Региональный форум МСЭ по развитию для стран СНГ и Грузии

Кишинев, Республика Молдова
31 марта – 01 апреля 2015 г.

Отчет о проведении региональной инициативы СНГ “Разработка рекомендаций и создание пилотного фрагмента системы электросвязи/ИКТ для поддержки защищенных удаленных розничных платежей и управления банковскими счетами на основе беспроводных сетей связи“

Евгений Бондаренко
Вице-председатель ИК2 МСЭ-D
Зам. Генерального директора ЗАО «Интервэйл»
E-mail: bond@intervale.ru

Вадим Каптур
Вице-председатель ИК1 МСЭ-D
проректор по научной работе ОНАС им. А.С. Попова
E-mail: vadim.kaptur@onat.edu.ua

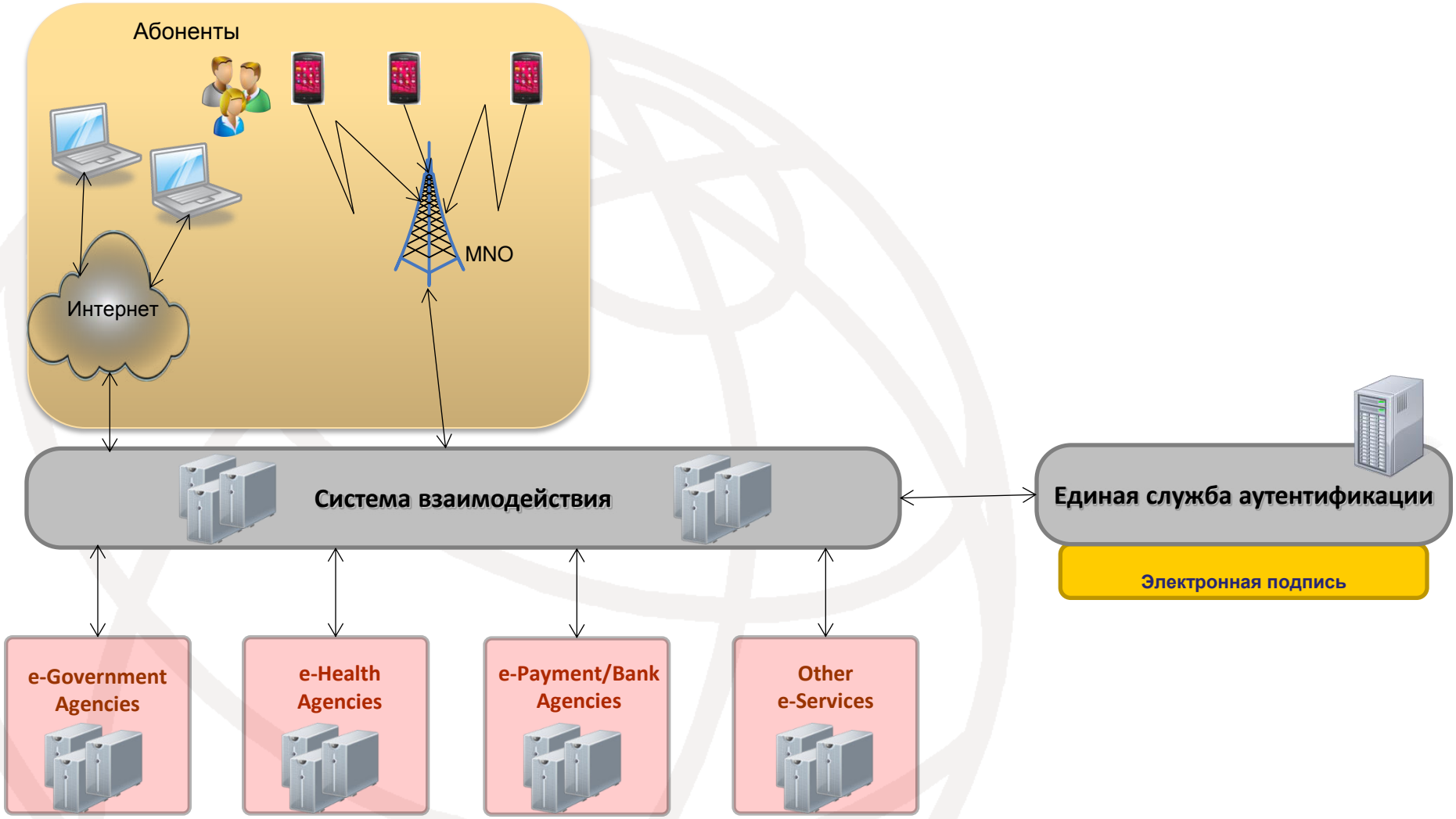
Особенности мобильных платежей

- Высокий уровень проникновения мобильной связи
- Доступность услуги в любое время в любом месте
- Удобный инструмент проведения бесконтактных платежей
- Возможность обеспечить высокий уровень безопасности
- Совместимость как с существующей платежной инфраструктурой, так и с инновационными системами платежей
- Логичное направление развития международных и локальных карточных платёжных систем
- Возможность инициирования финансовых транзакций как плательщиком, так и получателем (торгово-сервисным предприятием)
- Разнообразные средства платежа

