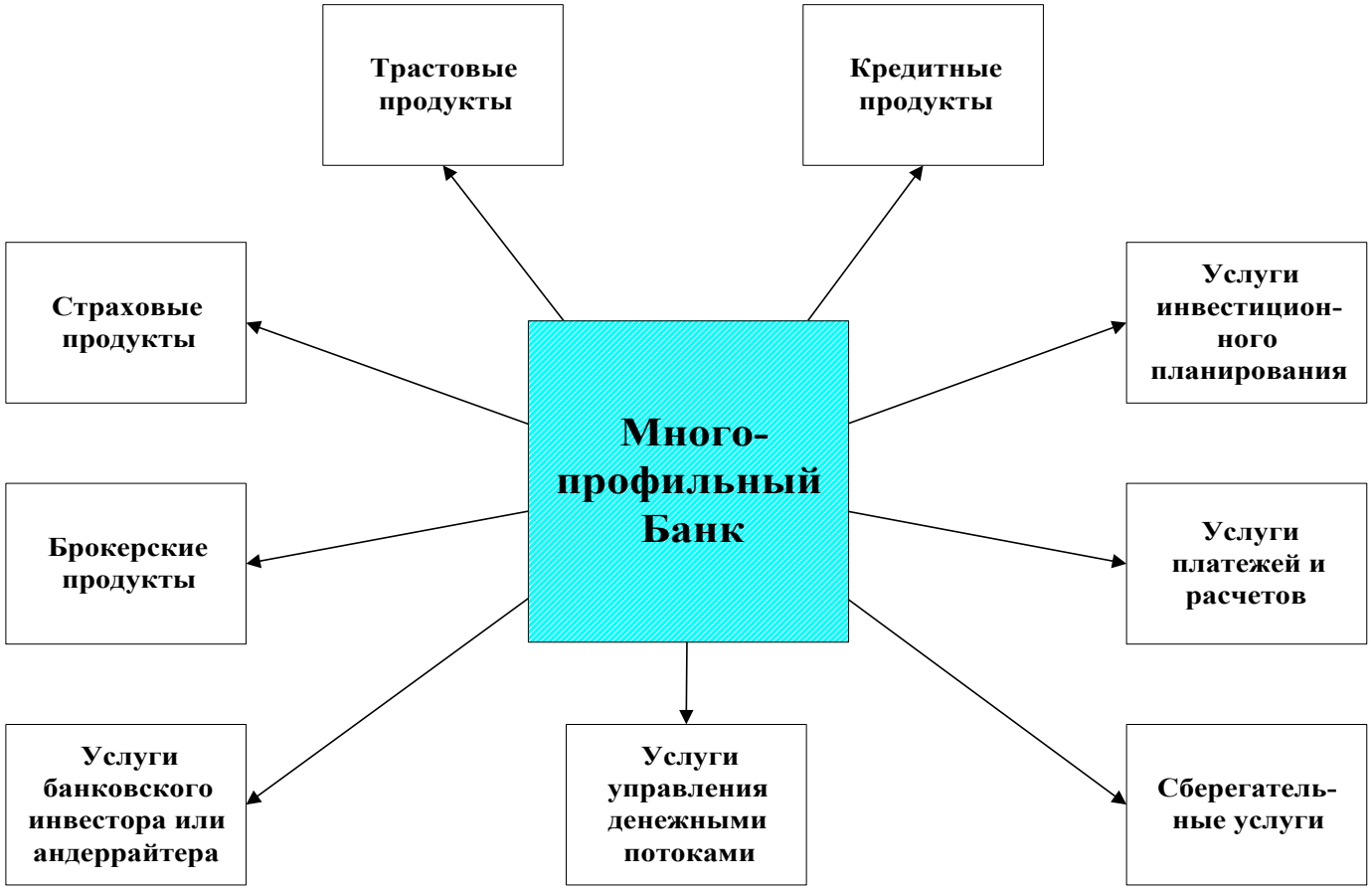
Система безопасности акционерного банка «Инвестиционно-банковская группа НИКойл»

кандидат технических наук,
заместитель начальника службы внутреннего котроля
Ануфриев Владимир Натанович

главный специалист службы содействия бизнесу
Калинсков Игорь Николаевич

АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ДЛЯ ФИНАНСОВОЙ КОРПОРАЦИИ 5



Устойчивая тенденция развития электронных каналов продаж +

Широкое распространение сети Internet

Совершенствование систем безопасности

МОДЕЛЬ ПРИКЛАДНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Руководство

Управленческие решения

Системы поддержки принятия решений

Система документооборота	Хранилище данных	Система технологического учета

Системы оперативного учета (backoffice)

Автоматизированный фронт-офис

Информация

Клиент

Клиент

Клиент

Клиент

ИНТЕГРИРОВАННЫЙ ЭЛЕКТРОННЫЙ ФРОНТ-ОФИС НИКОЙЛ 5

⇒ система удаленного управления клиентскими банковскими счетами

⇒ система удаленного управления клиентскими счетами через Интернет для частных лиц

