ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

ГЛАВНЫЙ
НАУЧНЫЙ ИННОВАЦИОННЫЙ
ВНЕДРЕНЧЕСКИЙ ЦЕНТР

ГНИВЦ

Бугры и выбоины на светлой дороге к СОПКА

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

СОПКА – общая схема

ГНИВЦ

1. ИТКС -> CIEM -> экспертная система (ЭС) -> корпоративный Центр -> Главный центр (ФСБ РФ)
2. ИТКС – информация циркулирует в зашифрованном виде, для анализа в ЭС ее надо расшифровать по схеме Т – подключения или по схеме «встреча по середине»
3. Скорости информационных потоков в ИТКС до 100 Гбит/с. Шифраторы на AES или ГОСТ по протоколам, например SSL или другим
4. Как расшифровать, мульткриптосхемный поток для направления и анализа в ЭС, на скорости более 1 Гбит/с для разных типов шифрования. Затем зачастую опять зашифровать. Это целая стойка для ОРМ
5. Разработка ЭС в области СОПКА имеет ряд проблем, характерных для систем искусственного интеллекта, которыми сами и являются. У кого есть ЭС для СОПКА?

abaranov@hse.ru, pbaranov@hse.ru

Призрачные надежды на быстрый успех

1. С помощью производителя разрабатываем схему подключения к СОПКА, соответствующую Вашей системе в данный момент. Фиксируем в Главном Центре
2. Все действующие системы модифицируются практически ежемесячно. Модернизируем схему подключения и направляем для согласования Главный Центр. Ждем ответа!
3. Организация разработчик подключения должна быть на договоре по сопровождению. Сегодня передаем по одним правилам, завтра - по другим
4. Разработчик подключения должен иметь варианты на новейшие изменения, требуемые прикладниками
5. Внутренние системы не должны подключаться к СОПКА, только имеющие подключения к Интернет! Иначе это двустороннее включение конфиденциальной системы в открытый мир.

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

СОПКА для корпоративных систем, а что для массового пользователя?

ГНИВЦ

1. Схема СОПКА: критическая корпоративная ИТС-узнаем, что есть инцидент компьютерной атаки– передаем информацию в Национальный центр (НКЦКИ) по закону № 187 от 26.07.2017
2. Возможная схема СОПКА для индивидуала: ПЭВМ – «внутренняя» программа – некий промежуточный центр обслуживания – НКЦКИ
3. Чего здесь нет? Есть ПЭВМ и НКЦИ, т.е. нет промежуточной стадии
4. Аналог - антивирусная служба. Плохо, что «внутренняя» программа, что-то докладывает о Вас в ФСБ РФ. Многие этого не захотят
5. Можно ли здесь построить бизнес? Например схема абонентского техобслуживания оборудования. Вызов специалиста по требованию клиента с небольшой абонентской платой или без нее

abaranov@hse.ru, pbaranov@hse.ru

Не удается сразу построить массовую схему ИБ. Начнем с хобота

1. Требования к массовой системе ИБ чрезвычайно высоки и в полном и даже значительном объёме невыполнимы
2. Индивидуальный пользователь плохо защищен. Нужен специфическим образом сертифицированный FW, защищающий от внешнего бот-агента
3. Проблема в широте применяемых ОС и средств ППО, а так же в низкой квалификации мысового пользователя. Нужен отечественный FW, устанавливаемый на ПЭВМ в режиме Plug and Play
4. Специфика сертификации в аналогии с КС1, т.е. независимости или слабой зависимости свойств FW от программно-аппаратного окружения
5. Промежуточный центр массового обслуживания СОПКА может предоставить гарантии неразглашения информации, поступающий с индивидуального ПЭВМ

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Устойчивость телекоммуникационной сети общего пользования и СОПКА

ГНИВЦ

1. Операторы связи России (ОСР) в количестве 2,5 тыс. являются элементами критической инфраструктуры. Их схема выхода на НКЦКИ аналогична общей?
2. Корпоративные пользователи КИИ подключены минимум к двум ОСР. Индивидуальные к одному. Как массовый пользователь ПЭВМ может обратиться в НКЦКИ, если его ОСР подвергся атаке и отключен от обслуживания?
3. Компьютерный инцидент это в том числе и техногенная авария (катастрофа) и отказоустойчивость. Инциденты с отказом оборудования подлежат компетенции НКЦКИ? Причина отказа выявляется много позже
4. Кто выдаст индульгенцию по отказоустойчивости? ГОСТ-Р.22.0.05-94 Безопасность в чрезвычайных ситуациях ТК71. ГОСТ-Р22.0.02

abaranov@hse.ru, pbaranov@hse.ru

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

СОПКА и GDPR

ГНИВЦ

1. GDPR – опять эти ЕС-овцы что то придумали, а мы к ним быстро присоединились и Роскомнадзор заверил, что у нас все хорошо
2. Суть GDPR в экстерриториальности требований по защите ПД граждан ЕС и высокий уровень санкций и штрафов, накладываемых инстанциями стран ЕС. Мы ждем первой реализации наказания за инцидент информационной безопасности
3. При всякой преднамеренной или непреднамеренной утечке в корпоративной ИТКС стараются ее скрыть от всех, включая СОПКА. С учетом GDPR скрывать надо еще тщательней в ручном режиме. Что получит СОПКА?
4. Необходимо разъяснение регуляторов о том, что выполнение закона № 152 полностью защищает владельцев ИТКС от GDPR и СОПКА не нарушает конфиденциальности ПД .

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ГНИВЦ

СПАСИБО ЗА ВНИМАНИЕ

abaranov@hse.ru