Что не так с федеральным законом «Об электронной подписи» (63-ФЗ), и как это можно исправить

Рисовальная машина за работой, © axisdraw.com

Электронная подпись в России впервые появилась в январе 2002 года вместе с принятием первого закона «Об электронной цифровой подписи» (1-ФЗ). Затем, спустя 9 лет, в апреле 2011 появился новый закон «Об электронной подписи» (63-ФЗ). Спустя еще 8 лет, в начале лета 2019, в СМИ стали появляться леденящие душу публикации о том, как с помощью электронной подписи воруют квартиры, как мошенники оформляют на ничего не подозревающих граждан фиктивные фирмы, и так далее, и тому подобное.

Давайте без лишних эмоций попробуем разобраться в сложившихся проблемах и подумаем, как их можно исправить.

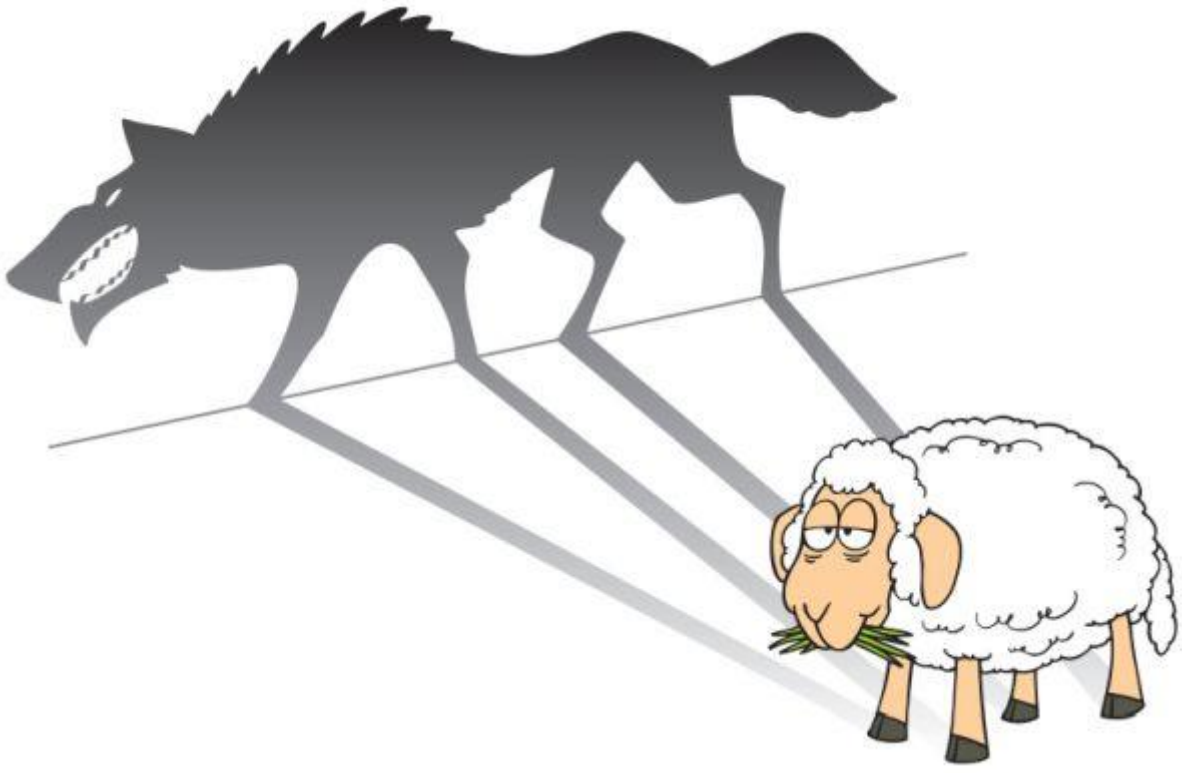
Содержание

Предисловие

- В данной статье речь пойдет только об **усиленной квалифицированной электронной подписи** (далее по тексту — электронная подпись).
- Везде, где упоминаются удостоверяющие центры, речь идет об аккредитованных удостоверяющих центрах.
- Для упрощения восприятия в статье частично используются «народные» термины вместо строгих юридических понятий.

Часть 1 — проблемы законодательства

Проблема № 1 — идентификация клиентов удостоверяющими центрами



© Яндекс.Картинки

С точки зрения информационной безопасности все перечисленные в начале статьи инциденты произошли в результате **недостаточной идентификации работниками удостоверяющих центров своих клиентов**. Но почему же так происходит в организациях, которым для своей работы требуются лицензия ФСБ России и аккредитация от Минкомсвязи?

Ответ прост: удостоверяющие центры зарабатывают с количества проданных электронных подписей. Ужесточение процедур идентификации клиентов снизит их прибыль.

Все люди хотят, чтобы все было просто, быстро, бесплатно и без усилий. Когда подобный человек обращается в удостоверяющий центр, он хочет мгновенно получить электронную подпись, да такую, чтоб не украли, и обязательно без всяких паролей и прочих глупостей. Человек, получающий подпись, как правило, получает ее не для себя, а для директора или бухгалтера той компании, где он работает. У человека, кроме получения подписи, еще уйма дел. Если человеку говорят, что доверенность, по которой он хочет получить подпись, должна быть нотариально заверенной, то человек считает это жуткой бюрократией. В следующий раз, когда человек захочет получить новую электронную подпись, он постарается обратиться в другой, более «клиентоориентированный» удостоверяющий центр.

Таким образом, мы получаем ситуацию, когда быть правильным удостоверяющим центром, проводящим строгую идентификацию клиентов, невыгодно. Всегда найдется другой удостоверяющий центр, относящийся к данному вопросу менее трепетно, чем и будет завлекать ленивых клиентов.

