ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

АКТУАЛЬНЫЕ ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БОЛЬШИХ КОРПОРАТИВНЫХ СИСТЕМ

АКАДЕМИЯ КРИПТОГРАФИИ РОССИИ
академик А.П. БАРАНОВ

ЧТО ЕСТ(Ь) ИАС ?

$10^3 \div 10^2$

УПРАВЛЕНИЯ ЦА

ОГРАНИЧЕННЫЙ КОНТИНГЕНТ - КОРПОРАТИВНЫЙ ПОЛЬЗОВАТЕЛЬ (КП)

ЯДРО ИАС

МАССОВЫЙ ОБЩЕ-ГРАЖДАНСКИЙ ПОЛЬЗОВАТЕЛ Ь (ОГП)

ВНЕШНИЕ ИАС

$10^4 \div 10^5$

$10^6 \div 10^7$

$10 \div 100$

ТРЕБОВАНИЯ по ФУНКЦИОНАЛУ, ВЛИЯЮЩИЕ на ИБ

- Корпоративная ИАС – обрабатывает (смешивает) различные категории тайны: персональные данные, банковскую тайну, налоговую тайну, коммерческую тайну и т.д. Мандатный доступ-доработка ОС
- Различная насыщенность (жесткость) требований к различным пользователям: к внешним ИАС и КП-интенсивные, мягкие к руководству и еще более мягкие к ОГП
- Практически нет ИАС ,изолированных от других ИАС. ИАС-КОП это ИАС – корпоративно -общественного применения
- ИАС-КОП вынуждена поддерживать актуальных агентов различных систем: СМЭВ, ГИС ГМП, ЕСИА, ИС ЦБ, ИС коммерческих банков, ИС Госведомств

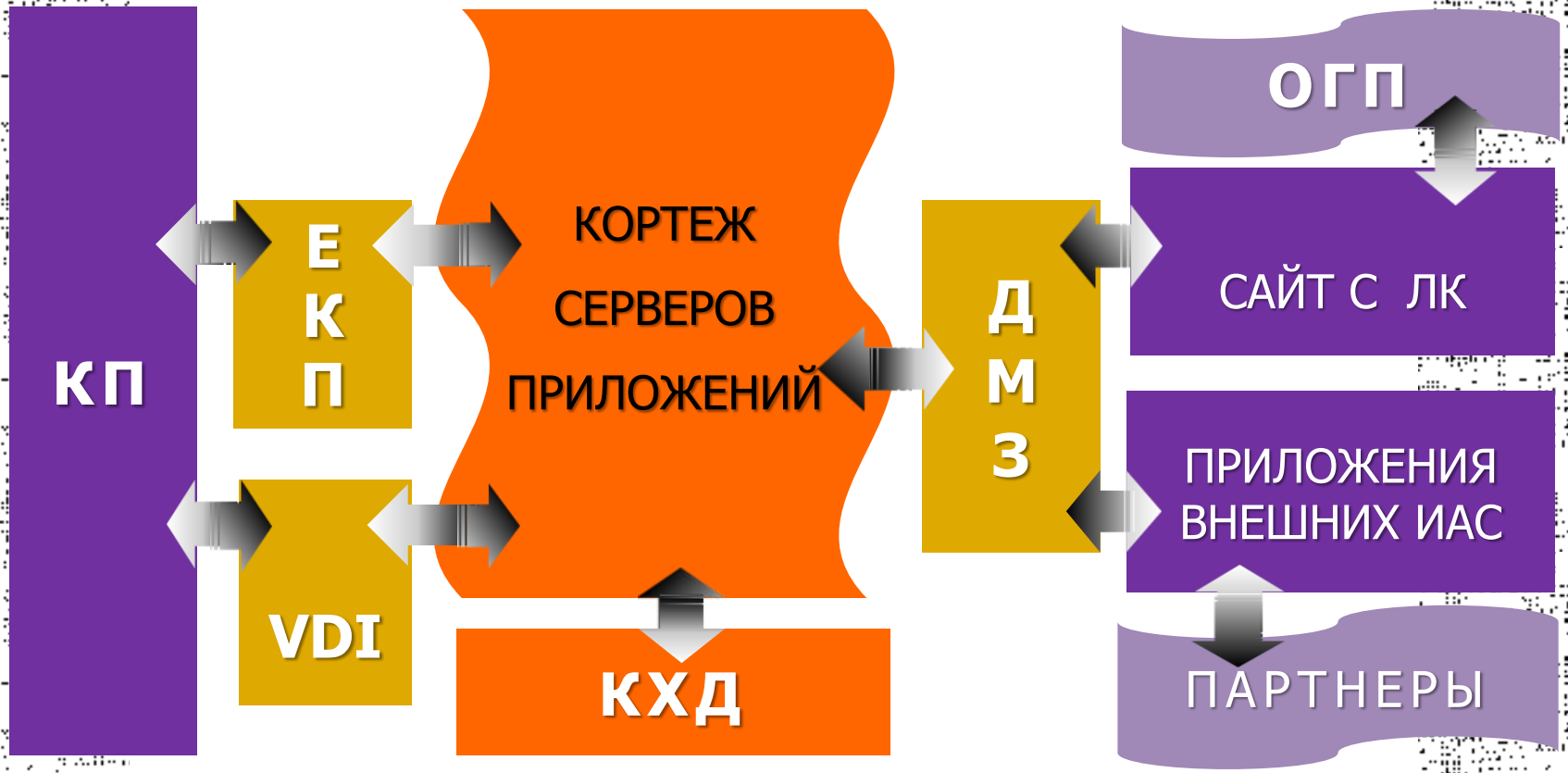
НОВЫЕ АКЦЕНТЫ ТРЕБОВАНИЙ по ИБ для ИАС-КОП

