЗАЩИТЫ WEB – ПРИЛОЖЕНИЙ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЗ 152 «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

Денис Александров,
Ведущий инженер
ЗАО «ПЕТЕР-СЕРВИС»

О Компании ПЕТЕP-СЕРВИС



**ПЕТЕP-СЕРВИС
1992**

**Complus Resources
Limited**

АКЦИОНЕРНЫЙ КАПИТАЛ



Москва



Новосибирск



Краснодар



Екатеринбург



Самара



Киев

ФИЛИАЛЫ

География основных клиентов



Основные клиенты



Много разных Web-приложений

Исполнителям комплексных бизнес-процессов необходимо использовать различные информационные системы:

- ◆ Биллинговая система
- ◆ Абонентская картотека
- ◆ Технический учет
- ◆ Обработка заявок и нарядов
- ◆ Активация оборудования
- ◆ И другие...

Зачем это нужно ...

В рамках сквозного бизнес-процесса при переходе из одной информационной системы в другую Исполнителю приходится:

- ◆ Осуществлять повторную регистрацию (logon)
 - ◆ Повторно вводить текущие параметры бизнес-процесса (номер лицевого счета, абонентский номер, код услуги...)
 - ◆ Переключать внимание на различные «окна»
-
- ❑ *Как избавиться от избыточных операций и увеличить эффективность работы пользователей?*
 - ❑ *Как унифицированным и экономичным образом защитить персональные данные абонентов, хранящиеся в различных системах?*

Тенденции в области информационной безопасности

Исторические проблемы - несовместимость систем управления аутентификацией, авторизацией и аудитом в разных продуктах.

Это означает для заказчиков:

- Трудоемкое администрирование учетных записей
 - Многократная регистрация пользователей в разных системах
 - Необходимость выдавать права в каждой системе по отдельности
 - Различные интерфейсы администрирования в разных системах
- Сложности при использовании
 - Отсутствие единой точки входа (много разных паролей)

Новые законодательные требования:

- Обязательность защиты персональных данных – ФЗ «О персональных данных»
- Для защиты персональных данных в крупных АС обязательно использование сертифицированных средств защиты

Содержание

- Зачем нужно «единое окно»
- Выполнение требований ФЗ 152
- Обзор общей схемы решения
- Механизмы интеграции
- Заключение

Требования законодательства

Федеральный закон РФ от 27.07.2006 №152-ФЗ

- **Постановление Правительства РФ** от 17 ноября 2007 г. № 781, утверждающее «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
- **Постановление Правительства РФ** от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- **Совместный приказ ФСТЭК, ФСБ, Мининформсвязи** от 13 февраля 2008 г. № 55/86/20, утверждающий «Порядок проведения классификации информационных систем персональных данных»
- **Приказ ФСТЭК России** от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»

Необходимые мероприятия



Необходимые мероприятия



Продукт HAS ACCESS MANAGER

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 2113

Выдан 11 июня 2010 г.
Действителен до 11 июня 2013 г.

Настоящий сертификат удостоверяет, что средство защиты информации от несанкционированного доступа «PETER-SERVICE HAS ACCESS MANAGER» (партия из 2000 (двух тысяч) экземпляров продукции с заводскими номерами с № 0001 по № 2000, маркированных знаками соответствия с № Г 318000 по № Г 319999) производства ЗАО «ПЕТЕР-СЕРВИС», является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999) - по 4 уровню контроля и технических условий ТУ5014-002-11150642-2009.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ФГУП «Государственное научно-производственное предприятие «Информастика» (аттестат аккредитации от 23.03.2009 № СЗИ RU.076.Б038.036) – техническое заключение от 13.05.2010, и экспертного заключения от 21.05.2010 органа по сертификации ООО «Центр безопасности информации» (аттестат аккредитации от 09.02.2007 № СЗИ RU.117.А10.004).

Заявитель: ЗАО «ПЕТЕР-СЕРВИС»
Адрес: 191186, г. Санкт-Петербург, Гороховая ул., д. 14
Телефон: (812) 326-1299

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанного в настоящем сертификате руководящего документа и технических условий осуществляется испытательной лабораторией ФГУП «Государственное научно-производственное предприятие «Информастика».