Оформление злоумышленниками поддельных сертификатов это не проблема какого-то конкретного удостоверяющего центра, а системный кризис уровня федерального законодательства. Можно сказать даже больше — это глобальная проблема (примеры тут и тут) самой технологии PKI, лежащей в основе закона.

Проблема № 2 — ограничение использования электронной подписи

Электронные подписи, как и любые другие технологии, переживают определенные циклы развития. Текущий закон «Об электронной подписи» — это закон этапа популяризации технологии (электронная подпись уже используется обществом, но ее проникновение все

еще далеко от повсеместного). В следствие этого закон больше ориентирован на массовость, нежели безопасность электронной подписи.

Единственный механизм ограничения использования электронной подписи приведен в п. 4 ст. 11 63-ФЗ. Там, в частности, говорится о том, что квалифицированная электронная подпись должна использоваться в соответствии с ограничениями, указанными в сертификате ключа подписи. К сожалению, данная формулировка не позволяет полностью запретить выпуск и использование электронной подписи, в результате чего от электронной подписи страдают граждане, которые никогда в жизни ее не выпускали (например, жертвы приведенных в начале статьи инцидентов).

Особо остро проблема ограничения использования электронной подписи касается должностных лиц.

В данный момент они вынуждены жертвовать личной безопасностью в угоду интересов работодателя. Это, в частности, проявляется в том, что электронная подпись, выпускаемая на них для удовлетворения нужд компании, может быть использована против их личных интересов, например, для неправомерного переоформления квартиры в Росреестре.

Проблема усугубляется тем, что количество людей, которым может оказаться доступна электронная подпись должностного лица, трудно поддается ограничению и практически не зависит от воли владельца подписи. В качестве примеров людей, которым может стать доступной электронная подпись должностного лица, можно привести:

- администраторов средств криптографической защиты информации (СКЗИ), ответственных за выпуск криптографических ключей и в том числе ключей электронной подписи;
- ИТ-работников, настраивающих информационные системы для использования электронной подписи;
- аудиторов, осуществляющих проверку работы организации (например, пентестеры);
- сотрудников государственных контрольных органов, осуществляющих в отношении организации контрольные мероприятия;
- сотрудников правоохранительных органов, проводящих в отношении компании работодателя оперативно-следственные мероприятия;
- команду конкурсных управленцев, руководящих компанией, если та инициировала процедуру банкротства;
- и, как ни печально, других лиц.

Проблема № 3 — получение извещения о выпуске электронной подписи

(c) м/ф «Трое из Простоквашино»

Инциденты с неправомерным использованием электронной подписи по сути своей очень похожи на кибер-кражи, осуществляемые злоумышленниками через системы «Интернет клиент-банк». В обоих случаях злоумышленники, завладев аутентификационной информацией жертвы, незаконно осуществляли от ее имени юридически значимые действия: снимали деньги со счета, оформляли кредиты, осуществляли регистрации фирм-однодневок и т. д.

Одним из эффективных способов снижения ущерба от кибер-краж стало предоставление банками возможности своим клиентам самостоятельно бороться за свою безопасность. Любой клиент, используя услугу уведомления об операциях по счету (например, SMS-информирование), может самостоятельно выявить несанкционированную операцию и заблокировать счет, чтобы минимизировать ущерб.

Текущий закон «Об электронной подписи» подобных форм защиты не предоставляет. В нем нет механизмов уведомления владельца о выпуске на его имя электронных подписей.

Проблема № 4 — правила использования СКЗИ

(c) Яндекс.Картинки

Текущая законодательная база, регулирующая использование электронной подписи, содержит требование по обеспечению безопасности, которое, в конечном счете, может привести к обратному эффекту и создать прецедент для оспаривания подписи. Разберем все по порядку.

П.п. 2. п. 4 ст. 5 63-ФЗ устанавливает требования к квалифицированной электронной подписи: *«для создания и проверки электронной подписи используются* ***средства электронной подписи, имеющие подтверждение соответствия требованиям****, установленным в соответствии с настоящим Федеральным законом».*

Указанные требования к средствам электронной подписи определены в Приказе ФСБ РФ от 27.12.2011 N 796. В п. 6 данного документа сказано, что средства электронной подписи (а это — СКЗИ) должны эксплуатироваться в соответствии с ПКЗ-2005. Там, в свою очередь, зафиксировано, что средства электронной подписи (СКЗИ) должны **эксплуатироваться в соответствии с правилами пользования ими (технической документацией)**.

Тут сразу возникает вопрос, будет ли считаться электронная подпись квалифицированной, если она сделана с помощью сертифицированного СКЗИ, эксплуатируемого не в полном соответствии с правилами пользования (технической документацией).

Однозначного ответа на данный вопрос законодательство не содержит. Следовательно, учитывая состязательность российского судопроизводства, по схожим делам будут выноситься диаметрально противоположные решения, что в конечном счете может привести к снижению доверия к электронной подписи, и сделает ее более уязвимой к атакам на неотрекаемость.

Для иллюстрации данной проблемы рассмотрим ситуацию, часто возникающую при получении квалифицированных сертификатов ключей подписи в удостоверяющих центрах. Суть ее в том, что срок действия сертификата может быть определен в 5 лет, а срок действия закрытого ключа (расширение PrivateKeyUsagePeriod OID 2.5.29.16) в 1 год и 3 месяца. Возникает вопрос, будет ли признаваться квалифицированной электронная подпись, созданная на 3-й год существования подобного сертификата?

Проблема № 5 — стандартизация средств электронной подписи

(c) Яндекс.Картинки

Если вы когда-нибудь сталкивались с настройкой компьютеров для осуществления юридически значимого электронного документооборота с гос. органами, то наверно помните тот ад, что при этом возникает. Жонглирование версиями криптопровайдеров, браузеров и плагинов, в результате которого система начинает хоть как-то работать, не поддается научному объяснению. Данное действо больше похоже на танец шамана, взывающего к духам бури, земли и огня у ночного костра.