⇒ система интернет-доступа к финансовым рынкам

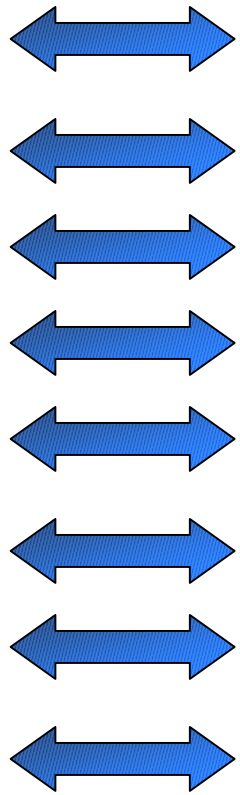
⇒ система удаленного получения отчетов о факторинговых операциях

⇒ система поддержки удаленного торгового интернет-терминала ММВБ

⇒ система электронного документооборота на электронных торговых площадках

⇒ электронная система продаж паев паевых инвестиционных фондов

⇒ система удаленного управления счетами-депо



ИНТЕГРИРОВАННЫЙ БЭКОФИС

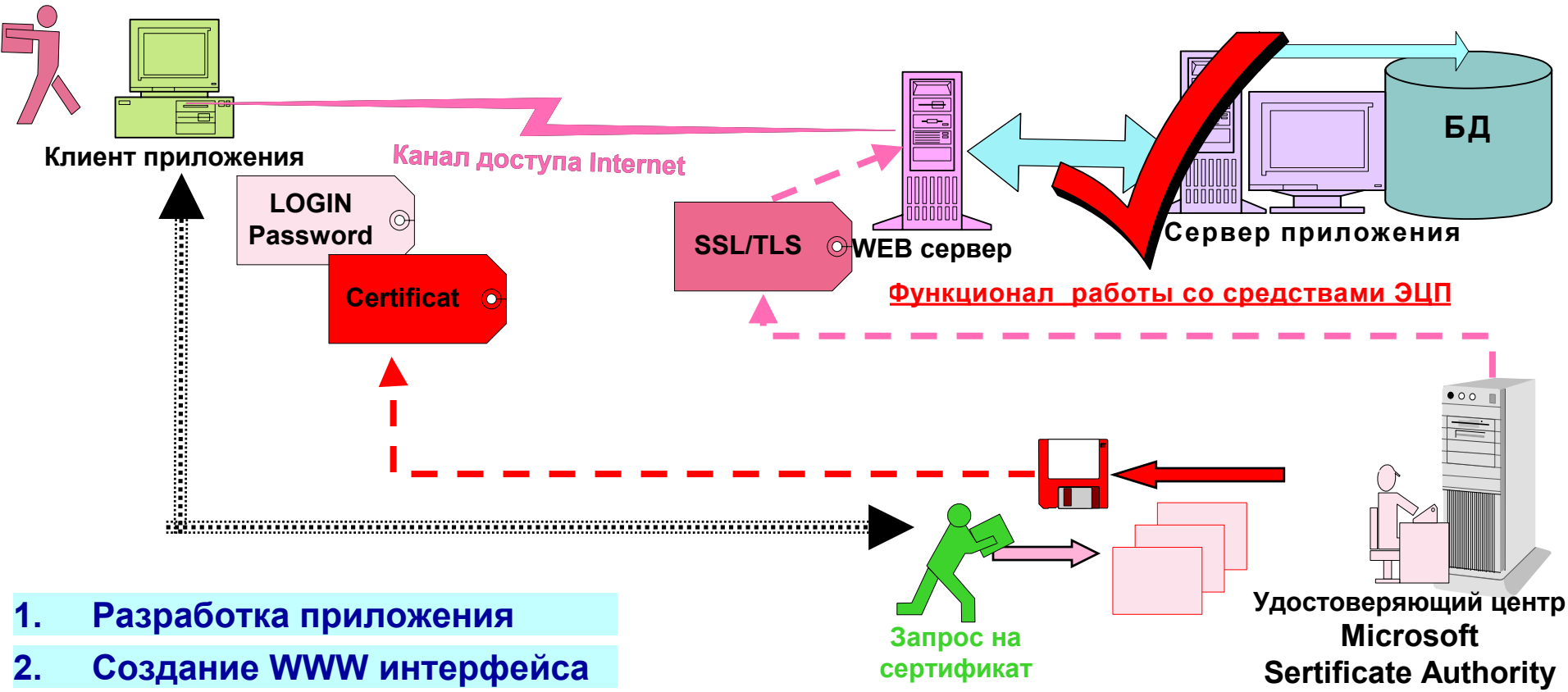
Система безопасности:

- авторизация и аутентификация
- защита от несанкционированного доступа, закрытие каналов передачи данных
- обеспечение целостности и актуальности данных при обмене с клиентами
- обеспечение юридической значимости электронных документов
- снижение риска возникновения и разбор конфликтных ситуаций

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - КОМПЛЕКСНАЯ ПРОБЛЕМА 5

- **административные мероприятия** (подбор и расстановка кадров, распределение зон ответственности, подчиненность, контроль исполнительской дисциплины)
- **технологические мероприятия** (политика информационно безопасности, инструкции, регламенты, обучение персонала и клиентов)
- **юридические мероприятия** (типовые договоры с клиентами, должностные инструкции и трудовые контракты)
- **технические мероприятия** (программные решения, аппаратные решения, администрирование систем)
- **управление рисками** (предотвращение и разбор конфликтных ситуаций)

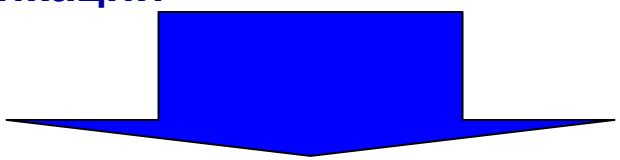
Типовой подход к построению и защите WWW приложений