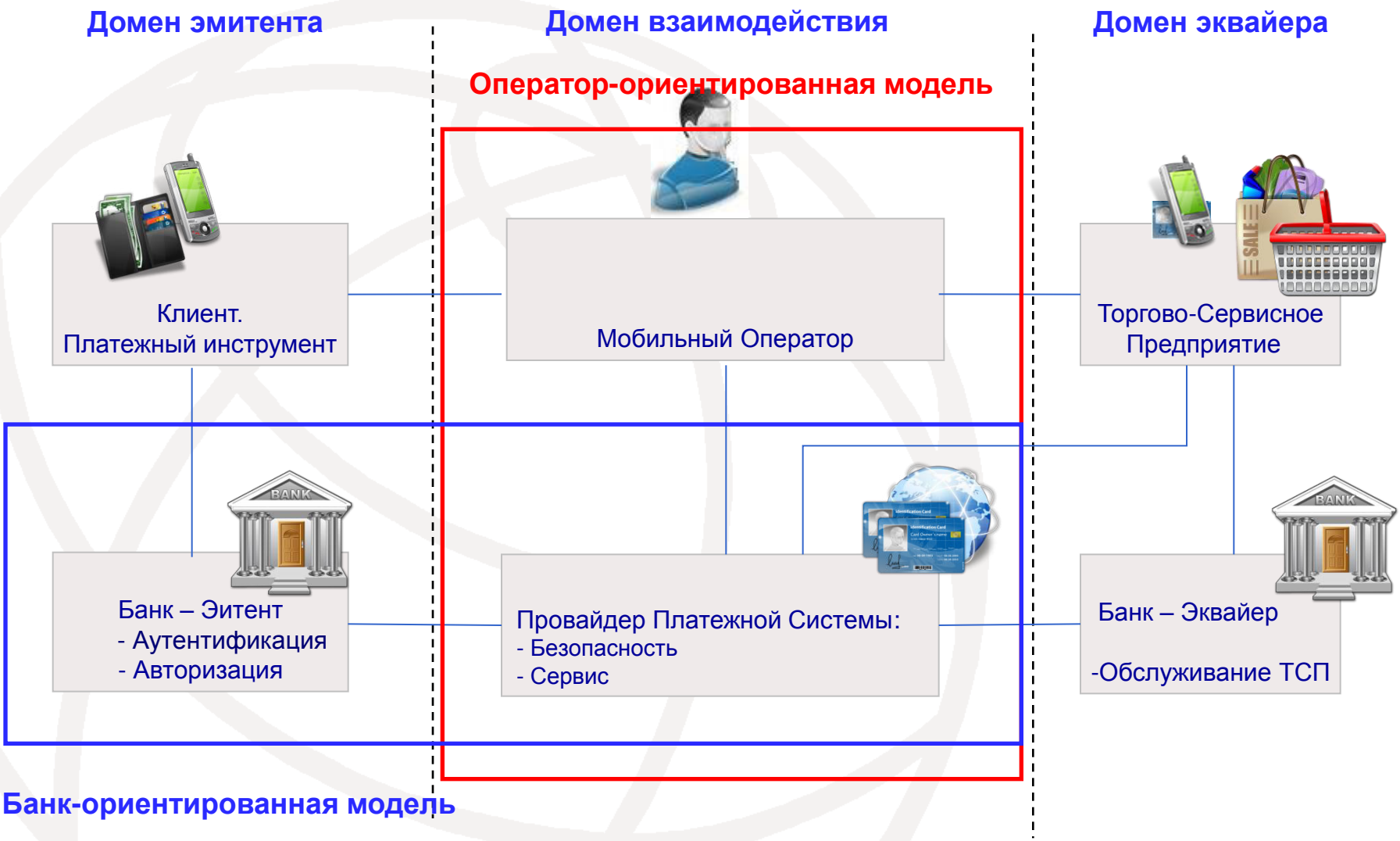
Сдерживающие факторы

- Консерватизм в поведении потенциальных пользователей
- Недоверие к безопасности мобильной связи
- Недостаточная распространенность компьютерной грамотности населения
- Сегодняшние мобильные устройства не были задуманы для обеспечения защищенных операций
- Неудобная клавиатура и маленький дисплей большинства мобильных устройств – непривычная эргономика
- Ситуация в различных регионах сильно различается – не существует единого решения
- Оптимальные решения еще не найдены

Система с единой службой аутентификации



Архитектура мобильной платежной системы



Рекомендация МСЭ-Т Y.2741

Множество вариантов реализации