При этом радость от успешной настройки быстро сменяется жуткой депрессией, когда выясняется, что работнику, для которого выполнялась настройка, нужно посылать отчеты в еще один гос. орган. А там свое СКЗИ, свои ключи и вообще всё свое. Ну и вишенкой на торте конечно же является тот факт, что два сертифицированных СКЗИ на одном компьютере в принципе не уживаются.

Таким образом, в копилку проблем текущего закона можно смело добавить отсутствие стандартизации и совместимости между СКЗИ, используемыми для формирования и проверки квалифицированных электронных подписей.

Постановление Правительства РФ от 09.02.2012 N 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при

организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» не в счёт, так как распространяется только на межведомственное взаимодействие, да и по сути не дает никакой конкретики.

Проблема № 6 — старые подписи

(c) Яндекс.Картинки

Давайте зададимся вопросом, что будет с документом, подписанным электронной подписью через 30 лет, а через 100 лет? Откуда такие сроки? Все просто: для сделок с недвижимостью характерно длительное владение собственностью. Вот поэтому и 30 лет, и 100 лет — не предел. Например, Александр II продал Америке Аляску в 1867 году, то есть 152 года назад.

Но вернемся к электронной подписи. С точки зрения технологии ее стойкость базируется на математических свойствах криптографических алгоритмов, лежащих в ее основе. При этом стойкость самих алгоритмов базируется лишь на незнании эффективных способов их взлома. Далеко не факт, что данных способов нет, или что они не появятся через 37 минут. Например, в эпоху продажи Аляски шифр Виженера считался неуязвимым, а сейчас его ломают студенты на первых лабораторках по криптографии.

Текущий стек криптографических алгоритмов, используемых для электронной подписи в России, базируется на ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 34.12-2015 и еще немереного числа рекомендаций по стандартизации и алгоритмов спутников. Что будет с ними через 30 лет? Есть мнение, что с ними уже сейчас не все здорово.

Проблема уязвимостей в алгоритмах и средствах электронной подписи не является чисто гипотетической. Мировая практика уже столкнулась с подобными вещами, например, уязвимость ROCA.

Таким образом, очередная проблема закона — это отсутствие регулирования, направленного на поддержание долговременной юридической значимости электронных документов.

Проблема № 7 — «атака назад в будущее»

(c) киносказки Александра Роу

Данная атака — это, пожалуй, осиновый кол в сердце электронного документооборота, использующего для заверения документов только электронную подпись.

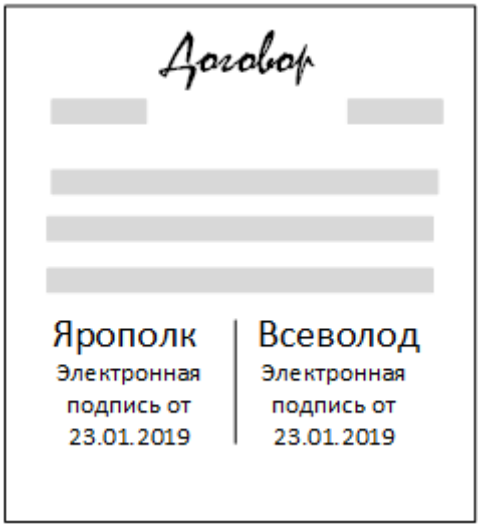
Проблема в том, что, манипулируя с датой формирования электронной подписи, злоумышленник может добиться как признания поддельной подписи, так и отрицания легитимной.

Жил был Ярополк и руководил он артелью заморских каменных дел мастеров. По просьбе заказчика своего, Всеволода, решил он упростить обмен бумагой окаянной и оформил себе квалифицированный сертификат электронной подписи.

Пример 1 - признание поддельной подписи

Ярополк и Всеволод договорились, что вместо бумажных пергаментов, от руки написанных, будут они по почте электронной слать друг другу файлы, в редакторе MS Word составленные и подписью электронной с помощью СКЗИ КриптоПРО и ПО КриптоАРМ

заверенные. По наставлению волхвов, в том толк знающих, решили дату подписи документов прописывать в файлах электронных перед их заверением.



Записали все это на пергаменте и скрепили подписями своими, назвав сей документ «Соглашением об электронном документообороте».

Долго ли, коротко ли работали они по такой схеме. Но затем жадность жабою тяжелою грудь Всеволоду сдавила, навевая мысли темные о том, что платит Ярополку он слишком дорого. Начали думы горькие изводить Всеволода по-разному: сна лиши, да настроение испортили.

Решил Всеволод с горем своим обратиться к знахарке местной, Бабой-Ягой величать которую. Та за плату щедрую надоумила Всеволода закрытый ключ электронной подписи у Ярополка выкрасть. Как известно, ключ тот содержался в приборе заморском, яйцо напоминающем (USB токен), в заднюю часть компьютера постоянно воткнутом.

Для плана своего коварного нанял Всеволод блудницу кареглазую, чтоб та чарами своими амурными разум Ярополку затуманила и в тридевятое царство съездить надоумила.

Пока в путешествии заморском Ярополк с блудницей развлекался, Всеволод в тайне прокрался в палаты белокаменные и прибор, яйцо напоминающий, ключ Ярополка содержащий, из задней части компьютера вынул и сбежал с ним.

Но не знал Всеволод, что перед отъездом своим Ярополк чары охранные на палаты свои наложить попросил. Чары те сработали и сигнал в дружину городскую направили. Прибыв на место и не найдя ворогов лютых, дружинники челядь Ярополка вызвали, чтоб та проверила, не украдено ли добро какое-нибудь ценное. Приказчик Ярополка обнаружил пропажу «яйца» заветного, ключ электронной подписи содержащего. Памятуя заветы волхвов, он немедленно к мастерам обратился, что «яйцо» то изготовили, чтоб заклятиями своими силу «яйца» они изничтожили. Мастера, следуя заветам предков, добавили сертификат электронной подписи Ярополка к списку отозванных сертификатов и наказ дали, чтоб Ярополк «яйцо» то не пользовал, даже если оно сыщется, и чтоб к ним он скорее за новым «яйцом» явился, новую электронную подпись получить.