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

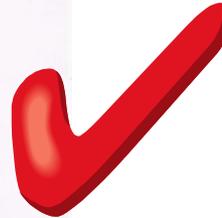


В.Селин

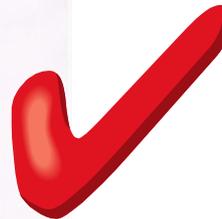
Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
11 июня 2010 г.



Наличие сертификата на средство защиты информации



Можно применять данное средство защиты в Web и мобильных приложениях

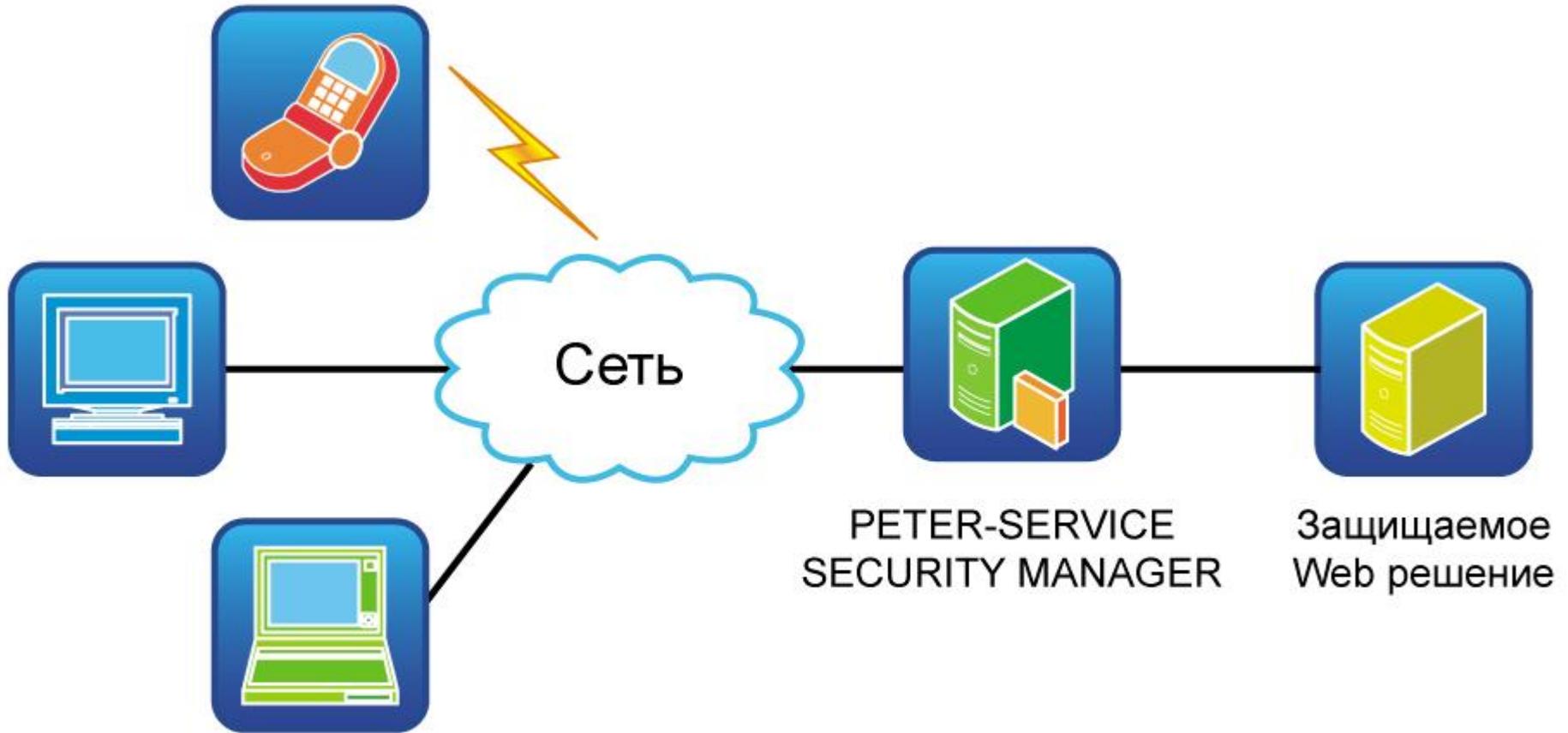


Масштабируемость и высокая производительность
10 мил. пользователей



Мультиплатформенность
(HP-UX, Linux, Sun Solaris, Windows)