Реализация сервиса:

- **На базе стандартных услуг мобильного оператора**
- **На базе специализированных приложений**
  - на SIM-карте.
  - на SD-карте
  - на встроенном SE
  - в памяти телефона

Безопасность:

- Аутентификация
- Шифрование
- Элемент безопасности
- TEE
- Облачное хранение

Технология коммуникации:

- SMS
- USSD
- GPRS
- EDGE
- UMTS
- DTMF
- Voice
- NFC
- Blue Tooth
- QR

Выбор оптимального решения

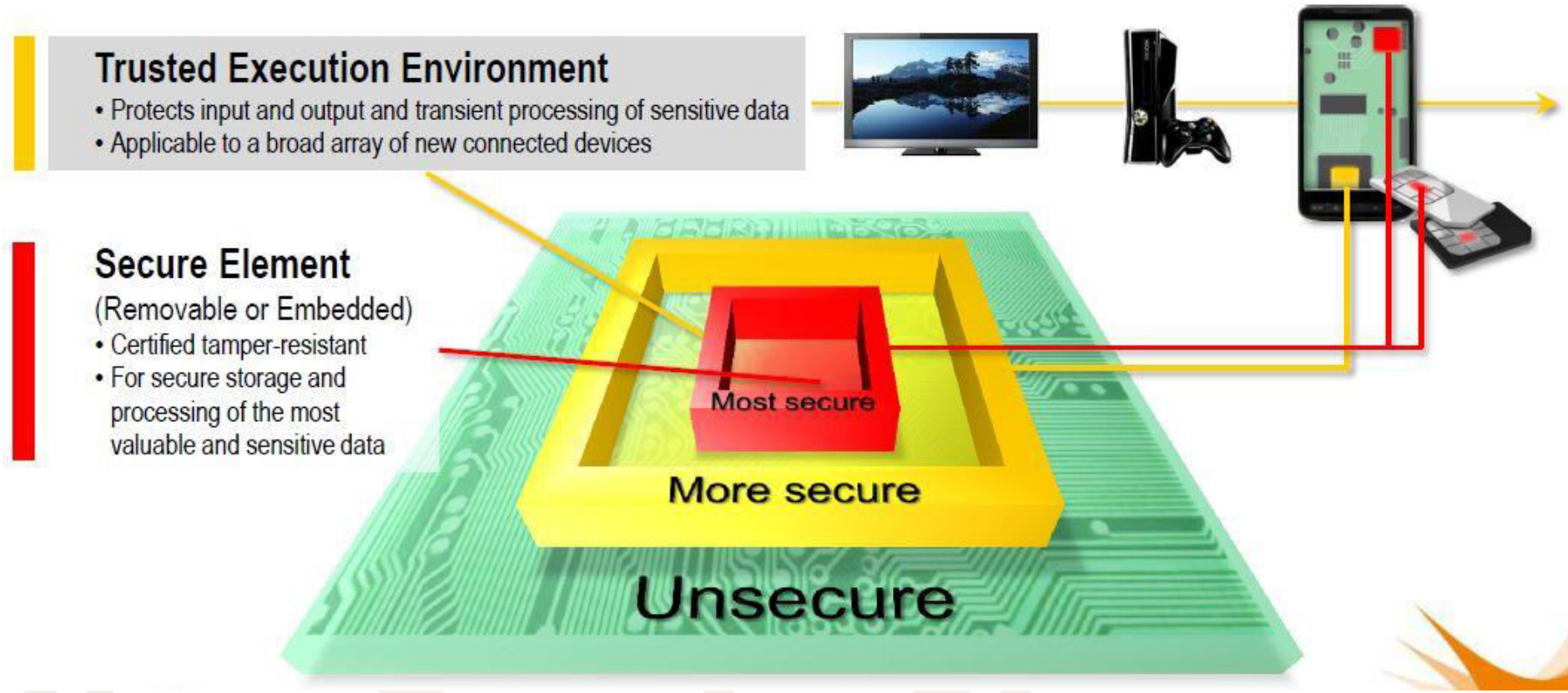
		Средство платежа				
		Bank account	Payment card	MNO account	e-money account	Other accounts
Техническая реализация	WEB	**	*		*	*
	SMS/USSD	*	*	**	*	*
	Voice	*	*			*
	Application	***	***	***	***	***

