ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

АКТУАЛЬНЫЕ ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ) КОМПЬЮТЕРНЫХ СИСТЕМ (КС)

АКАДЕМИЯ КРИПТОГРАФИИ РОССИИ
академик А.П. БАРАНОВ

Общее состояние задач ИБ

- Стратегические направления, сформулированные на Рускрипто – 2014, сохранили свою актуальность
- По отдельным направлениям можно перечислить успехи:
  - в организационной законодательно-творческой части;
  - в техническом обеспечении решения защиты ИБ;
  - в реализационной части нормативных актов регуляторов
- Существенных прорывов не состоялось
- Развитие КС в России продолжалось значительными темпами и выдвинуло серию конкретных практических потребностей в области ИБ реально создаваемых комплексов
- Потребности ИБ можно классифицировать аналогично стратегическим направлениям

Основные направления

- Многопроцессорные кластерные системы, основа защищенных облачных услуг
- Информационная безопасность программного обеспечения (ПО)
- Криптография в массовом применении
- Алгоритмические методы обеспечения безопасности информации в больших системах
- Апостериорная защита на основе мониторинга

Практические задачи ИБ кластерных систем ЦОДов

- Компьютерная надежность и устойчивость ЦОДов по выполнению облачных функций . TIER 1 ÷ 4 – катастрофоустойчивость
- Соответственно требования по Конфиденциальности, Целостности и Доступности ЦОД. Критические информационные технологии и требования к ним, как по Персональным Данным
- Конфиденциальность и разграничение управления кластером и прикладными серверами
- Целостность по отношению к ошибкам ПО при пересылке больших массивов (до 10 Тбайт) и зеркалировании БД
- Доступность – устойчивость прикладного ПО к действиям пользователя и администраторов кластеров

Информационная безопасность пользовательского ПО в конфиденциальных системах

- Развитие абонентского ПО на рабочих местах (РМ) массового пользователя ("толстого" клиента):
  - кроссплатформенность и кроссбраузерность;
  - усиление защиты хранимой ключевой инфы;
  - определение для пользователя и выдача рекомендаций по уровню НДВ. Объяснить, от кого защищаться пользователю
- Развитие облачных технологий ЭП. Каждому пользователю гарантируют свой "сейф" для хранения ключа. Кто гарантирует(регулятор) и что?
- Юридические гарантии по доступу к ключу, кроме взаимного договора

ИБ на РМ пользователя

- Сертификация РМ пользователя в "облаке" в сочетании "тонкого" (облачного) и "толстого" клиента. Разумное сочетание требований для общегражданского пользователя
- Удаленное тестирование РМ пользователя по ИБ и удаленная аттестация до уровня КА
- Мобильный офис с уровнем безопасности выше КБ1. Обоснование и формализация требований по защищенности информации при утере (краже)
- Маскирование систем ИБ – метод защиты информации

Криптография в массовом применении

- Усиленная неквалифицированная ЭП – возможность применения ослабленных требований регуляторов к квалифицированной ЭП
- В состав комплексов ЭП наряду с криптопровайдерами надо включать редактор для гарантированной степени, визуализации. Этого достаточно?
- ЭП для больших (10 Гбайт) файлов требует достоверность передачи сообщений.
  P (ошибки на бит) ≤ 10^{-11}. В протоколе HDSL для CRC всего 4 бита, как и в RS-232 ,а в USB определено 16 бит
- Какой класс достоверности передачи информации обеспечивает ваш провайдер I 1, I 2 или I 3?
- Исследования эффективности CRC в различных моделях образования ошибки и выбор проверочных полиномов

Практические вопросы алгоритмических методов обеспечения ИБ

- Каталог инцидентов ИБ (ИИБ) и их описаний в КС:
  - на базовом уровне действий администраторов, как в ЦОДе, так и на территориальном уровне;
  - на прикладном уровне – ДОБЫЧА и ВЫБИВАНИЕ описаний ИИБ от программистов прикладных программ
  - ИИБ о "внутренних" и "внешних" пользователях
- Аналитические системы анализа состояния ИБ в составе ЦУБИ – центра управления безопасностью информации
- Принципы агрегации всех систем мониторинга различных подсистем. Оптимизация загрузки трафика мониторинга между ЦУБИ и территориальными органами за счет интеллектуализации объектов СОБИ
- Контрольные системы ЦУБИ для больших АИС. Что контролировать? Только ИИБ?
- Защита систем СОБИ от ошибочных действий администраторов и обслуживающего персонала

Апостериорная защита информационного взаимодействия

- Автоматическое применение ЭП переносит ответственность на руководителей, освобождая от нее рядовой состав. Юридическое значение записей в журнале логов
- Сроки хранения электронных документов собственности граждан 75 лет. Сроки хранения данных о различных видах налогов до 10 лет. Как хранить, открыто или зашифровано?
- Объемы хранения у некоторых ведомств более 10 Тбайт. Срок хранения ключа подписи не более трех лет. Перешифрование и переподписание в распределенных базах сложно реализовать.
- Каков срок хранения информации в СОБИ учитывая возможность активизации отложенного программного воздействия?

Учить, объяснять 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