Всеволод узнал все это и еще больше пригорюнился. Отправился он с думами тяжкими к Бабе-Яге за советом мудрым. Узнав о горе Всеволода, Баба-Яга закатилась злобным хохотом и, проржавшись, молвила: «Это не беда! А делать тебе нужно следующее:

1. Запусти свой компьютер и переведи дату на три месяца назад, когда ключ Ярополка действовал еще.
2. Составь документ новый и напиши в нем, что Ярополк взял у тебя денег множество и с процентами отдать обязуется через три месяца.
3. В качестве даты подписания документа укажи дату, что на компьютере у тебя будет.
4. Подпиши документ сей своей электронной подписью и подписью Ярополка».

«Чует мой дух,» — сказала старуха — «что Ярополк на „яйце“ пароль по умолчанию оставил».

Всеволод так и сделал и через суд забрал у Ярополка денег видимо не видимо.

Так как, согласно п.2 ст. 11 63-ФЗ: «Квалифицированная электронная подпись признается действительной… при одновременном соблюдении следующих условий:… квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;» документ липовый, Всеволодом составленный, судьей годным признан был, поскольку подписью Ярополка был заверен, а дата формирования подписи с периодом, когда подпись действовала, совпадала. Оспорить дату эту окаянную Ярополк не смог, поскольку та по всем правилам «Соглашения об электронном документообороте» была поставлена.

Пример 2 - отрицание легитимной подписи

Раздосадованный трагедией ужасной, денег уйму стоящей, решил Ярополк отомстить Всеволоду, да так, чтоб той же монетой, чтоб по справедливости.

Принялся Ярополк читать писание, закон 63-ФЗ содержащее. Читал, читал… да и уснул. И приснился ему муж величавый, ликом Вещевого Олега напоминающий. Взирал тот муж на поле ратное, где полчища басурман поверженных кровью своей поганою Русь святую пачкали, и гласил речи грозные: «Кто к нам с чем за чем, тот от того и того...». По утру проснулся Ярополк в бодром здравии, ибо знал он теперь, что делать ему надобно.

Пришел Ярополк к Всеволоду и слово молвил, что, несмотря на все разногласия, у мастеровых его семьи, да дети малые, что без работы худо им, и предложил строить палаты белокаменные вместе и далее. Услышав это, Всеволод несказанно возрадовался и сообщил, что не против он продолжения сотрудничества, но платить будет по справедливости, то есть в два раза меньше прежнего.

Ярополк предложение то принял, но сказал, что «Соглашение об электронном документообороте» поменять надобно: слова про дату подписания документов от туда выкинуть. Также добавил он, что раз денег за работу вдвое меньше будет, то надобно аванс ему выдать, да наличными, чтоб мог он камня строительного привести, да часть жалования

мастеровым выдать. За деньги полученные расписку он составит безбумажную, электронной подписью заверенную. На том и порешили.

Выдал Всеволод аванс Ярополку и получил взамен расписку электронную.

После этого пошел Ярополк к мастерам, что «яйцо» с электронной подписью изготовили, и попросил новое «яйцо» сделать, так как старое у него лихие люди вместе с кошелем в подворотне похитили. Мастера отозвали подпись старую, да «яйцо» с новой выдали.

Проходит неделя, другая, а Ярополк работы и начинать не думает. Разгневался Всеволод и вызвал Ярополка, чтоб испросить с него за бездействие. А Ярополк слово молвит, мол денег аванса он так и не получил, не на что камень строительный приобрести. Всеволод почуял неладное, да в суд на Ярополка опять подал.

Во время слушаний предъявил Всеволод судье мудрому расписку электронную, подписью Ярополка заверенную. На что Ярополк ответил: «Подписка та поддельная лихими людьми составлена, что „яйцо“ его похитили».

Для разрешения спора этого сложного запросил судья у мастеров, что подпись Ярополку выпустили, дату отзыва подписи его электронной, так же вязл судья у Всеволода оригинал «Соглашения об электронном документообороте».

Поскольку соглашение то не содержало слов о том, что считать датой подписи электронного документа, а также, учтя тот факт, что стороны не пришли к согласию относительно самого факта подписи и соответственно даты ее совершения, судья мудрый принял решение, что дата электронной подписи электронного документа достоверно не определена.

После этого обратился он к п.2 ст. 11 63-ФЗ: *«Квалифицированная электронная подпись признается действительной… при одновременном соблюдении следующих условий:… квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа)* ***или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен****».*

На основании всего выше сказанного суд пришел к выводу, что электронная подпись под документом не действительна, так как дата подписания документа достоверно не определена, а на момент проверки подписи ее сертификат не действителен.

Часть 2 — работа над ошибками

Государство vs. удостоверяющие центры

Услышав о проблемах закона «Об электронной подписи», люди в первую очередь предлагают упразднить удостоверяющие центры и передать их функции государству. Одним из основных аргументов сторонников этой точки зрения является то, что эти «шарашкины конторы» не могут обеспечить безопасность предоставляемых услуг и сами являются потенциальными участниками конфликтов интересов (могут неправомерно выпустить подпись третьего лица и ей воспользоваться).

Следует отметить, что данные мысли не лишены логики, но для принятия взвешенных решений нужно учитывать и другие нюансы.

Экономические аспекты взаимодействия государства и частного бизнеса

Государство в эпоху цифровой экономики — это провайдер инфраструктурных сервисов, позволяющих экономике существовать и развиваться. Глобализация — неизбежный спутник цифровизации экономики — серьезно обострит конкуренцию между государствами. Инвестиции и человеческий капитал будут направляться в те страны, государственные сервисы которых наиболее эффективны.

