# Безопасность применения электронной подписи(ЭП) в условиях информационного противоборства

ЭП применяется каждым субъектом взаимодействия фактически в его собственных критических информационных инфраструктурах (КИИ), возможно, формально к ним не относящихся по Закону. Противоборство между личными КИИ и нападающей стороной приобрело массовый характер с использованием любых возможностей

# Противоборство в компьютерной сфере

- Противоборство- форма поведения в конфликтной ситуации, которая может привести к доминированию и в конечном итоге к уничтожению одного из оппонентов конфликта. Все средства- хороши, включая оперативные
- В противоборстве, защита в компьютерной сфере рассматривается традиционно как реакция на способы нападения, описанные моделью угроз, которая строится на основе модели защищаемой компьютерной системы(КС)
- Способы нападения формулируемые как компьютерные атаки разрабатываются в специальных ведомствах, зачастую не подлежат разглашению и поэтому не учитываются в публичной модели угроз для безопасников, отстающих от нападения, а массовому индивидууму приходится полагаться только на себя или производителя технологии
- Перечень угроз от регуляторов насчитывает более 200 позиций. Число возможных комбинаций из них 2 в степени 200 т.е. 10 в степени 60, что показывает невозможность анализа всех возможных способов нападения

# Агрессивное нападение на документ

- Поскольку формально- логических доказательств безопасности сложных КС не существует, уверенность в эффективности защиты появляется ,как следствие отсутствия эффективной атаки в круге известных, эффективных методов нападения
- По умолчанию считается, что все открыто опубликованные стандарты и форматы не содержат скрытых возможностей, поскольку могут быть в принципе выявлены. Однако, применяемая конкретным пользователем КС п может содержать реализации , которые никто не проверял и которые могли попасть в КС, например, в входе очередного обновления ОС по Интернет, как это происходит при обновлении современных версий Windows
- Массовый пользователь не может определить наличие этих «дополнений» и вынужден полагаться на Авось. Фиксация КС массовым пользователем без применения специальных мер информационной безопасности вызывает затруднения в добавлении ППО, что ограничивает расширение функционала
- Документ –продукт КС и при его подготовки так же может содержать «дополнения» неизвестные пользователю. «Вирусные» вставки есть в обиходе хакеров при «Соц. Инженерии», а не только агрессоров-спецслужб
- Документ на бумаге не содержит недокументированных возможностей?

# Сертификат и проверка его владельца в УЦ

- Проверка соответствия принятого битового файла прикрепленной к нему ЭП должна сопровождаться контактом с удостоверяющим центром подписанта или через портал Госуслуг. Требования по доступности АУЦ содержатся в Приказе Минцифры 584 от 13ю11.20 раздел 12 п.г и п.з в общем виде и фактически ориентируются только на доступ через Интернет
- Повсеместно распространилась практика использования графического штампа с ФИО подписанта, сертификатом ЭП, не удобным для визуальной проверки – 20, буквенно- десятичных символов  и без самой ЭП,  со ссылкой на ее наличие в электронной копии. ЭП БОМЖа  легальна и корректна!
- В потоке документооборота должна быть обязательной проверка ее по электронному исходнику, что требует скорости, а  атака на доступность УЦ в любое время при противоборстве может иметь много вариантов вплоть до персонального зашумления канала связи проверяющего Э
- Выход из тупика в регулярной публикации отмеченного соответствия на бумаге известен давно, но не практикуется УЦ из-за неудобства получения бумажной версии и постоянного ее обновления