PETER-SERVICE SECURITY MANAGER



Пользователи Web-систем
и мобильных приложений

Состав

- сертифицированное средство защиты информации от несанкционированного доступа, предназначенное для защиты информации в решениях, построенных на базе трехзвенной архитектуры PETER-SERVICE HAS ACCESS MANAGER
- web-сервер Apache с модулем XSLT-трансформации и WAF (mod_security)
- высокопроизводительный сервер приложений (HAS-сервер)
- web интерфейс для управления атрибутами доступа в HAS-сервер
- СУБД Oracle (Oracle Database 10g Express Edition)
- инсталлятор под все поддерживаемые операционные системы
- скрипты миграции

Подробная схема решения

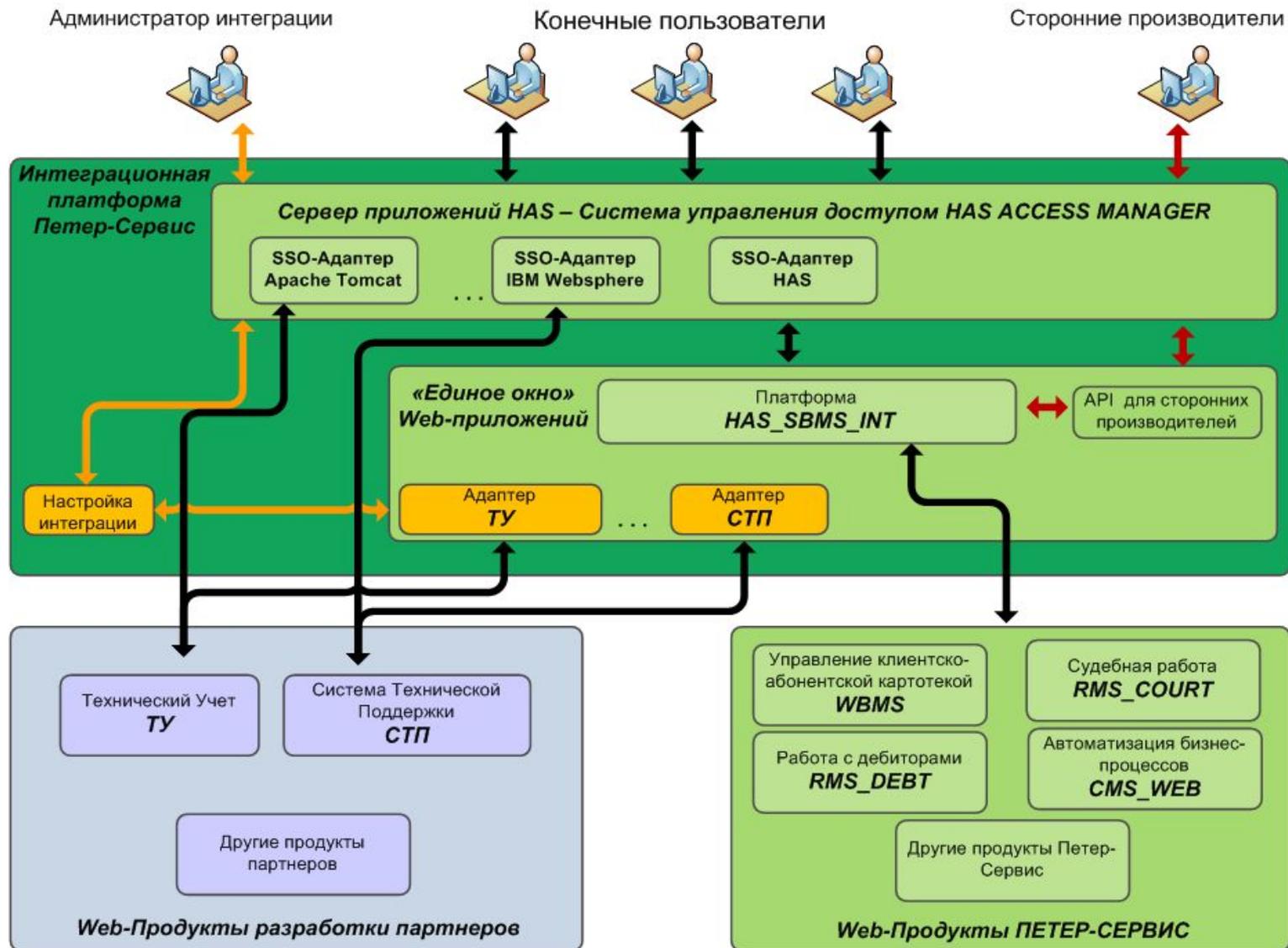


Схема решения: Пример

The screenshot shows a web-based CRM system interface. On the left is a navigation menu with various options. The main area displays a 'Карточка клиента' (Client Card) for 'Клиент 171002242274, ОАО "ПРОВЕРКА РАБОТЫ"'. Three yellow callout boxes point to specific sections of the interface:

- PETER-SERVICE WBMS**
Обработка абонентской картотеки
- PETER-SERVICE RMS**
Работа с должниками
- PETER-SERVICE CMS_WEB**
Автоматизация бизнес-процессов

At the bottom of the interface, a red text box states: **Различные Web-продукты от Петер-Сервис уже работают в «Едином окне»**

Copyright © 2003-2010 ЗАО ПЕТЕР-СЕРВИС

Варианты интеграции партнерских web-приложений

✓ Минимальная интеграция без передачи параметров бизнес-процессов

Необходимо зарегистрировать служебную информацию – мнемоническое имя формы, адрес и, опционально, набор передаваемых и возвращаемых значений.

✓ Интеграция с передачей параметров бизнес-процессов

Дополнительно требуется описать правила получения и преобразования типовых параметров для каждой связки приложений и создать интеграционные скрипты на языке программирования JavaScript для передачи параметров между вызываемыми формами.

✓ Полная интеграция внешних форм (WebX)

Может понадобиться в случае необходимости передачи дополнительных параметров в другие приложения, которые не могут быть переданы без изменения кода формы.

Интеграция на основе WebX

WebX представляет собой технологию работы Web-форм, регламентирующую способ оформления их программного интерфейса.



В настоящее время:

- ✓ Описания интерфейсов (API)
- ✓ Механизмы запуска WebX-форм (включая внешние)
- ✓ Различные инициаторы запуска
- ✓ Работа с несколькими рабочими областями
- ✓ Обмена параметров бизнес-процессов между формами

Интегрируемые партнерские web-приложения: редактирование параметров

Создать пользователя

Управление сервером

Статистика

Смена пароля
пользователя

Контрольные вопросы

Разблокирование
IP-адреса

Уровни доступа

Внешние системы

Операции

Синхронизация

Работа со словарем
фраз

Учет событий

- Список типов
событий

- Список типов
изменений

- Настройка учета
для истории
операций

- Настройка учета
для SMS
оповещения

USSD & SMS

- Номера сервисных
служб

- Правила
маршрутизации и
формирования
ответов

Режим администратора

Редактирование внешней системы

Идентификатор системы:

Название:

Порядок сортировки
закладки:

IP адрес и порт: :

Редактирование
параметров внешней
системы в интерфейсе
администратора

подстановку {MSISDN}
телефона абонента

подстановку {MSISDN}
телефона абонента

ON_ID. Введенное

в раздел <HEAD>

css">

Введенный текст будет вставляться в каждый документ полученный от внешней системы в раздел <HEAD>

Кодировка:

* - устаревшие поля (оставлены для совместимости).

[← Вернуться назад](#)

[Изменить →](#)

Пример подключения партнерских web-приложений

Раздел «Маркетинговые кампании» в Управление каналами доставки маркетинговых предложений



Сервис-Гид
Система самообслуживания абонентов

GUP

Абонент: 9029300588

Список маркетинговых
предложений

Управление каналами доставки маркетинговых предложений:

Вы можете ограничить список каналов, по которым осуществляется информирование Вас о новых маркетинговых предложениях. Для этого отметьте каналы, по которым Вы не хотите получать сведения о новых маркетинговых предложениях, и нажмите на кнопку **Сохранить**

Услуга управления каналами доставки маркетинговых предложений:

Запрещенные каналы доставки маркетинговых предложений:

- SMS
- EMAIL
- DMAIL
- Телефон
- Все каналы

Сохранить

Отмена

Отписаться

Пример подключения партнерских web-приложений

Раздел «Пополнение счета банковской картой» в Сервис-Гид



Сервис-Гид
Система самообслуживания абонентов

→ Пополнить счет «МегаФон»

[Пополнить свой счёт](#)
[Пополнить счёт другого абонента](#)
[Автоматическое пополнение счёта](#)