1. Разработка приложения
2. Создание WWW интерфейса
3. Организация и развёртывание Public Key Infrastructure
4. Подключение клиентов:
   - Включение средств защиты от НСД
   - Включение средств аутентификации клиента
5. Разработка и встраивание средств ЭЦП
6. Регистрация клиента в удостоверяющем центре

НЕДОСТАТКИ ТИПОВОГО ПОДХОДА

- Каждое приложение порождает свой удостоверяющий центр (УЦ)
- Для каждого УЦ требуются:
  - своя политика работы с сертификатами
  - отдельные ресурсы для администрирования
- Некоторые необходимые сервисы не разрабатываются:
  - средства интерактивной регистрации и поддержки плановых регламентных работ с сертификатами
  - средства для работы с EKU (Enhanced Key Usage)
  - настройка системной роли сертификата в приложении
- Клиенты вынуждены иметь свою пару секретный ключ/сертификат для работы с каждым приложением и не забывать о плановой смене каждого сертификата по специальной процедуре
- Для каждой платформы сервера приложений необходимо разрабатывать уникальное программное обеспечение для поддержки ЭЦП и ключей аутентификации



⇒ Увеличение общей стоимости владения системой

⇒ Рост рисков нарушения системы безопасности

ТРЕБОВАНИЯ К СИСТЕМЕ БЕЗОПАСНОСТИ

	I. Требования бизнеса	II. Требования службы информационной безопасности	III. Общие требования
1	общая клиентская база всех приложений электронного фронт офиса	двусторонняя аутентификация клиентов и серверов приложений с использованием криптографических процедур	минимальная общая стоимость владения системой
2	однократная регистрация клиента в системе безопасности	защита трафика с использованием криптографических процедур	открытые интерфейсы для прикладных программ
3	однотипные и максимально удобные для клиента процедуры регистрации и смены ключей, возможность самостоятельной генерации ключей клиентом	секретный ключ клиента должен обладать сертифицированной криптостойкостью и использоваться как для клиентской аутентификации, так и для формирования ЭЦП под электронным документом	независимость системы безопасности от платформ разработки и среды времени выполнения фронт офисных приложений
4	один сертификат и секретный ключ у клиента для работы со всеми электронным приложениям фронт офиса	средства ЭЦП в соответствии с положениями Федерального Закона «Об электронной цифровой подписи»	средства безопасности на стороне клиента должны поддерживать концепцию «тонкого клиента»
5	типовые, юридически корректные процедуры для разбора конфликтных ситуаций	Поддержка Public Key Infrastructure, поддержка сертификата стандарта X.509 v3	
6	поддержка массовых обращений клиентов	развитая система администрирования	Репутация поставщика решения и его готовность к заказным доработкам по отдельным техническим заданиям
7		протоколирование событий и средства анализа журналов событий	