# Атака на получателя

- Предметом защиты ЭП является документ различных форматов включая видео файлы, изначально формируемый в определяемой исполнителем компьютерной среде(КС), который может оказаться жуликом(БОМЖом)
- Получатель документа, защищенного от искажений посредством ЭП, не знает КС изготовителя, ориентируясь только на форматы и стандарты, присутствующие в заголовке файла. Например, JPEG, а в нем исполняемая вирусная вставка. ЭП может быть оформлена на БОМЖа и удостоверена в УЦ
- «Транзитная» атака на получателя, как следствие комплексного нападения. Автор документа может не знать его опасности и использоваться злоумышленниками «в темную», например для «вирусного» заражения
- Антивирусные продукты ограничены в возможностях защиты от атак, использующих «дополнительные возможности железа»- «закладки»
- Противоборство в настоящее время демонстрирует использование «закладок» не только спецслужбами, но и хакерскими элементами
- Подставная сотовая станция теперь умещается в чемодане, в разы подешевела и создает полную иллюзию работы в Интернете на смартфоне или планшете уже на расстоянии в сотни метров

# Бумажный вариант документа и ЭП

- Бумажный вариант и ЭП изготовляются автором на КС в условиях противоборства и бинарный, подписываемый фаил может отличаться по содержанию от верифицируемого на экране текста с «правильной» ЭП
- Ныне практикуется вариант документа с штемпелем о подписании ЭП с приведением сертификата и параллельным направлением электронного документа с ЭП. Как правило секретариаты, не проверяет легитимность ЭП через запрос УЦ. Проверка зарегистрированной фирмы на БОМЖа вообще проблема, связанная с установлением легитимности деятельности. СПАРК ?
- Бумажный и электронный документы могут отличаться хотя бы из-за разности версий шрифтов. «Правильно» подобранная хитрость может исказить в бумажной версии хотя бы один символ. Например, ноль 0 и О
- Проверять напечатанную на бумажной версии ЭП бессмысленно т.к. получить электронный авторский образ в его КС невозможно. Сканирование и перевод PDF файла в WORD  или другой формат дает отличный от авторского файл и его ЭП будет другой
- Аналогом бумажного файла с ЭП может быть другой отчуждаемый носитель, который визуализируется на доверенной КС. Пересылка токена почтой не практикуется, а это дополнительный канал защиты

# Децентрализованные системы в эпоху противоборства

- Объемы добычи и, следовательно, финансовые возможности хакеров возросли, что делает их нападение Комплексным, сравнимым с действиями спецслужб, а широта охвата пользователей массовой атакой, в которой даже маловероятный успех можно далее распиарить в сети представив его , как широкомасштабное наступление в информационном противоборстве и компрометацию идеи применения ЭП тем или иным важным ресурсом
- Казавшийся незыблемым блокчейн на самом деле устойчив только в предположении, что все КС работают т.к. предписано стандартами и описаниями разработчиков. Среди миллионов пользователей всегда находятся или могут быть специально созданные «слабые» элементы
- Криптовалютные биржи оказались зависимыми от порядочности администраторов, которой в ряду случаев не нашлось места (FTX, CoinCheck), а устойчивость мер массовой защиты недостаточной (маркетплейс Silk Road и др.)
- Борьба за деньги использует все легальные и преступные методы, как информационно- технические, так и негативно оперативные

# Как усилить позицию защиты ЭП в массах

- Зафиксировать набор надежных средств визуализации документов и в заголовке указывать его
- Поскольку всю КС в массовом порядке иметь доверенной невозможно, обработку документа начиная с демонстрации текста и выработки хеш функции следует поручить личному, устойчивому к изменению, отдельному устройству и только в некотором едином фиксированном на государственном уровне формате. Например, на отечественной, выверенной реализации аналога PDF, а лучше на собственной разработке
- Безопасность дешевой не бывает, бывает дешевая информация, которая не представляет ценности автору или получателю. Для малоценной информации предлагается законодательно разрешить использовать незащищенную КС
- Шифрование с применением имитоприставки сертифицированного вида усиливает защищенность документа и его ЭП. Может его добавить в КБ,КА?
- Информационное противоборство допускает не только информационные атаки , но и альтернативные, оперативные виды компрометации участников информационного обмена, включая фальшивую сотовую станцию и БОМЖа
- УЦ необходимо сосредоточиться на скорости восстановления системы и на недопущении утечки массива ПД, которые более всего компрометируют его