Для победы в конкурентной борьбе государству, как и бизнесу, нужны инвестиции. Где их взять?

Увеличивать налоги — не вариант, так как это приведет к снижению эффективности гос. сервисов: за ту же работу государство будет брать больше. Где еще тогда можно взять деньги?

Наиболее перспективными вариантами получения инвестиций являются государственно-частное партнерство и делегирование бизнесу части государственных полномочий. В качестве примеров подобного взаимодействия можно привести:

- частные охранные предприятия, которым государство делегировало часть своих функций по обеспечению безопасности;
- удостоверяющие центры, которым государство делегировало часть своих функций по формированию электронного пространства доверия;
- владельцев частных камер видеофиксации нарушений правил дорожного движения, которым на основании концессионных соглашений разрешено устанавливать камеры и зарабатывать на выписке штрафов автолихачам.

Таким образом, мы приходим к выводу, что государство всеми силами должно сохранить вовлеченность частного бизнеса в реализацию своих функций, обязательно обеспечив должный уровень их качества. В противном случае подобное взаимодействие несет больше вреда, нежели пользы, и от него лучше отказаться.

Дополнительным аргументом в пользу сохранения коммерческих удостоверяющих центров как общественных институтов, как ни странно, является человеческий фактор. Сам факт того, что человек служит в госоргане, а не трудится в частной фирме, не делает его честней и порядочней.

Если человек не проводил идентификацию заявителя на выпуск электронной подписи, будучи работником коммерческого удостоверяющего центра, то он не будет этого делать и будучи госслужащим. Для того чтобы процесс заработал, нужны дополнительные усилия: грамотная мотивация труда, обеспечение контроля и др. Все эти меры можно успешно реализовать как в коммерческих компаниях, так и в госструктурах — в общем случае разницы нет.

С учетом вышесказанного в данной статье мы будем исходить из того, что коммерческие удостоверяющие центры будут и дальше продолжать выпускать электронную подпись.

Решение проблемы № 1 («идентификация клиентов удостоверяющими центрами»)

Для обычного гражданина получение электронной подписи по значимости равносильно получению национального паспорта. По сути это два практически равносильных удостоверения личности, только первое — для реального мира, а второе — для «цифрового». Раз ценность удостоверений равна, то и защита их также должна быть равносильной. Другими словами **электронная подпись должна выдаваться столь же строго, как и паспорт**.

Но все же по сравнению с паспортом у электронной подписи есть важные отличия:

1. Если паспорт выдается на длительный срок (десятки лет), то электронная подпись — на короткий, как правило, не больше года и трех месяцев.
2. Обладание паспортом не требует специальных знаний. Обладание же электронной подписью требует. Например, при использовании электронной подписи часто возникают сугубо ИТ-шные вопросы, требующие оперативной технической поддержки.
3. Для того чтобы воспользоваться краденными паспортом или электронной подписью, злоумышленник должен преодолеть их систему защиты, например, переклеить фотографию в паспорте или взломать пароль на электронной подписи. При этом определить, что злоумышленник воспользовался краденным паспортом, можно по показаниям очевидцев или записям видеонаблюдения, установить же факт неправомерного использования электронной подписи практически невозможно.

Паспорта выдает МВД России. Следуя принципу равной защищенности, рассмотренному выше, получается, что оно же должно выдавать и электронные подписи. Однако, сделать это в рамках существующей структуры МВД России невозможно:

- Во-первых, потому что наряду с государственными функциями (идентификация, учет и контроль удостоверений личности, ...) МВД потребуется выполнять еще сугубо ИТ-шные функции: техническая поддержка, консультации и др.
- Во-вторых, для МВД потребуется организовать закупки технических и криптографических средств в массовых масштабах, а это будут гигантские бюджетные траты.
- В-третьих, МВД потребуется существенно расширить штат, так как количество выпускаемых / отзываемых электронных подписей существенно больше аналогичного количества паспортов.

Здесь упоминается МВД России, но приведенные рассуждения будут справедливы и для любых других гос. структур. Как ни крути, а затраты государства на передачу функций удостоверяющих центров в любой из своих органов будут гигантскими. Реальный экономический эффект, выраженный в снижении потерь от экономических преступлений, связанных с использованием электронной подписи, вряд ли будет значительным.

Оптимальный вариант решения сложившейся проблемы видится в совершенствовании процедуры выпуска электронных подписей. В частности, предлагается следующий набор мер:

1. Запрет оформления электронной подписи по доверенности (паспорт по доверенности получить нельзя).
2. Законодательное принятие методики идентификации заявителей на оформление электронной подписи, как минимум включающей в себя:
    - наличие не менее двух людей, проводящих идентификацию заявителей своими глазами (как во многих банках при оформлении вкладов или кредитов);
    - наличие процедур проверки документов, удостоверяющих личность заявителя, на предмет подделки.
3. Обязательная фиксация процедуры идентификации личности заявителя на фискальный видеорегистратор (исключающий возможность подделки видеозаписей) и хранение записей в течение 3 лет (срок исковой давности) со дня окончания срока действия сертификата ключа подписи.

