ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГЛАВНЫЙ
НАУЧНЫЙ ИННОВАЦИОННЫЙ
ВНЕДРЕНЧЕСКИЙ ЦЕНТР
ГНИВЦ

Криптография и информационная безопасность (ИБ) в цифровом обществе

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

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

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Методология оценки состояний и тенденций развития криптографии в обществе

ГНИВЦ

1. Наука – есть система доступных знаний о наблюдаемых нами явлениях действительности /В.Ф. Войно-Ясенецкий (Архиепископ Лука), доктор медицинских наук/
2. Явления: тенденции развития, информационные технологии в обществе и соответствующие им средства и способы ИБ
3. Элементы системы знаний о связи криптографии и общества:

а) Переход в 80х годах XX века от информационного общества к цифровому, как следствие развития возможностей технологической передачи, обработки и хранения информации

б) Повсеместное применение компьютерного потенциала привело к превалированию функциональных требований над ИБ

в) Криптография и ИБ – слуги (хоть и очень важные) прикладных потребностей общества. Эволюция ИБ определяется изменением функциональных потребностей общества

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Безопасная цифровая платформа существования общества – новый бренд

ГНИВЦ

1. Переход от цифровой услуги к цифровому взаимодействию всех частей общества на основе мобильных платформ с обеспечением различных уровней безопасности Фундамент цифровой платформы – достоверная, бесконтрольно не корректируемая информация на базе синхронизированных данных и визуализация приложений
2. ЭЦП – базовый принцип обеспечения целостности и неотказуемости от авторства исходных данных. ЭЦП стало важнее и востребование шифрования
3. Новые применения ЭЦП в архивном (до сотен петабит хранения) деле с длительностью хранения более ста лет выдвигают новые требования к условиям использования ключей и доверенной третьей стороне
4. Взаимодействие ведомств обеспечивается шифрованием, массового (миллионы пользователей) взаимодействия нет. Требуемая скорость 1 до 100 Гбит/с

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Доступность (устойчивость) к воздействию эквивалента жизнеспособности платформы

ГНИВЦ

1. Заблуждения о силе криптографии порождают иллюзии устойчивости существования и взаимодействия
2. Террористическая угроза работоспособности ИТС актуальна из за ошибок проектирования в реализации сложных систем
3. Шифрование информации и каналов передачи защищают от внешнего террориста. Защита от искажения функционального ПО внутренним противником реализуется ЭЦП с рядом существенных оговорок
4. Задача: с помощью криптографии защитить ППО от искажения внутренним противником с минимумом условий
5. Обфускация ПО с помощью криптографии и проверка ее «правильности»? Электронные «водяные» знаки и стеганография ПО для выявления факта искажения по ходу исполнения?

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Иллюзия абсолютности ИБ с помощью криптографии

ГНИВЦ

1. Криптография спекулятивно используется как синоним абсолютной надежности и перспективы всеобщего благополучия: блокчейн, квантовые криптография и компьютеры, искусственный интеллект и нейронные сети
2. Не существует массовой квалифицированной ЭП. Массовая ПЭВМ реально беззащитна от террористов и не может быть достаточным (по требованиям регуляторов) образом защищена
3. Выход в узкоспециализированных устройствах с фиксированным, неизменным сертифицированным ПО для реализации криптофункций
4. ПЭВМ общего массового применения должно рассматриваться только как элемент телекома
5. Возможен ли SSL без предварительного облака, т.е. без использования ранее созданной партнёром информации об его открытом ключе?

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Устойчивость (работоспособность) компьютерных систем и криптография

ГНИВЦ

1. Нет систем доказательно безошибочного проектирования компьютерных систем, не оставляющих «лазеек» для террористического проникновения. Доказательство: постоянно выпускаемые патчи, исправляющие ошибки
2. Теоретическая проблема в объеме (трудоемкости) тестирования и сложности (дороговизне) стендов – эмуляторов действительности
3. Реально высокая степень квалификации привлекаемых террористами специалистов взлома. Иллюстрация: возможность перехвата и дешифрования атмосферной части телефонного трафика
4. Публикации и широкое исследование криптосхем похоже на анализ ПО с открытым исходным кодом и процессорами с детальным описанием построения. Все ли прорехи публикуются?
5. Возможно ли применение методов выявления НДВ в ПО для анализа криптосхем?

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Устойчивость (работоспособность) телекоммуникационных систем

ГНИВЦ

1. Основа современного телекома – коммутатор и маршрутизатор. Это сочетание ПО и специализированной высокопроизводительной платформы (СП) на чипах (ASIC) фирм Marvell, Mellanox и др.
2. Маршрутизатор это два взаимодействующих блока. Блок управления (ПЭВМ) и спецблок быстрых переключений на ASIC
3. Блок управления администрируется через шифрованный канал и в настоящее время активно исследуется и сертифицируется
4. Блок на ASIC работает по фиксированным программам и на устойчивость исследуется как черный ящик. В случае наличия ошибки в ASIC, возможны террористические воздействия на него даже при шифровании трафика
5. Вывод: либо исследования ASIC, либо шифрование на уровне L1

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Устойчивость телекома и ГосСОПКА

ГНИВЦ

1. Криптография в виде шифрования пакетов и ЭЦП создает внешний периметр защиты в предположении устойчивости ASIC коммуникационного блока
2. ГосСОПКА – система противодействующая нападению, как на верхнем так и нижнем уровнях апостериорно. При нынешней структуре через Интернет
3. При «новейшем» воздействии террористов на СП и ASIC ГосСОПКА будет бездействовать. Можно представить ошибку в ASIC, когда воздействие будет размножаться и рассылаться по определенному сегменту адресов
4. Выход: переход к линейному шифрованию на уровне L1, с переходом на другие, не пакетные принципы образования сети или разработка собственных сертифицированных ASIC. Некоторые оценки последнего варианта 2 года разработки и 2 млрд. ₽
5. Возможна организация международной сертификации и аттестации на устойчивость от террористов?

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Заключение

ГНИВЦ

1. Криптография вступила в эру обслуживания массовых функций и массового применения. Нужны дешёвые, эффективные и простые в эксплуатации крипторешения. Например: надежный криптокошелек, действительно квалифицированная массовая ЭЦП.
2. Сфера, способы и перспектива применения ЭЦП сегодня шире, чем шифрование данных. Сдерживающим фактором является ненадежная, удаленная авторизация и необходимость взаимодействия с УЦ. Возможна ли ЭЦП без УЦ?
3. Криптография пока не может предложить способа кардинального усиления устойчивости современных телекоммуникационных систем против возможных ошибок разработчиков и использования этих ошибок террористами. Шифрование в IP протоколе не решает проблему устойчивости ASIC компоненты коммутаторов.
4. Величие наших замечательных достижений в области применения и развития криптографии мы будем обсуждать на секциях

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГНИВЦ

СПАСИБО ЗА ВНИМАНИЕ

abaranov@hse.ru