Четыре уровня защищенности Мобильной Платежной Системы

- Level 1: Защищенность обеспечивается средствами оператора связи
- Level 2: МПС использует однофакторную аутентификацию
- Level 3: Многофакторная аутентификация, шифрование данных
- Level 4: Дополнительно к средствам, перечисленным в Level 3 используется SE/TEE

Рекомендация МСЭ-Т Y.2740

Доверенная Среда Исполнения (TEE)



Host Card Emulation (HCE) - система с облачным хранением данных

- Без аппаратного элемента безопасности
  - Cloud-based solution
  - Tokens-based solution
- Гибридное решение (Cloud+SE)

Рекомендации в области законодательных и регуляторных аспектов

- Отметить необходимость разработки модельного нормативно-правового акта по мобильным платежам, определяющего правовые, регуляторные, технологические и бизнес аспекты данного вида деятельности.
- Обратить внимание участников глобального финансового рынка, в частности, международных платежных систем, на целесообразность своевременной адаптации стандартов финансовых сервисов для применения в индустрии мобильных платежей.
- Признать целесообразность создания в регионе СНГ консультационно-совещательного органа в области мобильных платежей и мобильной коммерции, формирующего принципы и рекомендации для участников рынка различных стран.

Рекомендации в области практики ведения бизнеса

- Следовать принципу «Комфорт клиента не в ущерб безопасности» при разработке и продвижении систем мобильных платежей.
- Стимулировать использование мобильных платежей для осуществления наиболее массовых финансовых операций (оплата налогов, госуслуг и ЖКХ) с целью популяризации мобильных технологий в интересах потребителей и государства.
- Отметить необходимость системного подхода к повышению финансовой грамотности и осведомленности населения об основополагающих принципах технологии мобильных платежей. Продолжить практику разработки и проведения специальных маркетинговых мероприятий, направленных как на популяризацию сервисов мобильных платежей, так и на повышение финансовой грамотности населения на локальных рынках.

Рекомендации в области развития технологий

- Применять многофакторную аутентификацию и стойкие криптографические алгоритмы для аутентификации клиентов и авторизации операций. Отметить необходимость хранения критических данных, используемых для аутентификации клиентов, отдельно от платежных реквизитов и другой финансовой информации.
- Признать перспективность применения средств биометрической аутентификации клиентов в индустрии мобильных платежей.
- Отметить перспективность перехода к использованию современных методов обеспечения защиты платежных реквизитов, в том числе различных вариантов реализации элементов безопасности (secure element), доверенной среды (TEE), технологии “Host Card Emulation” (HCE) и токенизации для обеспечения должного уровня безопасности мобильных платежей.

