ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

УГРОЗЫ БЕЗОПАСНОСТИ IT-ТЕХНОЛОГИЯМ В МАССОВЫХ ФИНАНСОВЫХ СИСТЕМАХ

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

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

abaranov@hse.ru, pbaranov@hse.ru

Основные массовые системы финансового сектора

- Е-банкинг и личные кабинеты различных назначений
- Отчетные системы и системы начисления платежей (ФНС, ГАИ, ПФ, ФТС, ФМС)
- Информационные сайты и порталы ведомств, организаций (ПГУ)
- Контрольные системы (ККТ, Маркировка, ЕГАИС)
- В массовых системах от 10^5 до 10^8 пользователей различной квалификации и устремлений. Реально имеет место многочисленный внутренний нарушитель

abaranov@hse.ru, pbaranov@hse.ru

Проблема стыковки требований различных регуляторов

- Требования к УЦ и ЭП со стороны ФСБ России и Минкомсвязи. Криптографическая компонента - ФСБ России – технический нарушитель. Организационно – оперативно – финансовая – Минкомсвязи
- Требования по защите ПД – ФСБ России и ФСТЭК России. Нет соответствия классов и уровней
- Требования к защите систем управления критическими технологиями (АСУ ТП) – ФСТЭК России. Требования к средствам обнаружения компьютерных атак ФСБ России. Нужна конкретная стыковка
- Совместный приказ ФСБ и ФСТЭК об утверждении требований к защите информации в ИС общего пользователя. Положительный пример

Пример попытки сведения в единую схему Защиты

	Системы и данные			
Механизмы ИБ	ПД 4 уровня	ИС общ. пользов. 2 уровня	АСУ ТП 4 уровня	ГТ 3 уровня
СЗИ НДС 4 подсистемы	+	–	+	+
НДВ 4 уровня	+	–	+	+
Контроль большого излучения	+	–	–	+
М Экраны 5 уровней	+	+	+	+
Шифровальные средства 5 уровней	+	–	+	+
ЭП и имитоприставка ЭП – 5 уровней	+	+	+	+
Защита от компьютерных атак	–	+	+	+
Оценка рисков	–	+	–	–
Мониторинг состояния системы Апостериорная защита	–	+	+	–

abaranov@hse.ru, pbaranov@hse.ru

Как проецируется схема Защиты на массовые системы

- Формально Е - банкинг и ЛК попадают под первые два столбца – ПД и ИС общего пользователя (ИС ОП)

  Вывод: Необходимо применять весь спектр механизмов ИБ
- Отчетные и контрольные системы – уже три столбца, ПД, ИС ОП, АСУ ТП.
- ГПУ - второй столбец, где отсутствуют необходимые требования доступности
- Ведомственные - применение подхода на основе оценки рисков не спасает. Кто апостериорно признает достаточно обоснованными эти оценки?
- Принципы защиты информации в системах различного уровня конфиденциальности и ГТ одинаковы, а кодексы правонарушений разные

Проблема оценки риска

- Цена риска соответствует формуле $S = E₽(\xi,\eta)$
  $\xi,\eta - 0,1$ случайные величины реализации угрозы и уязвимости, $₽(\xi,\eta)$ – функция цены
- Статистическая оценка $\hat{S}$ по n – независимым наблюдениям $s_1, \ldots, s_n$, имеет вид

$$\hat{S} = \frac{1}{n}\sum_{i=1}^{n} s_i \longrightarrow S \quad \text{при} \quad n \longrightarrow \infty \quad \text{т.е.} \quad n > 10$$

- Наблюдение и получение величин s_i, как следствие реализации одного вида угрозы и уязвимости случается у эксперта редко. Эксперты «распылены» в разных организациях
- Обеспечить $n > 10$ может только либо общественная организация фирм, либо регуляторы. Так можно создать официальный каталог рисков

abaranov@hse.ru, pbaranov@hse.ru

Требования регуляторов-кто противник?

- Требования к криптосредствам (ЭП и шифрование) фактически описывают не все возможности деструктивных воздействий, а только целенаправленное нападение
- Как корреспондируются требования ФСТЭК и угрозы безопасности. Какое отображение?
- Перечень угроз фактически описывает противника! Возможно ли создать официальный перечень угроз или типовых противников?
- Описание противника необходимо для доказательства и обоснования целесообразности финансирования мер защиты
- Цена ИБ - качество и сроки. Нужна разработка методов определения и признания цены ущерба

Примеры противника и его угроз

	Противник			
Угрозы	Кибер хулиган одиночка	Сообщество хулиганов	Преступное сообщество	Иностранные гос. структуры
Подбор пароля	–	+	+	+
Подмена sim карты пользователя	–	–	+	+
Исследование ОС на уязвимости	–	–	–	+
Использование вредных плагинов	–	–	+	+
Использование вирусных атак	+	+	+	+
Нарушение доступности ресурсов	–	–	+	+

abaranov@hse.ru, pbaranov@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, pbaranov@hse.ru

Приглашаем принять участие в мероприятиях

конференция РусКрипто

XVIII международная научно-практическая конференция «РусКрипто'2016»

22 – 25 марта 2016 года

Солнечный Park Hotel & SPA

Регистрация на сайте www.ruscrypto.ru

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

Регистрация на сайте www.vipforum.ru

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

СПАСИБО
ЗА ВНИМАНИЕ

abaranov@hse.ru
pbaranov@hse.ru