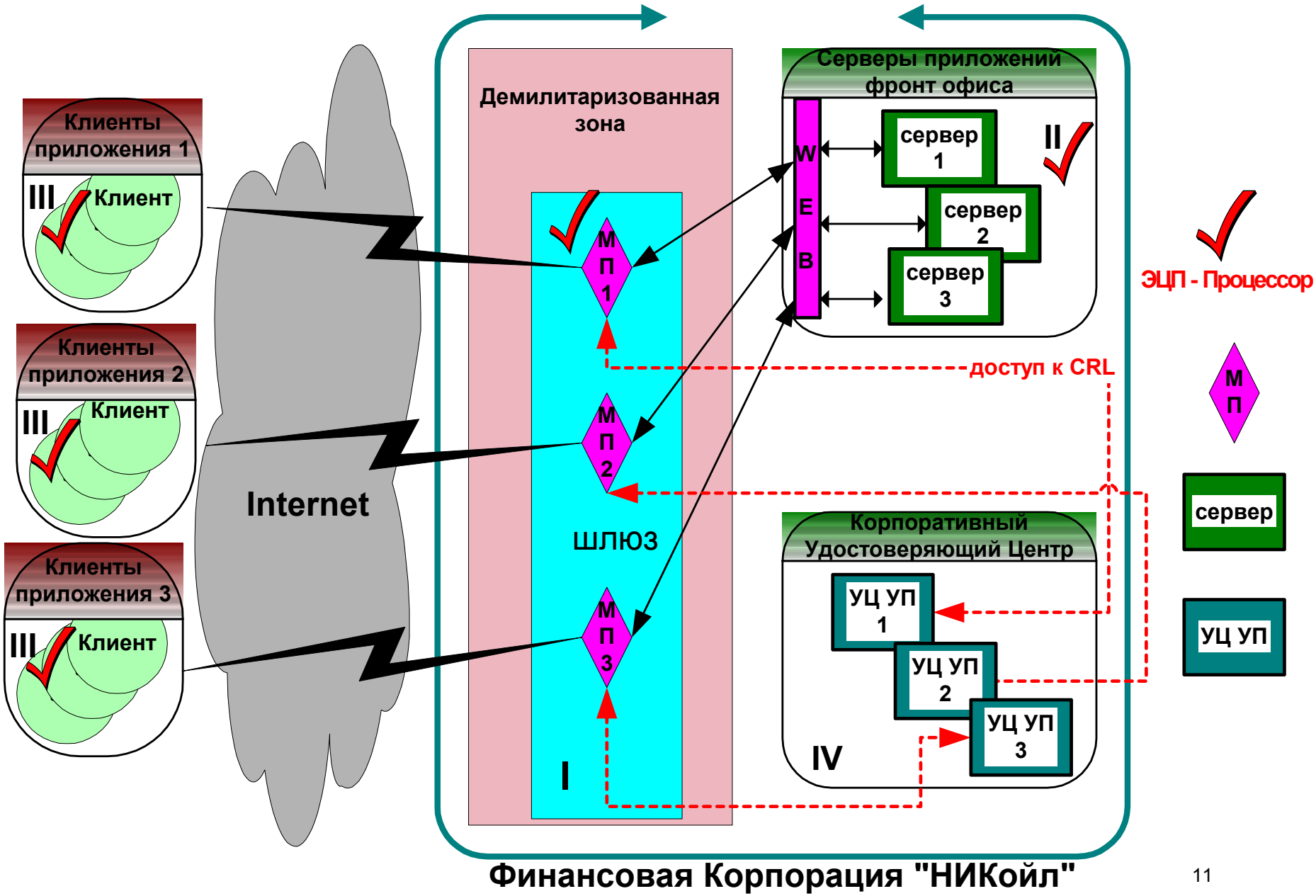
АЛЬТЕРНАТИВНЫЕ РЕШЕНИЯ

№ п/п	Наименование средства	Назначение	Поставщик
1	“Верба-OW” “ЯНТАРЬ АСБР” “Система криптографической авторизации электронных документов “Сигнатура”	Программное средство шифрования, имитозащиты и ЭЦП Программные комплексы защиты информации в автоматизированной системе банковских расчетов (шифрование, имитозащита, ЭЦП).	ЗАО МО ПНИЭИ
2	“Базис-защита”	Программная библиотека защиты информации (шифрование, ЭЦП)	ЗАО “АНКОРТ”
3	“Криптон-Подпись”	Аппаратно-программное средство шифрования данных, обеспечения целостности и подлинности информации, формирования ключей шифрования и ЭЦП	ООО Фирма “Анкад”
4	“Крипто-КОМ 3.0” “Message PRO” “Data PRO”	Аппаратно-программное средство генерации ключей шифрования и ЭЦП, шифрования, имитозащиты и ЭЦП. Криптобиблиотеки для разработчиков приложений	ЗАО “Сигнал-КОМ”
5	“АП ЗЭП-Win”	Программное средство генерации ключей шифрования и ЭЦП, шифрования, имитозащиты и ЭЦП в среде WINDOWS	ООО Фирма “ИнфоКрипт”
6	“КриптоПро CSP”	Программное средство шифрования, имитозащиты данных, обеспечения целостности и подлинности информации, формирования ключейшифрования и ЭЦП	ООО “Крипто-Про”

ПРЕИМУЩЕСТВА РЕШЕНИЯ КРИПТО-ПРО НА ПЛАТФОРМЕ MICROSOFT 5

- криптографический интерфейс фирмы Microsoft – CSP позволяет гибко настраивать клиентские и серверные **приложения на платформе Windows** для работы как **с сертифицированными**, так **и с** интегрированными **базовыми криптографическими средствами**
- криптографический интерфейс фирмы Microsoft – CSP **позволяет встраивать сертифицированные средства криптографии**, в том числе на базе «КриптоПро CSP», в любые клиентские и серверные приложения, функционирующие на платформе Windows
- решение имеет хорошо **документированные средства применения криптографического интерфейса** CSP, CryptoAPI и специализированного объекта COM (CapiCom.dll), позволяющего программировать клиента на базе Microsoft Internet Explorer
- «КриптоПро CSP», в отличие от базовых криптопровайдеров Windows, **обеспечивает работу с ключевыми контейнерами** на гибких магнитных дисках, устройствах Touch Memory (Dallas Semiconductor) и E-token
- продукт «КриптоПро CSP» **является сертифицированным решением**
- решение имеет **положительный опыт применения** в системах интернет-трейдинга

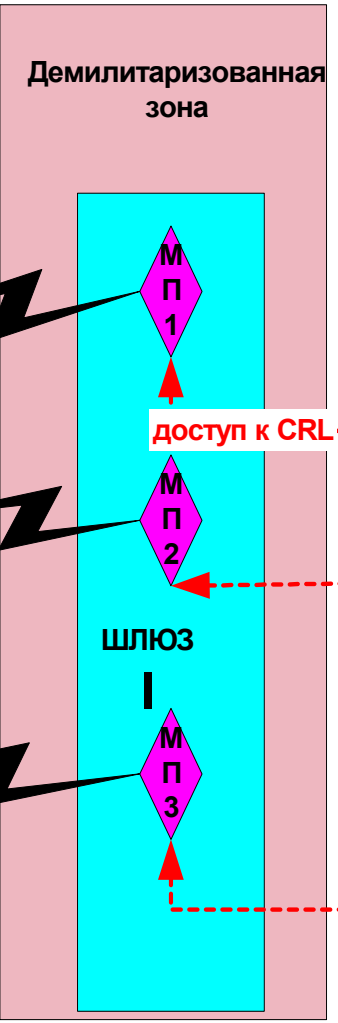
АРХИТЕКТУРА СИСТЕМЫ БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ ЭФО 5



