ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ
А.П. БАРАНОВ

abaranov@hse.ru

abaranov@hse.ru

Основные тенденции рынка информационных систем текущего периода

1. Расширение гуманитарного диалога общество – государство на основе Интернет
2. Резкий рост спроса населения – пользователя на взаимодействие с сайтами и порталами организаций различного вида собственности.
3. Возрастание количества и качетсва услуг со стороны организаций.
4. Замена стационарного компонента пользователя на мобильный во всех видах деятельности на основе облачных технологий.
5. Внедрение IT-технологий в применяемые населением приборы (машины) и их широкополосная связь с пользователем

\+ Необходимый функционал – потом ИБ

abaranov@hse.ru

Технические направления развития, соответствующие спросу рынка IT

1. Усложнение и регулярная модернизация прикладного ПО в организациях с одновременным упрощением его у населения.
2. Создание автоматизированных систем (АИС) исполнения регламентов деятельности организаций.
3. Массовый пользователь (более 10^7) не может эффективно применить на борту сложное в установке и администрировании ПО.
4. Средства ИБ на местах должны быть просты в применении, иначе их игнорируют.
5. Связь с АИС должна быть всегда и по возможности защищенной от непосредственного прослушивания.

\+ Главное функционал, а ИБ – потом!

abaranov@hse.ru

Проблемы ИБ, вытекающие из тенденций технического развития. Доступность.

1. Устойчивое исполнение регламентов требует системы синхронизованных ЦОДов с новыми требованиями по информационной связи:
   a) скорость в каналах связи до 100 Гбит/сек. с шифрованием на уровне L2. (В настоящее время везде L3);
   b) задержка при передаче шифрованных пакетов не более 0,1 мсек туда-обратно.
2. Ответ портала пользователю не должен занимать более 5 минут при одновременной обработке до 10^4 обращений с проверкой (подписанием) ЭЦП и расшифрованием (зашифрованием).
3. SSL с отечественным криптопровайдером на борту должен удовлетворять условиям: кроссплатформенность, кросс-браузерность, кросс-фирменность.
   !! Легкого в установке отечественного криптопровайдера нет
4. Нужна облачная, сертифицированная ЭЦП, без криптопровайдера на борту устройства пользователя.

abaranov@hse.ru

Целостность

1. Защита информации в АИС на предмет ее неизменности. Апостериорной защиты на основе мониторинга недостаточно.
2. Как гарантируется сохранность: записей о вкладах, кадастровых данных, массивов прав собственности и т.д.?
   - !! Последние инциденты с банками: злоумышленник представляется как администратор – кто остановит?
3. Любой связанный с деньгами документ должен иметь ЭЦП или имитоприставку. Авиабилеты, бронирование гостиниц и отдыха, обязательства турагенств и т.д.
4. ЭЦП эффективна только если есть **жесткое, конкретное, постоянное** в отдельные моменты времени регулирование и контроль.
5. Имитоприставка – как элемент системы «свой-чужой» эффективна только для централизованных систем

abaranov@hse.ru

Конфиденциальность

1. В АИС с большими объемами хранимой информации (от 100 Тбайт до 10 Пбайт) архивные носители не шифруются, т.к. каждый год их надо преешифроваывать на новых ключах.

   ? Что лучше - хранить в открытую или шифровать?

2. Прикладное ПО в актуальных АИС меняется каждый год. Зачастую с постоянной корректировкой базового ПО (версии ОС, СУБД, инструментария разработчика и т.д.). Прикладное ПО имеет объемы сотен Гбайт с 10^3-10^4 автоматизированных бизнес-процессов с использованием ЭЦП.

   ? Как быть с аттестацией по встраиванию?

3. Установка любого криптопровайдера на борту устройства гражданского пользователя проблемна. Хранение ключевой информации на устройстве массового пользователя также проблема.

   ? Может ли быть облачное шифрование?

abaranov@hse.ru

В каких направлениях необходима помощь регулятора

1. Перечни угроз фактически описывают противника!
   - ? Возможно ли создать официальное описание и перечень противников?
2. Описание противника необходимо для доказательства и обоснования целесообразности финансирования мер защиты.
3. Необходимо соотнести классы защиты по криптографии и техническим мерам защиты. Это можно сделать на уровне противника т.к. угрозы разные.
4. Проблема признания цены ущерба. Нужны официальные рекомендации. Рекомендации ГОСТ не работают.
5. Принципы защиты гостайны и коммерческой информации одинаковы, Кодексы разные.

abaranov@hse.ru

Актуальные темы исследований ближайшего будущего

- Методы определения цены информации и ущерба от инцидента ИБ
- Исходя из реальных успехов импортозамещения необходимо разработать подход к различному обеспечению ИБ систем различной степени конфиденциальности и ответственности (ГТ)
- Выделить классы систем, в которых реализуются различные варианты импортозамещения или импортоприменения
- Провести объективные, не ангажированные, признаваемые научно-технической общественностью сравнительные исследования продуктов на платформах open source и проприетарного ПО
- Оценить возможность и необходимость создания отечественного оборудования для применения в массовых системах

abaranov@hse.ru

Приглашаем принять участие

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

IV Международная научно-практическая конференция «Управление информационной безопасностью в современном обществе»

31 мая – 2 июня 2016 года

Высшая школа экономики

Москва, ул. Кирпичная, д.33

Регистрация на сайте

www.vipforum.ru

По вопросу участия обращайтесь в
Академию Информационных Систем
8 (495) 120-04-02

abaranov@hse.ru