Основным нюансом данного набора мер будет выбор второго человека, проводящего идентификацию личности заявителя на выпуск электронной подписи. Рассмотрим несколько вариантов, отличающихся друг от друга ожидаемой достоверностью идентификации и затратами на реализацию. Вторым человеком, проводящим идентификацию, может быть:

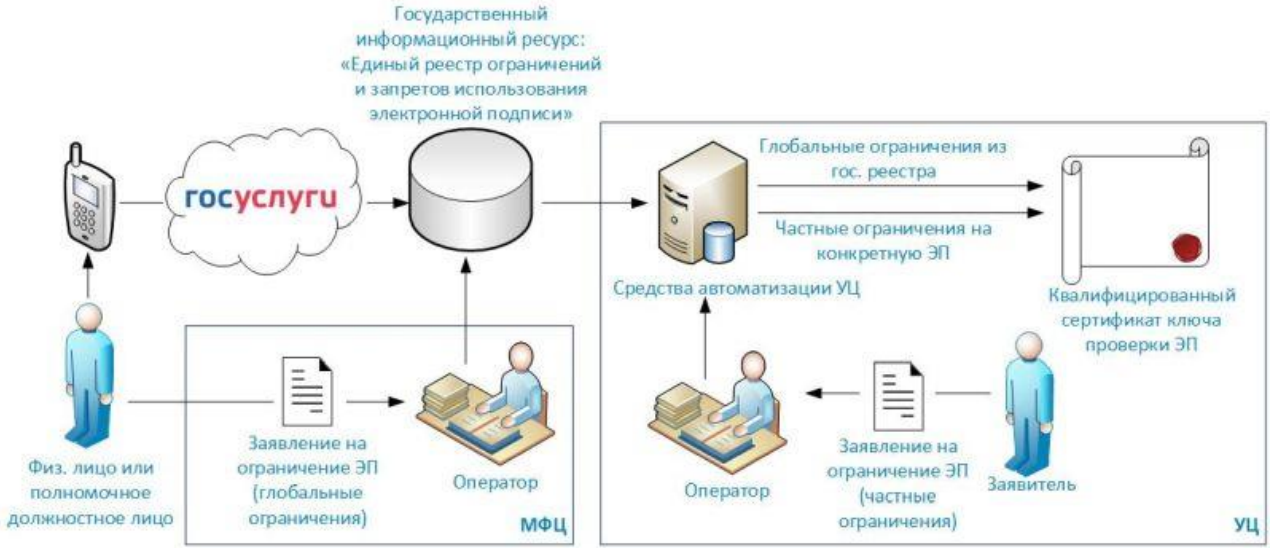
1. **Еще один работник удостоверяющего центра**. Самый дешевый вариант, обладающий минимальной безопасностью.

2. **Нотариус**. Более дорогой вариант, обладающий максимальной безопасностью без привлечения госслужащих.
3. **Сотрудник МВД России**. Самый затратный, самый безопасный вариант (если не они то кто?).

Реализация любой из предлагаемых мер неизбежно приведет к увеличению стоимости электронной подписи. Это, к сожалению, — неизбежное зло.

Усиливая процедуру идентификации заявителей на выпуск электронной подписи, нужно аналогичным образом усиливать и процедуры выдачи SIM-карт, и процедуры авторизации учетных записей на портале «Госуслуги».

Решение проблемы № 2 («ограничение использования электронной подписи»)



Технология PKI не содержит способов ограничения выпуска и использования электронной подписи. Подразумевалось, что если она не нужна человеку, то он просто ее не оформляет. Если же электронную подпись похитили, то ее обладатель незамедлительно обращается в удостоверяющий центр и просит, чтоб ее заблокировали. Блокировка подписи производится путем добавления сертификата ключа проверки подписи в список отозванных сертификатов (certificate revocation list, далее — CRL) с указанием даты и причины блокировки.

В момент проверки электронной подписи под документом анализируется дата ее формирования. Если эта дата позже или равна дате блокировки, то подпись под таким документом признается недействительной.

Таким образом, CRL является центральным элементом технологии PKI, отвечающим за доверие к выпущенным электронным подписям. Возможности влиять на «невыпущенные» электронные подписи через CRL нет.

Поэтому для исправления рассматриваемой в законе проблемы технологию PKI необходимо доработать. Причем данные доработки должны проводиться с учетом

обратной совместимости с уже существующими и работающими системами электронного документооборота.

Если в классическом PKI дерево доверия разрасталось от корневого удостоверяющего центра, то в случае государственного PKI центральным источником доверия является государство. Оно обеспечивает инфраструктуру доверия, в рамках которой существуют аккредитованные удостоверяющие центры.

Государство в лице своего уполномоченного органа должно принимать от граждан заявления (например, через МФЦ или «Госуслуги»), содержащие ограничения на выпуск и ограничения на использование электронной подписи. Полученные данные должны консолидироваться в государственный информационный ресурс — «Единый реестр ограничений и запретов использования электронной подписи».

На уровне закона удостоверяющим центрам необходимо вменить в обязанность в момент выпуска электронной подписи проверять данный ресурс на предмет установленных ограничений.

Если в реестре установлен запрет на выпуск электронной подписи, то удостоверяющий центр обязан отказывать заявителям в выпуске. Если в реестре содержатся ограничения на использование электронной подписи, то они должны быть внесены в выпускаемый сертификат ключа проверки электронной подписи.

Про ограничения на использование электронной подписи нужно поговорить подробнее. Дело в том, что, не смотря на упоминания о них в п. 4 ст. 11 63-ФЗ, по факту этот механизм не рабочий, поскольку в действующей законодательной базе отсутствуют документы, раскрывающие принцип его действия.

Исправим этот недостаток и рассмотрим один из возможных вариантов реализации ограничений на использование электронной подписи.

Первым этапом нам необходимо выработать модель, которая будет описывать ограничения на использование электронной подписи. Наиболее подходящей для этих целей будет дискреционная модель доступа, описываемая с помощью списков контроля доступа (access control list, ACL).

Список контроля доступа для электронной подписи должен содержать перечень областей, в которых электронную подпись разрешено использовать для заверения документов или в которых подпись запрещено использовать. Проблема в том, что считать этими «областями».

В идеале это должны быть информационные системы, в рамках которых ведется электронный документооборот. Но данный идеал недостижим, так как потребует создания и поддержания глобального реестра информационных систем в рамках государства. Если государственные или муниципальные информационные системы еще можно как-то учитывать, то информационные системы коммерческих организаций не поддаются учету в принципе — многие компании сами не знают, какие системы у них работают.