ФУНКЦИИ

- формирование шифрованного канала между клиентом и сервером
- организация клиент/серверной аутентификации с использованием криптографических процедур
- проверка принадлежности сертификата клиенту
- проверка наличия подписи под документом, в том числе количество подписей под документом
  - ❑ проверка ЭЦП под документом
  - ❑ контроль целостности документа
  - ❑ проверка цепочки издателей сертификата (принадлежность сертификата соответствующему приложению)
  - ❑ проверка отозванности сертификата
  - ❑ проверка времени жизни секретного ключа
  - ❑ проверка системной роли сертификата
  - ❑ проверка корректности последовательности подписей соответствующих системных ролей под документом
- подписанное уведомление о доставке документов
- архивирование электронных документов
- ведение журналов событий связанных с открытием и закрытия сессий клиентов, получением/отправкой документов, результатами проверки ЭЦП

КОМПОНЕНТА I: ШЛЮЗ БЕЗОПАСНОСТИ



МП 1

ТЕХНОЛОГИЯ:

- С каждым приложением связан свой модуль политики (МП):
  - реализует функции безопасности, перечисленные на слайде 12
  - предоставляет интерфейс настройки политики безопасности приложения
  - формирует шифрованный канал передачи данных с сервером приложения
  - перенаправляет запросы клиентов на WWW серверы приложений
  - проверяет ЭЦП под документами сервера приложения
  - создает подписанные документы-квитанции для клиента

ПЛАТФОРМА:

- Microsoft Internet Security&Accelerate Server Enterprise Edition (ISA сервер), нагрузо- и отказоустойчивость обеспечивается кластерной технологией
- для сервиса FIREWALL ISA как опция есть средства отражения типовых атак для IP протокола

ОБЕСПЕЧИВАЕТ:

Выполнение требований

(II,7) протоколировать события и обладать средствами анализа журналов событий. документом

(II,6) иметь развитую систему администрирования.

(III,1) минимизация общей стоимости владения системой (ОСВ)

(III,3) платформенная независимость системы безопасности от платформ разработки и среды выполнения фронт офисных приложений

ЭЦП - Процессор

ПЛАТФОРМА:

- **работает на Windows под операционными системами Windows 95/98/ME/NT/2000/XP**
- **использует CapiCom для доступа к криптопримитивам CSP;**

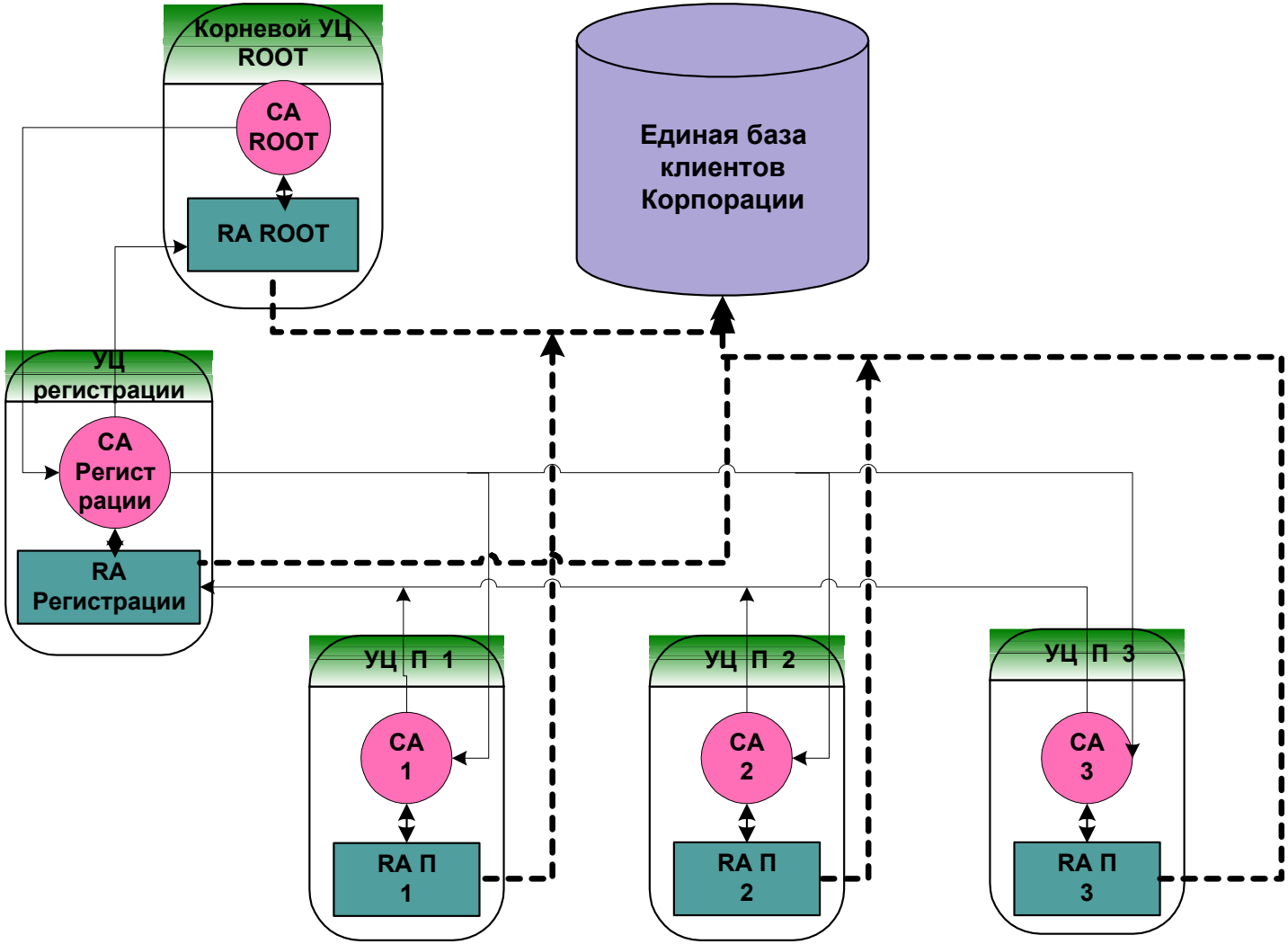
ТЕХНОЛОГИЯ:

- **выполнен в виде компоненты Active-X для интерпретируемых языков на стороне клиента**
- **выполнен в виде библиотеки динамической загрузки на стороне шлюза безопасности и/или сервера приложений**
- **использует CapiCom для доступа к криптопримитивам CSP;**
- **предоставляет стандартный высокоуровневый набор функций для работы с ЭЦП:**
  - **простановку подписи под электронным документом,**
  - **проверку целостности электронного документа,**
  - **проверку цепочки издателей сертификата,**
  - **проверку имени издателя сертификата,**
  - **проверку времени жизни сертификата и секретного ключа,**
  - **проверку отозванности сертификата (наличие в CRL),**
  - **загрузку актуальной версии CRL на локальную станцию из CrlDistributionPoint (CDP),**
  - **разбор и извлечение полей сертификата**

ОБЕСПЕЧИВАЕТ Выполнение требований (III,4)

средства безопасности на стороне клиента должны поддерживать концепцию «тонкого клиента»

КОМПОНЕНТА IV: УДОСТОВЕРЯЮЩИЙ ЦЕНТР



Запросы на сертификат от подчинённых УЦ

Доступ сервисов RA в единую базу УЦ Корпорации

КОМПОНЕНТА IV: УДОСТОВЕРЯЮЩИЙ ЦЕНТР

- **Основное звено нашей реализации Public Key Infrastructure**
- **Проектировался с учётом основных положений Федерального закона (1-ФЗ) об Электронной цифровой подписи**
- **Имеет трёхуровневую иерархическую структуру**
- **Обеспечивает выпуск сертификатов ключей ЭЦП для применения в корпоративной системе «НИКойл» и системах общего пользования**
- **Предоставляет программный интерфейс для внешних приложений**

ОБЕСПЕЧИВАЕТ ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ:

(I,1) **ведение общей клиентской базы в системе безопасности**

(I,2) **однократная регистрации клиента в системе безопасности, обеспечивающая последующую работу клиента во всех существующих и вновь создаваемых фронт офисных приложениях**

(I,3) **наличие в системе безопасности однотипных и максимально удобных для клиента процедур регистрации и доступа к электронным приложениям фронт офиса Корпорации**

(I,4) **наличие у клиента одного секретного криптографического ключа для работы со всеми электронными приложениями фронт офиса**

(I,5) **наличие юридически корректных процедур для разбора конфликтных ситуаций за счёт наличия в составе Автоматизированного Рабочего Места разбора конфликтных ситуаций**

КОМПОНЕНТА IV: УРОВНИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 5

Корневой УЦ (ROOT):

- установление отношений доверия с УЦ внешних партнёров корпорации и с УЦ государственного уровня
- выпуск сертификатов и списков CRL УЦ регистрации

