



ПЯТЬ ВОПРОСОВ

ПЕРЕД ТЕМ, КАК СФОРМУЛИРОВАТЬ СТРАТЕГИЮ
ОТРАСЛИ ЭП



Дмитрий ДУБЫНИН

директор Департамента развития технологий цифровой идентификации Минцифры России, модератор ключевой дискуссии «21 год законодательству об ЭП»

В 2023 году исполнился 21 год законодательству об электронной подписи (ЭП). За это время многое сделано и участниками рынка, и регуляторами. Отрасль понимает, что эта тема в России будет

развиваться и дальше. Но есть и насущные вопросы, которые необходимо обсуждать и решать. Например, возникла потребность в пересмотре стратегии отрасли: инструментов, сервисов, среды доверия, обеспечения

безопасного и удобного применения электронных документов. О том, из чего бы могла состоять новая стратегия, говорили участники прошедшей в Санкт-Петербурге XXI международной конференции по проблематике инфраструктуры открытых ключей и электронной подписи «PKI-Форум Россия 2023».

При подготовке Ключевой дискуссии «21 год законодательству об ЭП: текущие достижения, направления и стратегия развития», мы понимали, что каждая отрасль имеет свои направления развития, но при этом стратегии как правило универсальны и включают три аспекта:



- ♦ создание безопасной современной инфраструктуры;
- ♦ создание безопасных и доверенных сервисов, которые необходимо внедрять в правоотношения с гражданами;
- ♦ кадровые вопросы.

Но, прежде чем говорить непосредственно о стратегии, участники ключевой дискуссии обсудили вызовы и проблемы, с которыми отрасль сталкивается постоянно. Были сформулированы пять вопросов.

ВОПРОС ПЕРВЫЙ:

Отрасль не понимает тактики и стратегии регулятора. Что с этим делать?

Вячеслав Бражко, начальник Управления режима секретности и безопасности информации, Федеральное казначейство:

— Мы не решили вопросы, прописанные в 63-ФЗ «Об электронной подписи». Наверное, это больше вопрос

к Минцифре, но мы не видим результатов действия этого закона. С точки зрения Федерального казначейства, стратегия есть: увеличено количество действующих сервисов, происходит улучшение их качества и стабилизация работы отдельных сервисов. В настоящее время наблюдается тенденция увеличения как числа цифровых сервисов у государственных органов, так и объёма запрашиваемых сертификатов. Стратегически нужно довести качество сервисов до приемлемого уровня.

Важным направлением будет дальнейший рост числа сервисов, и конечно, возвращение доверия населения. В этом и будет заключаться стратегия Федерального казначейства.

Александр Баранов, действительный член Академии криптографии РФ:

— Главная проблема — это действенность существующих правил. Нужно действовать в соответствии с законами, как они написаны, а не как их можно трактовать.

Вторая проблема — массовая информационная безопасность. Что такое электронная подпись? Тот же паспорт, который используется при подписании электронных документов. При этом ЭП лежит в открытом доступе на компьютере или телефоне и ничем не защищена. Уже были инциденты с незаконным использованием ЭП, их заблокировали, но могут возникнуть новые.

Стратегическая задача должна заключаться в сбалансированности применения ЭП в новых условиях с учетом требований информационной безопасности. Нужно оценить все риски. Это должны сделать и регулятор, и общественность.

Константин Дробаденко, представитель 8 Центра ФСБ России:

— Отсутствие понимания тактики и стратегии регуляторов характерно для всех отраслей во все времена. Положения, которые содержатся в законодательных актах, могут быть выполнены только при существовании механизмов, которые принесут прибыль участникам рынка. При этом последние, выполняя требования, будут развивать рынок дальше.

Мы движемся вперед, пытаемся расширить границы использования ЭП. Для этого нужно выводить на рынок новые сервисы, соблюдая баланс между ними и обеспечением ИБ. Этот баланс всегда находится вручную, конкретно для определенного сервиса.

Есть положения, которые до сих пор не заработали. В частности, институт доверенных лиц третьей стороны. Причина — отсутствие механизмов, стимулирующих развитие этого института.

Реализация законодательства — улица с двусторонним движением. Это и попытки регулятора оформить правилами определенные положения. И широкое информирование общественности, чтобы создать рыночные механизмы саморегулирования, которые позволят реализовывать эти положения. Конечно, есть определенные трудности при создании этих механизмов, но я бы не драматизировал ситуацию в области ЭП — положения приняты, должны появиться процессы, стимулирующие развитие ЭП. Если у регулятора что-то не получается, значит, положения будут меняться.