Курс лекций и рекомендации по организации лабораторного цикла по предмету «ПРОЕКТИРОВАНИЕ, ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПЛАТЁЖНЫХ СИСТЕМ»

Структура курса

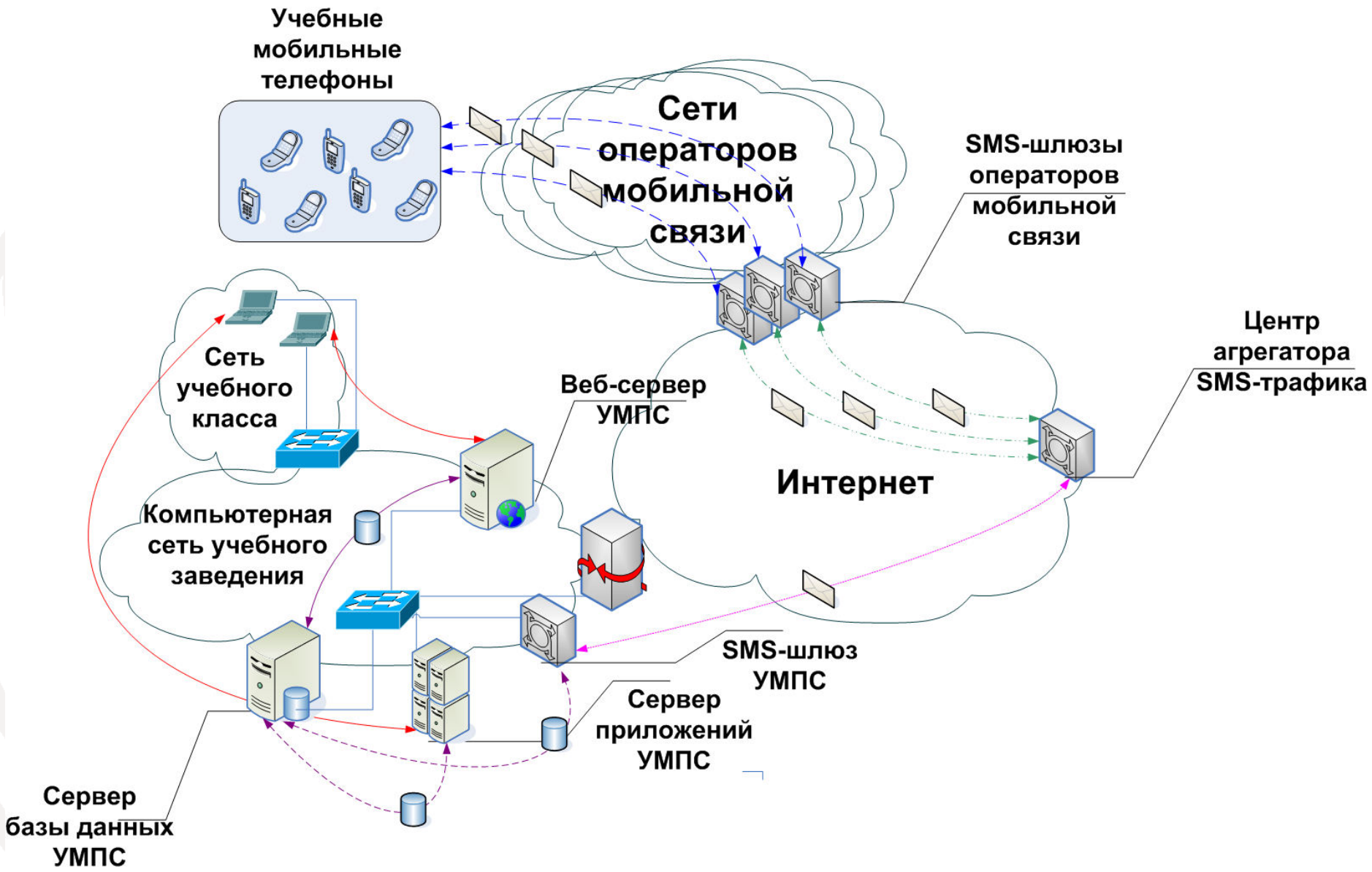
Часть 1. История развития и ключевые понятия мобильных платёжных систем