→ Работа с банковскими картами

[Регистрация банковской карты](#)
[Зарегистрированные карты](#)
[Выбрать активную](#)
[История платежей](#)
[Удалить](#)

→ Управление защитными кодами

[Восстановить код](#)
[Изменить код](#)

→ Помощь

[Об услуге](#)
[Условия предоставления услуги](#)
[О регистрации банковской карты](#)
[Об оплате счёта](#)
[Вопросы и ответы](#)

ВОЗМОЖНОСТИ УСЛУГИ



→ Пополнить свой
лицевой счет



→ Пополнить счет
другого абонента



→ Подключить автоматическое
пополнение счета

КАРТЫ

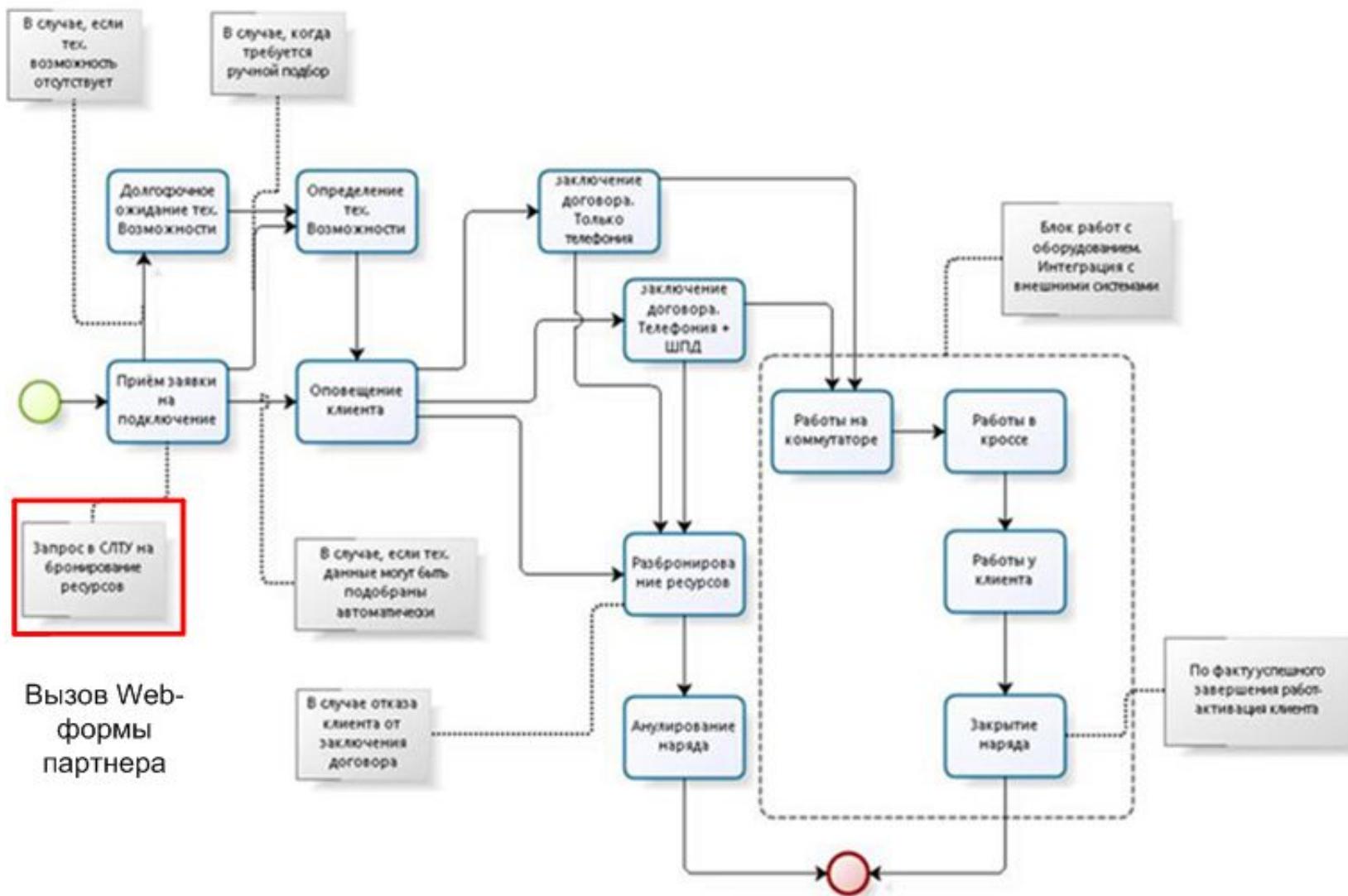


[Ваши
зарегистрированные
карты](#)