Фёдор Новиков, начальник управления ЭДО, ФНС России:

— Электронная подпись активно внедряется в различные сферы, в процесс вовлекаются новые люди. Мы даем возможность использовать инструмент в разных отраслях жизни. Обратная задача состоит в том, чтобы отрасль помогла нам ресурсами, знаниями, сервисами. Те решения, которые уже были приняты, необходимо интегрировать в повседневную жизнь граждан с должным уровнем безопасности.

Есть важные, но тяжелые решения, которые не могут быть реализованы простой или квалифицированной ЭП. Именно эти моменты нужно жестко регулировать, использовать более доверенные сервисы и продукты — решения, которые предстоит найти. Эту задачу нужно решать всем вместе, что мы уже и делаем.

Игорь Качалин, генеральный директор АНО «Национальный технологический центр цифровой криптографии»:

— Не всегда отрасль — объединение людей и организаций с разными



Константин Дробаденко (ФСБ России)

технологическими и бизнес-интересами — представляет себе развитие сервисов. Часто они вводятся в эксплуатацию без надлежащей проработки вопросов безопасности.

Этот момент требует законодательного и технического решений, усилий разных людей и организаций. Хотелось бы, чтобы появился некий перспективный план развития сервисов, на основе которого можно было бы заранее отрабатывать вопросы нормативного регулирования и стандартизации в области безопасности, которые легли бы в основу востребованных сервисов.

Дмитрий Гусев, заместитель генерального директора «ИнфоТеКС»:

— Как представитель разработчиков хочу отметить несколько проблем. Первая — отрасль с механизмами и решениями, которые обсуждаются, развиваются и реализуются. В этом движении она обогнала отрасль электронного документооборота, к которой теперь должны быть приложены все усилия.

Известны примеры, когда в простой структурированный документ должны быть внесены атрибуты ЭП, чтобы человек мог оперировать подписью. Эта простая потребность вызвала глобальное замешательство в сообществе. До сих пор не существует

окончательно принятого решения, хотя технически оно готово.

Отсутствие стандартизации структур и данных в большинстве отраслей является стопором развития экономики данных. В ней хорошо разбираются только глубоко погруженные специалисты. Эти сложные вопросы мы не сможем решить здесь и сейчас. Отсюда проистекает вторая проблема — проблема регулирования, определения правил, в рамках которых система может жить и развиваться. Любое предписание будет тормозить развитие системы. И эти две проблемы неотделимы друг от друга.

Необходимо понимание механики того, как исходные бумажные документы должны трансформироваться в электронные машиночитаемые документы, как должно выстраиваться регулирование. По этому вопросу предстоит дискуссия с представителями отраслевых институтов.

На практике мы сталкиваемся с тем, что подписанный регулятором документ порождает вопросы в области безопасности. Чем больше требований по ИБ, тем хуже они структурированы и тем менее детальная модель угроз выстраивается. Прикладная часть задачи перекладывается на плечи специалистов по ИБ, которые превращаются в технологов и расписывают бизнес-процессы предприятия.

ВОПРОС ВТОРОЙ:

Нормативное регулирование отстает от темпов развития технологий и потребностей рынка. Как изменить ситуацию?

Константин Дробаденко. Я бы вернулся в 2011 год, когда был принят 63-ФЗ «Об электронной подписи». Тогда в России было предложено ультралиберальное регулирование использования ЭП. Любой хозяйствующий субъект мог выполнить требования ч. 3 ст. 16 закона и стать аккредитованным центром, создавать и выдавать квалифицированные сертификаты.

Это было рискованное регулирование, но оно принесло больше пользы, чем вреда. Рынок активно развивался. Когда стало понятно, что отрицательные черты преобладают, понадобилось время, чтобы в 2019 году изменить парадигму.

Сейчас мы пытаемся выстроить сбалансированное регулирование. Но многие положения 2019 г. до сих пор не реализованы, например, сроки перехода на машиночитаемые доверенности (МЧД). Рынок воспринял эту идею и движется в нужном направлении. То есть тут нормативное регулирование даже обгоняет технологии: мы выдвинули положения и теперь пытаемся обеспечить их технологическое выполнение.

В целом же нормативное регулирование незначительно отстает от развития технологий и потребностей рынка, а иногда пытается направить развитие технологий для обеспечения интересов личности, общества и государства, что позволит в дальнейшем обеспечивать стабильное развитие ЭДО в стране.

Игорь Качалин. Если говорить про технические аспекты регулирования, то создание новых криптографических механизмов, обоснование их качества, стойкости и соответствия требованиям — сложный трудоемкий и наукоемкий процесс, требующий времени. Опыт ТК-26 показывает, что хорошо выверенный стандарт в области криптографии — это нескольких лет работы.