Лекция 1. **История развития мобильных платёжных систем и их роль в современном мире**
Лекция 2. **Классификация мобильных платёжных систем**
Лекция 3. **Архитектурные модели и общие принципы работы мобильных платёжных систем**
Лекция 4. **Сценарии использования мобильных платёжных систем**
Лекция 5. **Ключевые принципы обеспечения безопасности мобильных платёжных систем**

Часть 2. Технологии построения, методы проектирования и обслуживания мобильных платёжных систем

Лекция 6. **Протоколы и телекоммуникационные механизмы, применяемые для реализации мобильных платёжных систем**
Лекция 7. **Методы проектирования современных мобильных платёжных систем**
Лекция 8. **Особенности организации системы технической эксплуатации мобильных платёжных систем**
Лекция 9. **Существующие технические решения мобильных платёжных систем**

Архитектура учебной мобильной платёжной системы



Возможные сценарии лабораторных работ

Лабораторная работа 1. Регистрация клиента в системе мобильных платежей

Цель работы: Ознакомление с принципами реализации сценариев регистрации клиента и платёжного инструмента в системе мобильных платежей согласно Рекомендации МСЭ-Т Y.2741.

Лабораторная работа 2. Осуществление финансовых операций Клиентом

Цель работы: Ознакомление с принципами реализации сценария осуществления клиентом финансовых операций в рамках собственной системы платежей согласно Рекомендации МСЭ-Т Y.2741.

Лабораторная работа 3. Осуществление финансовых операций Предприятием

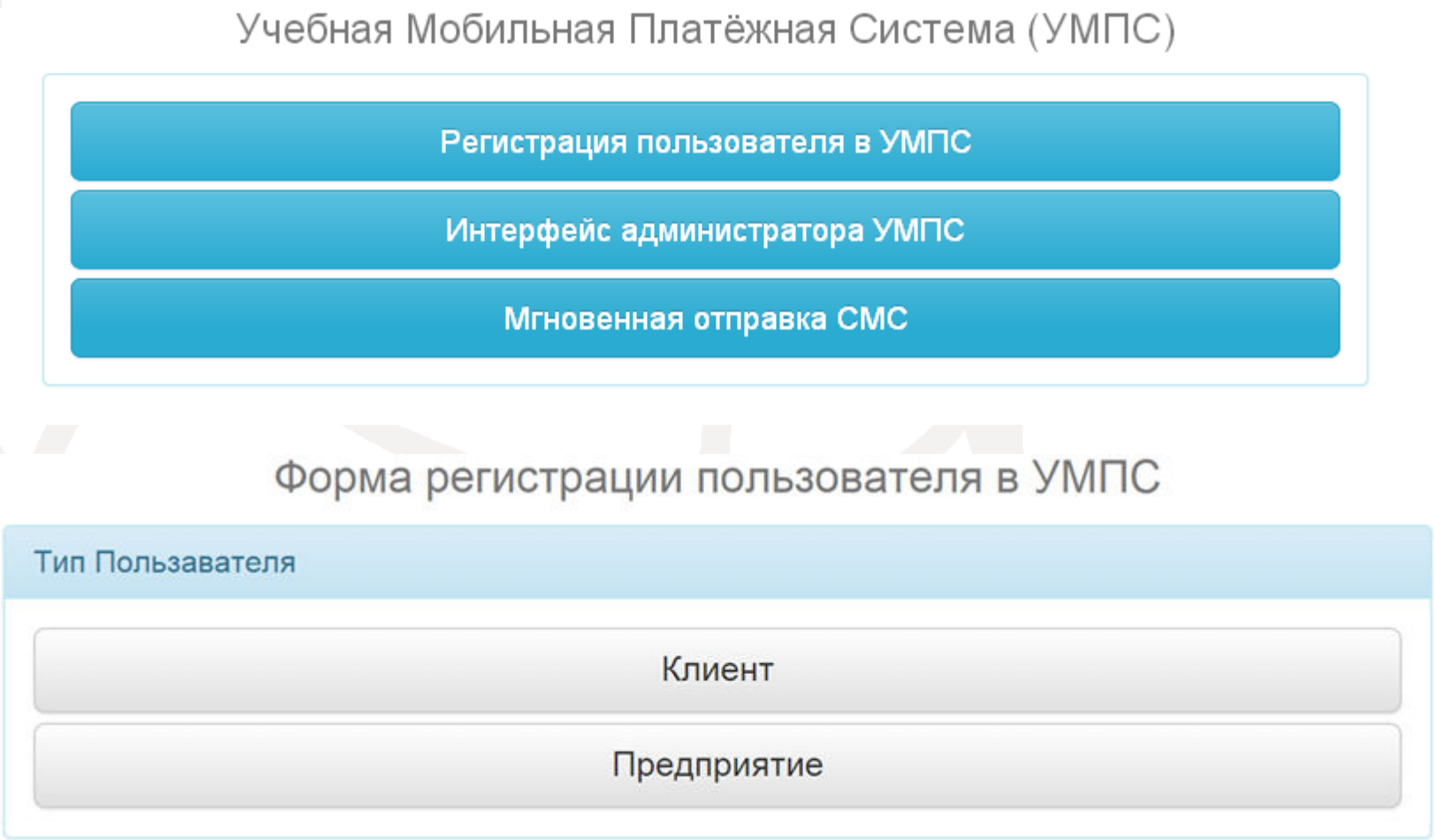
Цель работы: Ознакомление с принципами реализации альтернативных сценариев (выставление счёта Предприятием, перевод средств) осуществления финансовой операции, а также закрепление изучения сценариев, регламентированных Рекомендацией МСЭ-Т Y.2741.