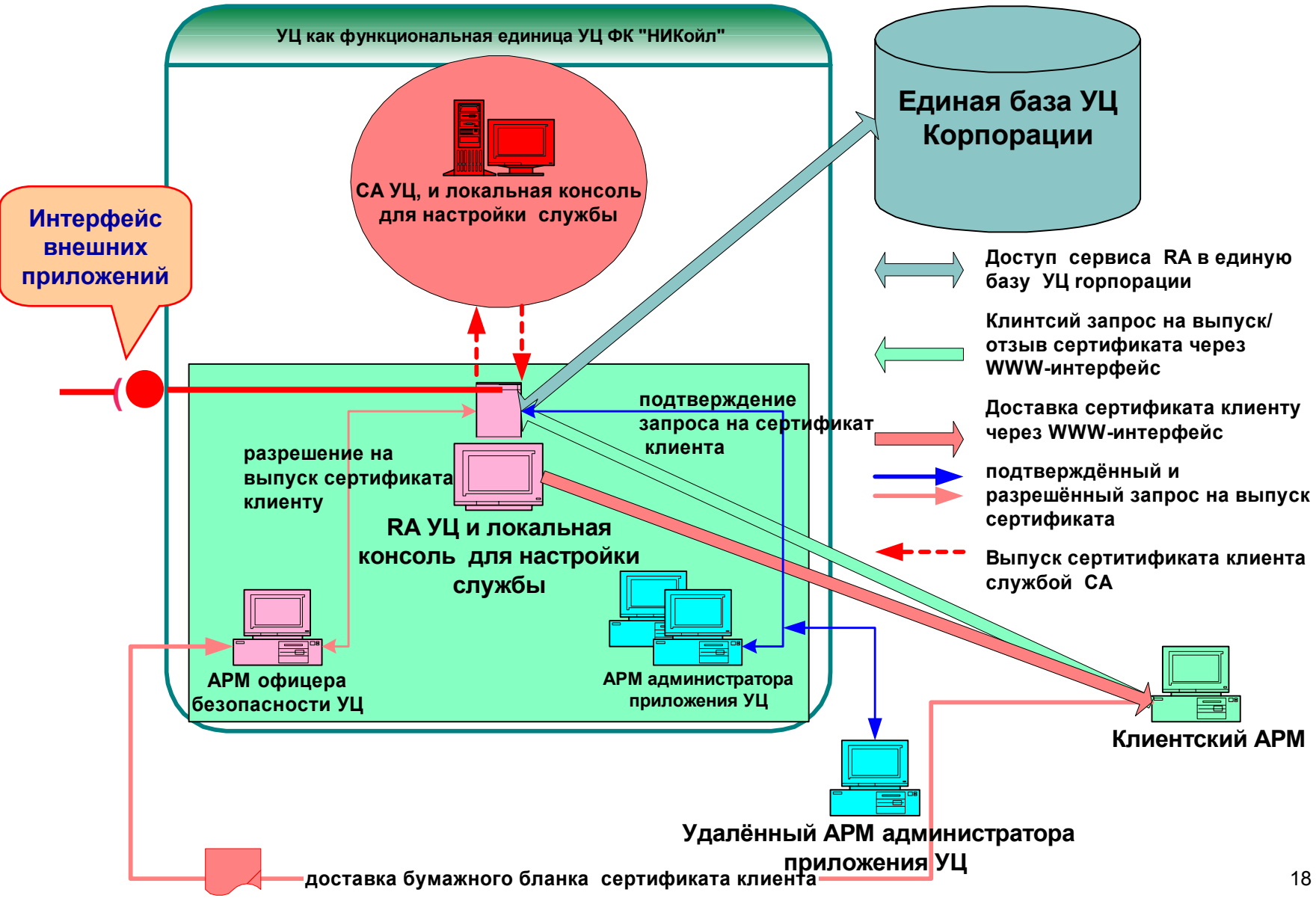
УЦ регистрации:

- регистрацию клиентов в единой клиентской базе при непосредственной однократной явке клиента в центр регистрации и выдачу клиенту технологического ключа ЭЦП для аутентификации на регистрационном УЦ и подписи запроса на сертификат боевого ключа
- удалённый WWW-интерфейс для генерации боевых ключей ЭЦП и запросов на сертификат клиента с рабочего места клиента
- выпуск боевых секретных ключей ЭЦП и сертификатов клиентов непосредственно в регистрационном центре «… по обращению участников информационной системы …, Глава III, Статья 9, п. 1, ФЗ №1» для использования « … в информационных системах общего пользования, Глава III, Статья 9, п. 1, ФЗ №1»
- отзыв сертификатов клиентов через занесение сертификатов в списки CRL и опубликование списков CRL
- настройку параметра времени жизни секретного ключа и сертификата и контроль этих параметров
- процедуры плановой и внеплановой смены ключей и сертификатов клиентов
- средства голосовой авторизации клиента на регистрационном УЦ
- выпуск сертификатов УЦ приложений

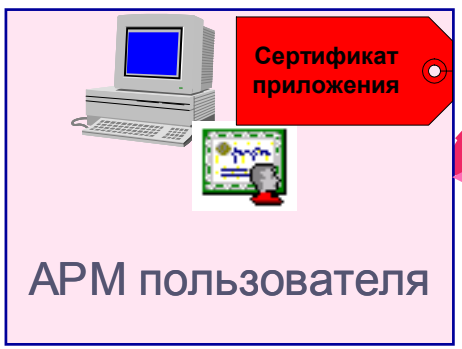
УЦ приложения:

- WWW-интерфейс для формирования клиентом запроса на сертификат
- выпуск сертификата клиента для разрешённой роли
- прекращение или приостановка работы клиента в приложении через отзыв или приостановку действия сертификата клиента для данного приложения

КОМПОНЕНТА IV: ЛОГИЧЕСКАЯ ЕДИНИЦА УРОВНЯ УЦ



РЕГИСТРАЦИЯ КЛИЕНТА



Доставка документов администратору приложения

1. Регистрация клиента (левый офицер безопасности):
   - явка клиента в центр регистрации
   - проверка установочных данных клиента
   - выдача клиенту технологического ключа для аутентификации на центре регистрации

