ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНЫЙ ИННОВАЦИОННЫЙ
ВНЕДРЕНЧЕСКИЙ ЦЕНТР
ГНИВЦ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ) БОЛЬШИХ ДАННЫХ (БД) В МАССОВЫХ 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

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Современные системы сбора и обработки больших (массовых) данных

ГНИВЦ

- Система: датчики (пользователи, граждане, сотрудники ведомства)
  - операторы системы, промежуточное звено (может не быть)
  - ЦОДы (ведомств, организаций)
  - потребители, контролеры, руководители
- Массовый характер датчиков $10^6 \div 10^8$
- Реально достигнутые объёмы собираемых, хранимых, обрабатываемых данных:
  от 100 Тбайт - 1 Пбайт
- Скорости для поступления информации: с мест (от датчиков) до 100 Мбит/сек, от операторов в ЦОДы до 10 Гбит/сек
- Конфигурация синхронизированных баз данных сейчас в ЦОДах со скоростью обмена 10 Гбит/сек. Реальная потребность в 2018 – 40 Гбит/сек, видна перспектива на 60-100 Гбит/сек (Infiniband)

abaranov@hse.ru, pbaranov@hse.ru

ИБ системы, работающей с БД

- Систему БД (СБД) необходимо рассматривать в комплексе: источники, обработка, использование данных, оценка результата. Одновременно, каждая часть – своя ИБ и модель угроз
- Внешние среды: среда, из которой черпают информацию датчики. Внешние взаимодействующие системы и их угрозы
- Постоянное обновление ПО на всех уровнях в силу изменения внешних условий (законодательство, новые задачи, новое железо, импортозамещение, новые ОС и СУБД)
- Злонамеренный и непреднамеренный (случайный) характер воздействия

  Z.B. CRC – существенно защищает от случайного искажения и бесполезно в качестве Хеш-функции
- Оценки рисков при злонамеренных действиях фактически есть в требованиях Регуляторов. Оценки рисков при случайном стечении негативных обстоятельств требуют анализа и проникновения в бизнес-процессы и не могут опираться на универсальные модели угроз

abaranov@hse.ru, pbaranov@hse.ru

Конфиденциальность 1 (простая)

- Триада: Конфиденциальность, Целостность, Доступность, должна быть адаптирована, как к самой СБД, так и к внешним средам
- Всегда в СБД (кроме технологических, где min-коммерческая тайна) имеются персональные данные (ПД). Большие и массовые СБД требуют дешевого КС–3, как минимум. Следовательно, нужна целостность всего ПО, включая прикладное, постоянно корректируемое
- Применению сертифицированных (квалифицированных т. е. сертифицированных) средств криптозащиты альтернативы не видно. Исключения по Закону

  Z.B. Налоговый кодекс

Конфиденциальность 2 (простая)

- Защита каналов передачи: самая разработанная задача. Для конфиденциальной информации можно применить «квалифицированный» SSL, но его реально нет для массовых датчиков (мультиоперационность, мультибраузерность). Может ли обычный гражданин выполнить все условия «квалифицированности» криптосредств и, следовательно, получить автоматическую юридическую значимость данных?
- Проблема «массового», неквалифицированного датчика в его слабой юридической защите. Достаточно только сертифицированного, обновляемого шифрования в прикладной задаче?
- Защита соединения ЦОДов требует:
  а) шифрования на уровне L2, чтобы пакеты не переставлялись при синхронизации баз данных;
  б) min задержки, не более на 0,1 - 0,5 мс

Конфиденциальность 3 (сложная)

- Конфиденциальность методов обработки данных. Что же они в Центре хотят выловить? В основном нужно найти и выправить преднамеренное искажение данных
  Z.B. В ФНС - что хотят известно (Налоговый Кодекс), а как – конфиденциально. В ПФ, ЕГАИС, Маркировка, ФТС аналогично
- Конфиденциальность алгоритмов обработки данных иногда отсутствует (ЕПГУ,СМЭВ,ОФД), но требуется защита ПД от НСД если данные расшифровываются в центре или у промежуточного звена
- Способы сбора и характер данных от датчиков могут много сказать о цели и методе обработки. Как скрыть детали алгоритмов в том числе от датчиков? Спрятать иголку в стоге сена