- Равнозначимость обеспечиваемой конфиденциальности и юридическая равноответственность при взаимодействии ядер розличных ИАС
- Разграничение по доступу:
  - между ОГП и корпоративными пользователями (КП);
  - между различными ИАС;
  - между ОГП различных ИАС
- Юридически значимое, согласованное по срокам архивное хранение
- Сочетание ИБ с кроссплатформенностью, а так же широтой и доступностью (простотой) услуг
- Гражданская информационная оборона

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И ЮРИДИЧЕСКОЙ ЗНАЧИМОСТИ ВЗАИМОДЕЙСТВИЯ ИАС-КОП

- Шифрование информации на основе ГОСТ освоено на скоростях до 10Гб/сек. Обеспечено закрытое взаимодействие ЦОДов ,включая зеркалирование
- Остается актуальной проблема встречного шифрования в IP-потоке и тестирования реализации SSL различных производителей. Пример: день Всеобщего приема граждан в декабре
- ЭП больших(10Гбайт) файлов и проблема установления достоверности передачи информации у провайдеров. Ошибки CRC могут начинать сказываться
- Физическая раздача и контроль замены ЭП при массовой , более 10^7 пользователей усиленной ЭП
- Усиленная ЭП, простая, облачная ЭП – юридическая значимость. Сейчас только взаимные договора. Проблема краденных пар логин - пароль

ТИПИЗАЦИЯ ПРЕДСТАВЛЕНИЯ ПРИКЛАДНОГО УРОВНЯ ЯДРА ИАС-КОП



ПЕРВООЧЕРЕДНАЯ ЗАДАЧА ИБ – РАЗГРАНИЧЕНИЕ ДОСТУПА В КЛАСТЕРЕ ЦОДа

- Обеспечение и сертификация защиты от НСД в виртуальных серверах приложений на кластерной основе
- Разграничение и сертификация доступа к данным и процессам в кортеже серверов VDI
- Разграничение доступа в КХД базового, начального, транзакционного слоя
- Разграничение доступа в БД для аналитического сегмента.Сертификация по требованиям ИБ многомерных и реляционных БД

АРХИВНОЕ ХРАНЕНИЕ В ИАС-КОП

- Архивное хранение это передача информации во времени
- Конфиденциальность, целостность , доступность в такой передаче
- Конфиденциальность - хранение в шифрованном или незашифрованном виде петабайт памяти? Срок действия ключей шифрования?
- Катастрофоустойчивость или сколько ЦОДов хватит два или четыре? Требования TIER1-4 не об ИБ. Защищенный в каком смысле ЦОД?
- Периодическая смена видов носителей – вечное хранение

Качество услуг в ИАС-КОП и ИБ

- Проблема сочетания ИБ и качества услуг для КП:
  - быстрое изменение функционала серверов приложений из за модернизации законодательства;
  - централизованное управление компонентами СОБИ требует эффективного подчинения КП правилам ИБ;
  - апостериорная защита нуждается в регулярной демонстрации эффективности
- Для "внешних" ИАС существует Проблема доступности
  - стандартизация и унификация на прикладном уровне и уровне представлений видов запросов – ответов. XML – слишком широк, XBRL – малоизвестен
  - как перейти с одного вида запросов на другой, не выкидывая предыдущее ? Конвертация?

ИБ И КАЧЕСТВО УСЛУГ ДЛЯ ОГП

- Простое, бесплатное, контролируемое распространение ЭП
- Как дешево и доступно, в смысле навыков, обеспечить безопасность ключей, информации и гарантировать целостность ПО у ОГП (10^7 пользователей)?
- Необходимы простые в использовании тестеры для неквалифицированного пользователя, выявляющие "боторизацию» или шпионскую программу
- Что эффективнее на РМ у ОГП априорная или апостериорная защита ?
- Государственные и коммерческие организации мало работают с массовым пользователем по пропаганде ИБ. Гражданская информационная оборона возложена на самих граждан

КАК НАМ РЕОРГАНИЗОВАТЬ "РАБКРИН"?

- Компьютерный продукт для ОГП должен обязательно содержать рекомендации ИБ на РМ
- Наряду с созданием систем типа ПГУ, необходимо в комплекте создавать и продукты для защиты РМ у ОГП
- К платежной карточке нужна инструкция по ИБ. Где хранит пароли владелец трех карточек?
- Удаленное управление банковскими счетами стало массовым явлением у ОГП. Какие меры ИБ предлагаются банками для вкладчиков?
- Создание общегосударственной системы мониторинга скомпрометированных пар логин – пароль, для своевременного конфиденциального оповещения и замены

УЧИТЬ, ОБЬЯСНЯТЬ И ПРОПАГАНДИРОВАТЬ ИНФОРМАЦИОННУЮ ГРАЖДАНСКУЮ ОБОРОНУ

- Наряду с обучающими программами на ТВ по арифметике и информатике необходимы программы по ИБ для ОГП, школьников, студентов
- Необходимо развитие сети обучающих программ: бакалавриата и магистратуры. Специалитет уходит в прошлое. Требуются бакалавриатские программы
- В ВШЭ организована магистерская программа "Управление Информационной безопасностью" с 20 бесплатными местами и программой двойных дипломов
- В этом году проводится Третья бесплатная , открытая конференция в ВШЭ по вопросам ИБ с включением докладов иностранных специалистов
- Целесообразно использование зарубежного опыта для пропаганды реальной, повседневной ИБ, с привлечением общественных профессиональных организаций


СПАСИБО ЗА
ВНИМАНИЕ