В качестве альтернативы можно разграничивать использование электронной подписи на уровне субъектов юридических взаимоотношений, то есть в самой электронной подписи указывать, для каких компаний (а также физ. лиц или гос. органов) ее можно использовать,

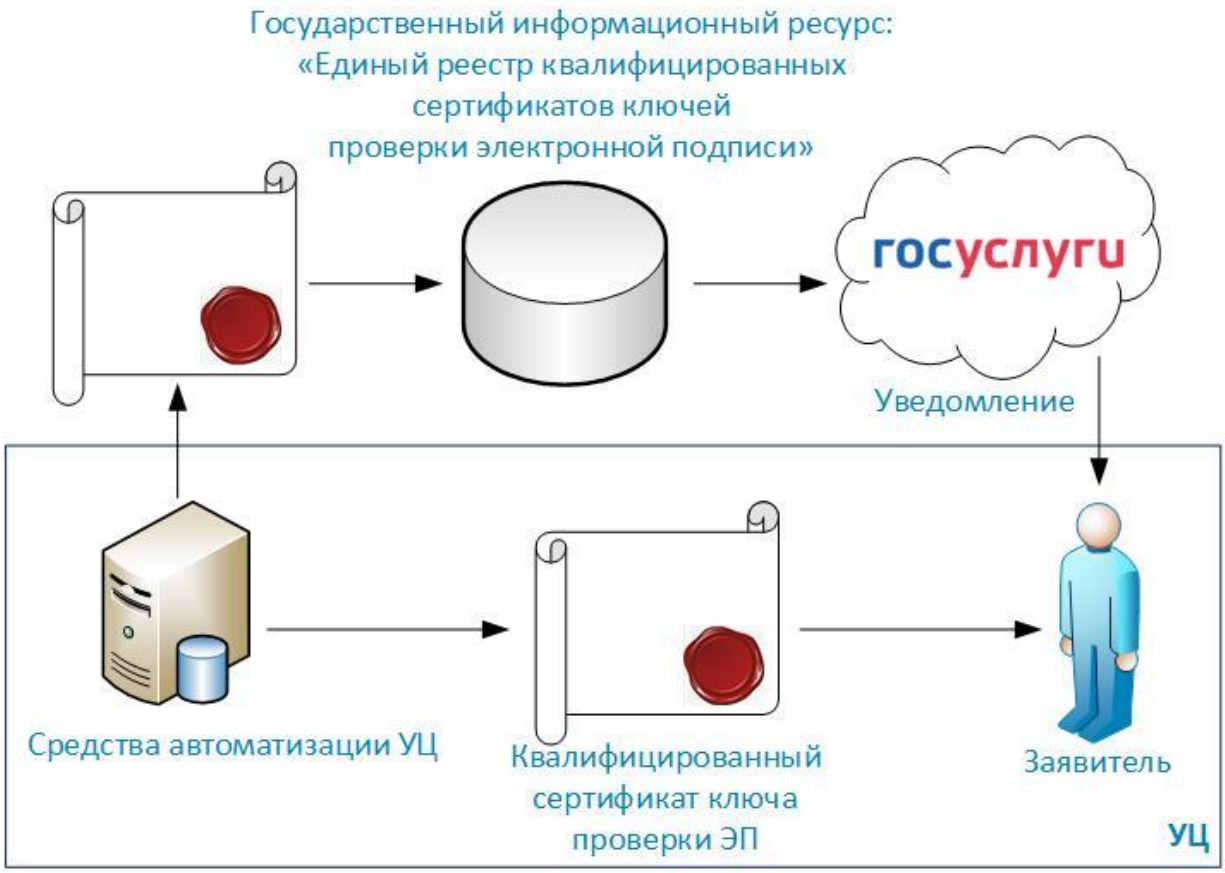
а для каких нет. Юридические лица могут идентифицироваться с помощью данных из ЕГРЮЛ, например, по совокупности значений ИНН и ОГРН. Идентифицировать физическое лицо можно по совокупности значений ИНН и СНИЛС.

Приведенный механизм разграничения доступа (ограничения из гос. реестра) — глобальный по всему пространству доверия, формируемому государством. Приведенные ограничения должны в обязательном порядке учитываться всеми удостоверяющими центрами при выпуске любых электронных подписей.

Заявителем при обращении в удостоверяющий центр могут быть установлены дополнительны (частные) ограничения, сужающие сферу использования электронной подписи. Это позволит обеспечить выпуск электронных подписей с разными областями действия, что будет актуально для защиты подписей должностных лиц.

Установка глобальных ограничений на использование электронных подписей должна порождать отзыв всех действующих электронных подписей, сфера действия который выходит за рамки дозволенного.

Решение проблемы № 3 («получение извещения о выпуске электронной подписи»)



Информирование граждан о выпуске на них электронных подписей, пожалуй, самая простая из всех приведенных в данной статье задач. Решить ее можно следующим образом:

1. Удостоверяющие центры, выпуская электронную подпись, направляют копию сертификата в адрес уполномоченного государственного органа.
2. Уполномоченный орган консолидирует все полученные сертификаты в государственный информационный ресурс — «Единый реестр квалифицированных сертификатов ключей проверки электронной подписи».
3. Субъекты права: юридические или физические лица — смогут узнать о выпуске на них электронных подписей из портала «Госуслуги». Для повышения оперативности на портале можно сделать доработки, позволяющие подписаться на уведомления по этим событиям.

Конечно, не у всех подключены «Госуслуги», но в тоже время никто не мешает их подключить, тем более будет хороший повод.

Решение проблемы № 4 («правила использования СКЗИ»)

© Яндекс.Картинки

Современные СКЗИ могут обеспечивать должную защиту только при соблюдении ряда жестких ограничений, прописанных в технической документации. Например, для всех СКЗИ, работающих на компьютере под управлением Windows, устанавливается требование отчистки файла подкачки при завершении работы. Несоблюдение данного требования приводит к риску кражи ключей электронной подписи в периоды времени, когда компьютер выключен.

