ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНЫЙ ИННОВАЦИОННЫЙ
ВНЕДРЕНЧЕСКИЙ ЦЕНТР
ГНИВЦ

Перспектива применения шифртехники (КС2 или КС3)

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ
А.П. БАРАНОВ
abaranov@hse.ru

ДОЦЕНТ НИУ ВШЭ
П.А. БАРАНОВ
pbaranov@hse.ru

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Современные черты крупных создаваемых и эксплуатируемых систем

ГНИВЦ

1. По Массовый пользователь – $10^5 \div 10^7$ абонентов. Низкая квалификация основной группы. Высокие требования абонентов к устанавливаемому ППО в части простоты эксплуатации, удаленной установки, частой, существенной корректировке и низкой цены
2. Связь и взаимодействие через Интернет в варианте применения смартфонов
3. Применение только программных средств для различных базовых операторов систем IOS, Windows, Android и др.
4. Обработка чувствительной и конфиденциальной информации, дополнительной к ПД. Конфиденциальность растет: банковская, налоговая, медицинская, коммерческая и другие виды информации

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Примеры массовых систем

ГНИВЦ

1. Портал госуслуг (ПГУ) и взаимодействующие с ним госсистемы. Более 10^7 абонентов
2. Единая система идентификации и авторизации (ЕСИА). Все госорганы и банковские системы – абоненты ЕСИА
3. Система контроля кассовой техники (ККТ) - 10^6 абонентов
4. Маркировка товаров (в том числе ЕГАИС) - 10^5 абонентов
5. Личные кабинеты граждан – абонентов ведомственных систем (ПВДНП, МВД, ПФР и др.) – 10^7 пользователей
6. Необходимые скорости протокольного шифрования растут. Уже надо 40-60 Гбит/сек

abaranov@hse.ru, pbaranov@hse.ru

От кого защищаемся с КС2?

1. Внешний противник для канала связи реализует утечку информации (Z.B. персональных данных и др.) при передачи от одного объекта к другому. Противник может иметь доступ к каналу связи и не иметь доступа к СВТ ,где функционирует СЗИ т. е. нарушитель не пытается подделывать данные
2. По требованиям ФСБ РФ к защите ПД это - КС2 для систем 4 -2 уровней защищенности, а госсистемы почти всегда 1 уровень
3. Рабочее место может использовать широкий спектр ОС и аппаратных платформ. Однако массовый пользователь требования, содержащиеся в условиях действия сертификата, не выполняет
4. Проблема в неравной защищенности партнеров. Какова юридическая значимость взаимодействия через ПГУ с ЭП на массовом РМ, если она (ЭП) неквалифицированная?

abaranov@hse.ru, pbaranov@hse.ru

Уровень КСЗ – защита от внутреннего нарушителя

1. Актуальные примеры внутренних нарушителей в сфере торговли:
   a) пользователи ККТ;
   b) производители контрафактной продукции;
   c) контрабандные товары
2. Среда оказания госуслуг и противодействие незаконным операциям:
   a) использование материнского капитала и др. поддержки малообеспеченных граждан на основе поддельных документов;
   b) получение кредитов на основе недостоверных сведений о доходах;
   c) безосновательный возврат Налога на добавленную стоимость с использованием фирм «однодневок»;
   d) неоплаченное использование услуги (платные дороги, стоянки, банкоматы)
3. Пользователь системы может быть организатором и исполнителем мошеннической схемы, в том числе в составе группировки
4. Цель применения КСЗ – неотказуемость от произведенных пользователем действий

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Особенности реализации ИБ в ГИС 1–ого класса. Не криптографические методы

ГНИВЦ

1. Режим online совершения действий в составе VDI. Сертификаты ФСТЭК по разграничению доступа к общей базе данных и проверка по НДВ. Следовательно, требования к ОС и СУБД– наличие исходных текстов
2. Режим offline, как временный с переключением и передачей информации наработанной в offline в online систему. Сертифицированный виртуализатор с исходными текстами
3. Что есть исходные тексты в современных системах разработки ПО, опирающиеся на САПР. Кто сертифицирует САПР, а ранее транслятор?
4. Импортозамещение. Проблема отечественной аппаратной платформы в телекоммуникационной компоненте. Сборки в России из импортных компонент отечественные?
5. Закон № 187 от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации». Категория значимости и их соответствие категориям систем обработки ПД. Сколько будет стоить?

abaranov@hse.ru, pbaranov@hse.ru

Системы с использованием КСЗ

1. Шифрсредства (ШС) аттестованные по КСЗ присутствуют в виде законченных изделий: Застава, ЕС Смарт, автономные шифраторы
2. Проблема в фиксации программной среды, требуемая при сертификации по КСЗ. Каждое обновление требует дополнительной аттестации
3. Практически невозможно аттестовать ШС в составе комплекса, имеющего программные средства общего назначения без исходных текстов
4. Все выше отмеченное относится, как к средствам шифрования трафика, так и к квалифицированной ЭП
5. Для средств ЭП, аттестованных по КСЗ, нужны общие правила «быстрой, легкой» модернизации ПО. Z.B. Замена драйверов печати и т.д.

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Выводы

ГНИВЦ

1. Возникновение массовых систем с повышенными требованиями по ИБ, как в среде ответственности ФСТЭК, так и по линии ФСБ РФ – новое явление
2. Аттестация по КСЗ и выше требует глубокого изучения применяемого базового и ППО с наличием исходных текстов, как самого ПО, так и средств его разработки
3. Упрощение пользовательского интерфейса и функционала нарастает, при этом требования ИБ массовым системам будут так же повышаться. Абонент ставится во главу угла перед ИБ
4. На очереди ПГУ и ЕСИА, затем ведомственные системы
5. В ближайшее время вслед за законом № 187 возникнет вопрос об устойчивости технологической системы России, как от внешнего, так и от внутреннего воздействия. Шифрование и ЭП будут применятся тотально, как средства обеспечения целостности всей системы

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГНИВЦ

СПАСИБО ЗА ВНИМАНИЕ

abaranov@hse.ru
pbaranov@hse.ru