Лабораторная работа 4. Отключение платёжного инструмента в системе мобильных платежей

Цель работы: Ознакомление с принципами реализации сценариев удаления платёжных инструментов и пользователей из мобильной платёжной системы (согласно с Рекомендацией МСЭ-Т Y.2741).

Программная реализация лабораторного цикла

http://mobile-banking.onat.edu.ua



Программная реализация лабораторного цикла

Административный интерфейс для лабораторного цикла по предмету
"ПРОЕКТИРОВАНИЕ, ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПЛАТЁЖНЫХ СИСТЕМ"

Клиенты, Счета и Услуги | SMS и Транзакции

SMS и Состояния

ID	Номер Телефона	Текст SMS	Статус
310758	+380682595559	Kod podtverzhdenyia operatsyy: 43-51-67	исходящее /не обработано
310757	+380681234567	Kod podtverzhdenyia operatsyy: 36-43-27	исходящее /не обработано
310756	+380582595559	Schet 1300 podtverzhden	исходящее /не обработано
310755	+380582595559	CONF#CF94-68-98	входящее /обработано
310754	+380582595559	Kod podtverzhdenyia operatsyy: 94-68-98	исходящее /не обработано
310753	+380582595559	Klyent 140 podtverzhden	исходящее /не обработано
310752	+380582595559	CONF#CF63-26-23	входящее /обработано

Стр. 1 из 12 430 | 10 | Просмотр 1 - 25 из 310 750

Транзакции

ID	Клиент	Номер С	Тип Транзакции	Дата и Время	Сумма	Подтверждение	Дополнительная Ин
43	+380682595559	1310	2 - регистрация нового счёта	2014-09-24T17:21:20.367Z	0	Ожидает (43-51-67, клиенты:	
42	+380681234567		1 - регистрация нового клиен	2014-09-24T17:20:19.360Z	0	Ожидает (36-43-27, клиенты:	
41	+380582595559	1300	2 - регистрация нового счёта	2014-09-23T21:23:16.904Z	0	Выполнено (94-68-98)	
40	+380582595559		1 - регистрация нового клиен	2014-09-23T21:21:29.309Z	0	Выполнено (63-26-23)	
39	+380933647777	1290	3 - добавление средств к счёт	2014-09-23T10:28:03.631Z	100	Выполнено (18-69-10)	Средства по счету за
38	+380682595559	1000	4 - снятие средств со счёта	2014-09-23T10:28:03.628Z	-100	Выполнено (18-69-10)	Оплата счета товара
37	+380933647777	1290	3 - добавление средств к счёт	2014-09-23T10:09:43.517Z	100	Выполнено (92-35-95)	Средства по счету за

Стр. 1 из 5 | 10 | Просмотр 1 - 10 из 44

Региональный семинар МСЭ для стран СНГ
“Мобильные платежи: проблемы и перспективы развития”
Баку, Азербайджан, 14-16 октября 2014 года

THE REPUBLIC OF AZERBAIJAN
MINISTRY OF COMMUNICATIONS
AND HIGH TECHNOLOGIES

INTERVALE

68 участников из 14 стран

Резюме

1) Семинар продемонстрировал актуальность тематики мобильных платежей и большой интерес к ней как со стороны банков, так и со стороны телеком операторов.