Реализовывать данные требования или нет — целиком в зоне ответственности подписанта. Осуществить должный государственный контроль (так как государство является провайдером доверия) за соблюдением им этих требований в общем случае невозможно. Но в то же время, если подпись уже поставлена, то способ ее формирования ни коим образом не должен оказывать влияние на ее признание и статус.

Следовательно, законодательная база должна быть модернизирована таким образом, чтобы максимально снизить риск отказа от подписи или изменения ее статуса обусловленный действием (или бездействием) подписанта. Подобные изменения назрели уже давно, так как основополагающие документы, регламентирующие применение СКЗИ (ПКЗ-2005, ФАПСИ 152), уже морально устарели.

Решение проблемы № 5 («стандартизация средств электронной подписи»)

© Яндекс.Картинки

Стандартизация средств электронной подписи должна привести к тому, чтобы потребителям не было разницы, какое стандартизированное СКЗИ использовать.

Стандартизации должны быть подвергнуты:

1. Архитектура и структура СКЗИ.
2. Прикладные программные интерфейсы (API), используемые для вызова функций СКЗИ и взаимодействия со средой функционирования криптосредства (СФК).
3. Форматы ключевой информации, справочников открытых ключей, списков доверенных и отозванных сертификатов, входных и выходных сообщений.
4. Ключевые носители.

5. Сопутствующие алгоритмы и протоколы.
6. Параметры криптоалгоритмов и протоколов.

На данный момент СКЗИ сертифицируются по 6 классам: КС1, КС2, КС2, КВ1, КВ2, КА1. Каждый класс определяет только угрозы, которым должно противостоять СКЗИ, но не устанавливает никаких требований совместимости. В результате два криптосредства, скажем, класса КС1 абсолютно не совместимы друг с другом.

Соответственно, в рамках стандартизации должны быть разработаны профили СКЗИ соответствующих классов, но уже с ограничениями по совместимости и с привязкой к конкретной среде функционирования. Например, «Стандартизированный криптопровайдер КС1, для работы в операционной системе Windows 10».

Решение проблем № 6 («старые подписи») и № 7 («атака назад в будущее»)

© Яндекс.Картинки

Проблемы «старых» подписей, взломанных криптоалгоритмов и махинаций с датами подписания документов не могут быть решены только с помощью электронной подписи.

Для устранения этих недостатков необходимо абстрагироваться от банального использования электронной подписи и посмотреть на проблему с точки зрения юридически значимого электронного документооборота в целом.

Здесь к защите, обеспечиваемой электронной подписью, может быть добавлена защита, обеспечиваемая сервисами доверенной третьей стороны. Только с помощью данных сервисов можно устранять обозначенные проблемы.

Примерами сервисов доверенной третьей стороны будут:

- служба штампов времени, позволяющая достоверно установить дату формирования электронной подписи;
- служба гарантированной доставки сообщений, позволяющая достоверно установить факт передачи документов между участниками электронного документооборота;
- служба электронного нотариата, реализующая функции нотариуса, но применительно к электронным документам;
- служба архивации и длительного хранения электронных документов, позволяющая обеспечить юридическую значимость документа даже в условиях потери стойкости криптографических алгоритмов, используемых для формирования электронных подписей;
- и др.

Очевидно, что использование данных сервисов будет не бесплатным. Их повсеместное внедрение как обязательных требований может негативным образом сказаться на популяризации и массовости использования юридически значимого электронного документооборота в экономике страны. Тут требуется дифференцированный подход, при котором в зависимости от значимости подписываемых документов устанавливается обязательность использования данных сервисов. В качестве примеров особо значимых документов можно привести документы по сделкам с недвижимостью, судебные решения, законодательные акты и др.

Послесловие

Итак, мы с вами познакомились с некоторыми проблемами в текущем законе «Об электронной подписи». Проблем множество, но даже в этой статье нам не удалось рассмотреть их все. Мы поговорили лишь об одном, правда, наиболее значимом виде электронных подписей — квалифицированной усиленной электронной подписи.

Важно задать вопрос, приносит ли электронная подпись больше пользы, нежели вреда?

Субъективно многие граждане испытывают к электронной подписи недоверие, считая что все, что творится в цифровом мире, можно легко подделать. Отчасти они правы, но какова альтернатива? Собственноручная подпись и бумажные документы?

Если на данный момент стало известно всего о двух случаях кражи квартир с использованием электронной подписи, то количество аналогичных краж, совершенных с помощью традиционных бумажных документов, превысит это числов в тысячи раз.

Наше представление о стойкости собственноручной подписи иллюзорно и граничит с самообманом. Мало того, что ее может подделать любой человек с мало-мальски развитой мелкой моторикой рук, так она уже может быть воспроизведена с помощью машины.

Абсолютно стойкой защиты, к сожалению, не бывает. Это справедливо как для электронной, так и для собственноручной подписи.

Чем более массово электронная подпись будет использоваться, тем чаще ее будут пытаться подделывать (неправомерно использовать). Это неизбежно. Но все же процент правомерного использования электронной подписи значительно опережает процент неправомерного, а положительный эффект от закона превышает негативный.

Важно оперативно латать «дыры» в законодательстве, постоянно повышая планку затрат злоумышленников на совершение преступления. При этом сами латки должны быть легкореализуемыми и эффективными.

Дополнительные материалы

- Справочник российского законодательства по информационной безопасности — *основные законы и подзаконные акты, регулирующие ИБ в России, в том числе и электронную подпись.*
- Модель угроз СКЗИ — содержит описание угроз в отношении СКЗИ и неотказуемости электронной подписи.
- Блог Натальи Храмцовой «Кто не идет вперед, тот идет назад» — *много материалов по вопросам электронной подписи и электронного документооборота.*