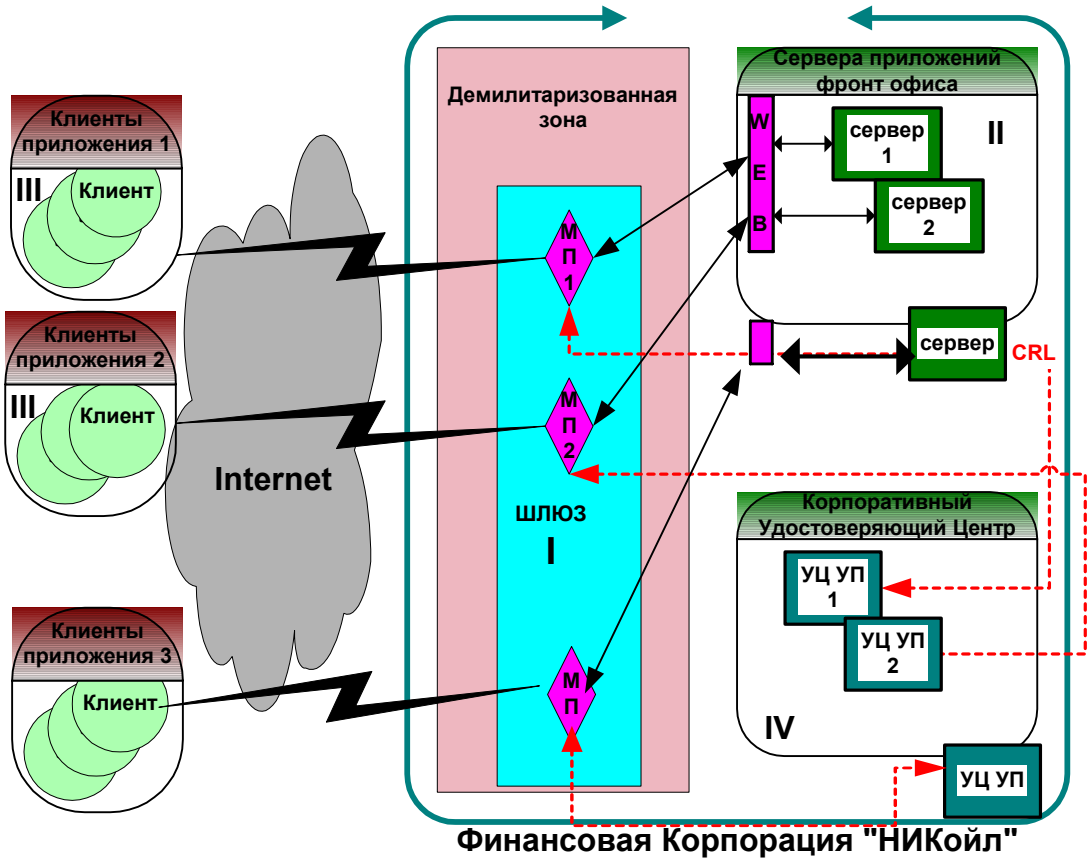
2. Формирование клиентом боевого ключа ЭЦП и запроса на сертификат со своего рабочего места

4. Получение запроса правым офицером безопасности, проверка оформления регистрации и выпуск боевого сертификата

5. Отправка клиентом документов администратору приложения и формирование запроса на сертификат для работы клиента с приложением 1

6. Проверка соответствия системной роли сертификата регистрационным данным приложения и выпуск сертификата

ИНТЕГРАЦИЯ НОВОГО ПРИЛОЖЕНИЯ В СИСТЕМУ БЕЗОПАСНОСТИ 5



1. Разработка сервера приложения
2. Разработка политики безопасности приложения:
   - аутентификация в приложении
   - работа с ЭЦП в приложении
   - состав сертификата
   - политика системных ролей в приложении
   - политика работы с сертификатами
   - регистрация событий
   - ведение юридически значимых архивов
3. Разработка Модуля Политик безопасности на шлюзе безопасности для данного приложения
4. Развёртывание УЦ для данного приложения
5. Организация WWW интерфейса приложения и УЦ приложения
6. Регистрация клиентов приложения и начало промышленной эксплуатации

МЕЖДУНАРОДНЫЕ РЕКОМЕНДАЦИИ

- Национальный Институт Стандартов и Технологий США (NIST) и Национальное Агенство Безопасности (NSA) «Профили Защиты для операционных систем, межсетевых экранов, систем выявления вторжений, токенов и PKI»
- Отделение компьютерной безопасности Национального Института Стандартов и Технологий США (The National Institute of Standards and Technology's Computer Security Division):
  - Выбор ИТ продуктов для обеспечения безопасности (Selecting IT Security Products (SP800-36))
  - Сервисы безопасности ИТ (IT Security Services (SP800-35))
- ISO 15408 Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности ИТ)
- Control Objectives for Information and related Technology (CoBIT) «Контрольные Объекты для Информационной и смежных Технологий»
- ISO/IEC 17799:2000 Information technology -- Code of practice for information security management
- A comprehensive risk assessment tool (CRAMM)

ИСТОЧНИКИ ДОПОЛНИТЕЛЬНОЙ ИНФОРМАЦИИ 5

- «Обеспечение безопасности Интернет-транзакций в финансовой корпорации «НИКойл»//Windows 2000 Magazin, №7, 2002 г.
- http://www.microsoft.com/rus/government/newsletters/issue17/10.asp

- Ануфриев В.Н., e-mail: avn@nikoil.ru, http://avn.nikoil.ru
- Калинсков И.Н., e-mail: kal_in@nikoil.ru

- Финансовая Корпорация НИКойл http://www.nikoil.ru
- Брокерская компания НИКойл http://www.brokerage.nikoil.ru
- Депозитарная компания НИКойл http://www.depository.nikoil.ru
- Сервисная компания НИКойл http://www.banquet.nikoil.ru
- Промышленно-страховая компания http://www.iic.ru
- Управляющая компания НИКойл http://www.management.nikoil.ru
- Операционная факторинговая компания НИКойл
- http://www.factoring.ru
- электронная коммерция http://www.e-nikoil.ru