Конфиденциальность 4 (сложная)

- Основной метод защиты от НСД: – двухфакторная аутентификация и любые сертифицированные средства в ЦОДах; - разграничение полномочий датчиков, промежуточных звеньев и обработчиков, т.е. Замки и FW, Мониторинг и апостериорная защита с SIEM

  Z.B. ОЭД – отчетность не расшифровывает, а только подтверждает получение, а ОФД расшифровывает и должен иметь аттестацию, min, по 3 классу защиты ПД

- Разграничение доступа между различными ведомствами к ресурсам ЦОДов. Гарантии и контроль за действиями. Сейчас это на уровне offline, требуется смешанный режим с online и Java, для КС-3,при периодической, удаленной корректировке ПО

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГНИВЦ

Целостность 1

- Кто нарушитель и где? Массовый датчик нарушитель и угроза. Принудительная целостность: ККТ, Отчетность, АСК НДС-2, ГАС «Выборы», данные о производствах (ЕГАИС, Маркировка, Платон)
- Целостность и юридическая значимость ЭП это разные свойства. Неизменность блока данных и его авторство (с гарантируемой неотказуемостью). Проблема в рукописной доверенности
- Фиксация времени поступления данных. Единая Служба доверенного времени. Разные виды ЭП. Враг - внутренний и внешний нарушитель
- Достоверность, как разновидность целостности. Выявление преднамеренного вранья. Форматный контроль. Перекрестные тесты

Целостность 2

- Целостность системы обработки (ПО), связь с поиском НДВ и защитой от НСД. Доверенность Java – машины с разными ОС. Применение РМ попеременно в режиме online и offline
- Удаленная аутентификация датчика решаемая проблема при соответствующей организации научно-технических работ различных исполнителей
- Обеспечение «относительной» целостности ПО в условиях текущего постоянного изменения (совершенствования). Безопасный регламент обновлений. Удаленный разработчик и его РМ
- Блокчейн вне закона! Формирование блока - сплошная криптография, - Хеш, ЭП, SSL т.е. применяется достоверный, массовый, квалифицированный крипторовайдер, а его нет в России. Следовательно, это частная, корпоративная сеть. Какова устойчивость при компрометации части сети?

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГНИВЦ

Доступность

- Портал Госуслуг это переключатель или совокупность сервисов? Равнодоступность сервисов разных ведомств для датчиков
- Защита от компьютерных атак фактически апостериорно-априорная защита. Датчики захвачены врагами. Какова защита оперативных массовых критических систем на массовом сегменте
- Сколько и какие ЦОД нужны? ТИЕР – это катострофоустойчивость, а не доступность. Нужны требования по работоспособности и доступности систем по аналогии с системами критических технологий
- Защищенная доступность для контроля состояния датчиков и защищенные мобильные рабочие места контролеров. Защищенный мониторинг массы датчиков
- Возможность применения аналитических технологий личным составом без специального, дополнительного образования. «Простой» по восприятию результатов SIEM с рекомендациями по оперативным методам реагирования

abaranov@hse.ru, pbaranov@hse.ru

Приглашаем принять участие

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Магистерская программа «Управление ИБ»

приглашает на

V Международную научно-практическую конференцию
«Управление информационной безопасностью в современном обществе»

30 мая – 1 июня 2017 года

Высшая школа экономики
Москва, ул. Кирпичная, д.33

Регистрация на сайте
https://bm.hse.ru/bi/isconf2017/

По вопросу участия обращайтесь к
Елину Владимиру Михайловичу
ЭП velin@hse.ru
Тел. 8 926 174 41 46
8 926 774 41 46

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГНИВЦ

СПАСИБО ЗА ВНИМАНИЕ

abaranov@hse.ru
pbaranov@hse.ru