ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСТИТЕТ

ГЛАВНЫЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР

ОПЫТ МАССОВОГО ПРИМЕНЕНИЯ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ (ЭП)

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ РОССИИ
А.П. БАРАНОВ

ОБЪЕМЫ ВЗАИМОДЕЙСТВИЙ

ОПРЕДЕЛЕНИЯ:

ОРГАНИЗАЦИЯ – Юридическое или физическое лицо, использующее для взаимодействия автоматическую ИС (АИС)

ПОЛЬЗОВАТЕЛИ – Используют автоматизированные ИС

А) Взаимодействие пользователей с организациями Пользователей $>10^{7}$, организаций $>10^{6}$,

В) Взаимодействие организаций с организациями. Гос. организаций <100. Юридических лиц $<3 \times 10^{6}$

ВЫВОД:

В случае А связей более 10^{13}

В случае В не более 10^{9}

ХАРАКТЕР ВЗАИМОДЕЙСТВИЯ СО СТОРОНЫ ПОЛЬЗОВАТЕЛЯ

- Пример, система Портал Госуслуг или ведомственные порталы:
- Получение справочного материала - запрос – ответ
- Предоставление собственных материалов, включая отчетные, с обязательными сроками доставки и получения подтверждений
- On-Line взаимодействие через личные кабинеты пользователей

ХАРАКТЕР ВЗАИМОДЕЙСТВИЯ ОРГАНИЗАЦИЙ

- Госорганы с Госорганами: СМЭВ, МЭДО, ГАС «Выборы», ЕБД, ГИС ГМП и другие
- Частные связи через СМЭВ . ЦБ – ФНС, ПФ – ФНС, ФМС – ФНС, ССП – ФНС
- Основная среда взаимодействия – Internet. Частные сети виртуальны и криптографически защищены
- Везде требуется юридически значимый ЭДО и универсальная ,пригодная для разных сетей ЭП

ТРЕБОВАНИЯ К ЭДО В ПОЛЬЗОВАТЕЛЬСКОЙ (НЕ ПРИКЛАДНОЙ) ЧАСТИ

- Идентификация системы с которой происходит взаимодействие. Набираем ГИС ГМП, а нам предлагают Комрунет
- Юридический статус взаимодействия.
- Не всегда обязателен Федеральный закон № 63
- Идентификация (чтобы не приняли за другого) возлагается на пользователя
- Доступность организации для пользователя и наоборот. Юридическая верификация работоспособности транспортной сети

ТРЕБОВАНИЯ К ЭДО СО СТОРОНЫ ОРГАНИЗАЦИИ

- Идентификация пользователя или АИС. Проблема личного получения ЭП. Надежность ЕСИА из системы Госуслуг?
- Пользователь или хакер, как пользователь. Взломан личный кабинет пользователя?
- Нет требований по ИБ массового пользователя на его рабочем месте
- Не все АИС сертифицированы или аттестованы адекватно при связи с партнером
- Внутренний нарушитель опасен не только для АИС , где он легитимен
- Большой ИРУЦ при более , чем 100 УЦ

ПРОБЛЕМЫ ИБ, СВЯЗАННЫЕ С ЭП, ДЛЯ НЕСЕКРЕТНОЙ ИНФОРМАЦИИ

- Ключ SSL образуется с применением СКЭП
- В СКЭП сохраняется информация об АИС и организации пользователя. СКЭП – перегружен!
- Отечественные крипто-библиотеки не проверяют автоматически валидность СКЭП пользователя или организации. Это в приклад
- Нет технических требований к УЦ по доступности и сроках отзыва СКЭП
- Аналитические сегменты АИС могут требовать проверки валидности старых типов СКЭП

ПРОБЛЕМЫ ИБ АИС, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ ПРИМЕНЕНИЯ ЭП

- Отечественный SSL не используется массовым пользователем, т. к. плохо встраивается в обновления ОС
- Юридическая значимость под вопросом, т. к. способ отображения информации не определен
- По прежнему актуально решение по своевременной сертификации при обновлении средств ЭП в модернизируемом ПО
- Сертификация ИБ, включая ЭП в «больших» системах типа ГИС ГМП, «новый» СЭДО, Госуслуги проблематична
- Наблюдается рост ценности персональных данных

ВЫВОДЫ

- Имеется отставание законодательного обеспечения развития рынка применения ЭП. Автономизация. Федеральный Закон № 63 в этом году вступил в полную силу и сразу устарел
- В силу объективных причин регуляторы перегружены техническими функционалами, с которыми не справляются в требуемое, короткое время
- Общественная инициатива по созданию СРО в области ИБ запаздывает. Требуется признание фактической необходимости СРО со стороны регуляторов

СПАСИБО

ЗА ВНИМАНИЕ