[Зарегистрировать
карту](#)

Конструирование бизнес-процессов



Бизнес–процессы облегчают жизнь

Обращения клиентов

РЕГИСТРАЦИЯ ОБРАЩЕНИЯ

Обращение | Контакт и клиент | Файлы

Регистрационный №: _____ Абонент: Не выбран

Тема: 1 Дилерский портал/Дилерский портал. Миграция физического лица.

Тип клиента (физ./юр.)	Физическое лицо
* Номер абонента	+7952
* Серия паспорта абонента	
* Номер паспорта абонента	

Описание: _____

Подсказка оператору

Для начала процесса миграции:

1. Отправьте с телефона Абонента USSD запрос на номер *777#.
2. Если миграция запрещена, объясните Абоненту причину, а также предложите ему обратиться в ЦОА для регистрации письменного заявления для решения данного вопроса. Если миграция запрещена по причине низкого уровня ARPU, абонент имеет право мигрировать на лицевой счет юридического лица.
3. Если миграция разрешена, расскажите Абоненту об условиях миграции и предупредите Его о том, что услуги "Всегда вместе" и "Любимые номера" не всегда сохранятся при переходе на контракт.
4. Если Абонент согласен с условиями перехода на контракт, начните процедуру. Для этого выберите Тему обращения: процедуру: "Дилерский портал. Миграция физического лица" или "Дилерский портал. Миграция юридического лица".
5. Далее введите Номер его телефона в формате: 952000000000 и все остальные поля, помеченные звездочкой (*).
6. После внесения данных нажмите кнопку "Сохранить".
7. После сохранения "Обработка..." --> "Далее...".

В поле "Описание" Вы увидите результат проверки.

больше не показывать

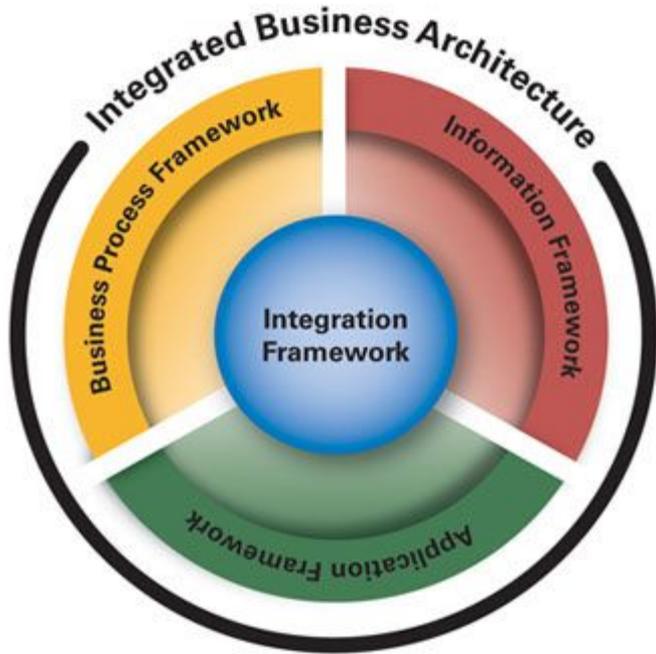
Планир. окончание: 01.01.2099 00:00:00 Приоритет: Высокий

Дата закрытия: _____

К контакту (отмена изменений) | Обработка... | Сохранить

Copyright © 2003-2008 ЗАО ПИТЕР-СЕРВИС

tmforum Framework



Customer Management
Service Management
Resource Management
Supplier/Partner
Management

Enterprise Management
Security Management

Заключение

- Выполнение требований ФЗ № 152 «О персональных данных» (HASAM)
- Единые окно Web-приложений с механизмами единой аутентификацию, авторизацию и аудита
- Проработанные механизмы интеграции (WebX)
- Открытые интерфейсы взаимодействия (API)
- Поддержка механизмов построения бизнес–процессов (WorkFlow)



Спасибо за внимание !

Денис Александров

Ведущий инженер

E-mail: Denis.Alexandrov@billing.ru

URL: <http://www.billing.ru>