2) Представляется целесообразным проведение подобных семинаров на систематической основе в разных странах с участием местных телекоммуникационных и банковских организаций.

3) Заинтересованным ведомствам и операторам рекомендуется принять участие в работе недавно созданной группы МСЭ-Т FG DFS, которая в настоящее время обобщает имеющийся опыт, лучшие практики и стандарты в этой области, имеющиеся в различных международных организациях и регионах.

СПАСИБО !

Реализация уровней безопасности

<table>
<tr><th rowspan="2">Измерение защиты</th><th colspan="4">Уровень безопасности</th></tr>
<tr><th>1-й уровень</th><th>2-й уровень</th><th>3-й уровень</th><th>4-й уровень</th></tr>
<tr><td>Управление доступом</td><td colspan="4">Доступ к каждому из компонентов, входящих в инфраструктуру системы должен быть разрешен только в соответствии с уровнем полномочий персонала или пользователей системы.</td></tr>
<tr><td>Аутентификация</td><td>Аутентификация в Системе обеспечивается средой передачи данных мобильного оператора</td><td>Однофакторная аутентификация при использовании услуг Системы</td><td>Многофакторная аутентификация при использовании услуг Системы</td><td>Персональное подключение к услугам с предоставлением персональных данных, с обязательной аутентификацией личности. Многофакторная аутентификация при использовании услуг Системы. Обязательное применение аппаратного криптографического модуля</td></tr>
<tr><td>Неотказуемость (сохранность информации)</td><td colspan="4">Невозможность инициатору или участнику транзакции отказаться от своих действий после их совершения обеспечивается применением юридически закрепленных либо оговоренных во взаимных контрактах способов и совместно с принятыми механизмами аутентификации. Все действия системы персонала и пользователей системы должны подвергаться обязательной регистрации. Журналы регистрации событий должны быть защищены от изменений и содержать действия всех пользователей.</td></tr>
<tr><td>Конфиденциальность данных</td><td colspan="2" rowspan="2">При передаче обеспечивается средой передачи данных (безопасность связи), а при хранении и обработке данных - механизмом хранения данных и средствами по управлению доступом в Системе</td><td rowspan="3">При передаче сообщений должны обеспечиваться применением дополнительного шифрования сообщения, и применение протоколов передачи данных, обеспечивающих защиту информации, передаваемой участниками взаимоотношений (включая проверку целостности передаваемой информации); при хранении и обработке данных - дополнительными механизмами шифрованием и маскированием данных при их хранении и четким разграничением доступа в соответствии со служебными полномочиями</td><td rowspan="3">Выполнение требований 3го уровня с обязательным применением аппаратных средства шифрования и защиты информации на стороне Клиента</td></tr>
<tr><td>Целостность данных</td></tr>
<tr><td>Защита персональной информации</td><td colspan="2">Гарантируется отсутствием в передаваемых сообщениях sensitive data, и реализацией необходимых механизмов хранения данных и средствами по управлению доступом в Системе. Компоненты системы не должны иметь скрытых возможностей по несанкционированному сбору и передачи информации.</td></tr>
<tr><td>Безопасность связи</td><td colspan="4">Гарантируется доставка сообщения адресату и защиту информации от несанкционированного просмотра при передаче по каналам связи. Обеспечивается провайдерами сети мобильного оператора.</td></tr>
<tr><td>Доступность</td><td colspan="4">Гарантирует отсутствие препятствий для доступа к данным и услугам системы со стороны авторизованных и уполномоченных пользователей системы. Обеспечивается провайдерами сети мобильной связи и провайдерами услуги.</td></tr>
</table>

Рекомендация МСЭ Y.2740

Спецификация команд учебной мобильной платёжной системы