Даже имея базовые криптографические протоколы и механизмы,

построить на их основе новый протокол — трудоемкая задача, требующая обоснования правильности построения и выбора примитива. Поэтому тут всегда будет отставание от технологий и потребностей рынка.

Что можно сделать? Вовлечь в работу молодых специалистов.

Александр Баранов. Мы наблюдаем технический застой. Задача должна иметь комплексное решение, где главная проблема — увязать одно с другим. Это должно быть принципиально новое решение.

Дмитрий Гусев. Я развернул бы вопрос в другую сторону. Нормативные документы всегда отстают от темпов развития технологий. Если мы в федеральных законах и подзаконных актах уйдём от технических деталей и вынесем их в отдельный стандарт — это выход из ситуации. Но того, что делает ТК 26, мало, чтобы говорить о развитии полноценного ЭДО.

У нас есть технологический задел, но мешает отсутствие стандартов, выпущенных профессиональным сообществом. Стандарты рождаются в спорах между техническими экспертами и компаниями, которые понимают, как устроена начинка. Никакой законодатель или регулятор не сможет погрузиться так глубоко.

Мы знаем, как сделать ЭП, и уже сделали ее, она работает во множестве бизнес-кейсов и госсистем. Но мы ждем требований регулятора. Надо смотреть на эту проблему в другой плоскости и тогда появится решение.

ВОПРОС ТРЕТИЙ:

Длительные сроки оценки сертифицируемых решений. Как на это можно повлиять в текущих условиях? Какого результата ожидать при положительном исходе?

Дмитрий Гусев. Сроки оценки криптографических продуктов выливаются в месяцы, а то и больше года. Когда мы говорим о внедрении криптографических механизмов в прикладные ГИС, жизненные циклы разработки и согласования



Игорь Качалин (НТЦ ЦК)

совпадают. Но бизнес живет в другой парадигме: кто первый вывел решение на рынок, тот и получил прибыль. Бизнес не готов ждать согласования месяцами.

Проблема сроков согласования постоянно обсуждается на профильных конференциях и находит отклик у регулятора. Коллеги готовы рассматривать предложения без снижения или с контролируемым снижением уровня безопасности, чтобы бизнес мог принимать для себя решение, и он готов идти на риск. Каким образом? Оптимизируется существующий линейный порядок проведения оценки. Можно идти параллельным путем и интегрировать один процесс в другой — за процессом разработки СКЗИ и прикладной системы проводить оценку влияния или первичные исследования.

Здесь можно сослаться на опыт ФСТЭК и создания доверенного ядра Линукс на базе ИСП РАН. Эта работа уже ведется, в ней участвуют и компании, и исследователи. Совместными усилиями они создают доверенное ядро доверенного кода и свою базу,

которая может использоваться разработчиками прикладных систем, — чтобы они «с нуля» не проходили все процедуры проверки безопасности своих систем. Аналогично идет работа по программным компонентам, подключаются и разработчики аппаратных платформ, чтобы привнести доверенный драйвер для «железа» в общий список доверенного кода.

Это единственный вариант решения проблемы. Так можно достичь глубокого уровня контроля процессов разработки, решения проблем цепочек поставки и избежать внедрения закладок в OpenSource решения. Так сократится и срок согласования.

Фёдор Новиков. Специфика работы ФНС как госструктуры связана не только со скоростью получения сертифицированных решений, но и с привязкой к бюджетным циклам. Это параллельные проблемы.

Я разделяю мнение коллег, что бизнес страдает от недополучения прибыли. Для ФНС это становится проблемой недополучения налогов в казну. Мы заинтересованы, чтобы



Вячеслав Бражко (Федеральное казначейство)



Дмитрий Гусев (ИнфоТекС)

бизнес активнее внедрял новые решения, оптимизировал затраты и вкладывал средства в развитие.

Константин Дробаденко. Я бы хотел подчеркнуть сложность перехода. Оценка соответствия решений, по итогам которых выдаются сертификаты, — это опыт и требования, написанные поколениями криптографов и инженеров. Это статическая модель безопасности: мы выдвигаем требования и проверяем соответствие им.

Необходима смена парадигмы. Она должна быть проведена в строго определенных областях. Смена парадигмы связана с риск-ориентированным подходом. Можно обратиться к опыту западных стран, которые в области массовой криптографии ориентируются на такие подходы и на динамическую модель противодействия актуальным угрозам.

Это серьезная смена воззрений: должна быть наработана и методика, и опыт, который можно воплотить в методических документах. Это единственный путь, по которому мы можем идти от сертификации решений к сертификации процессов. Быстрого решения вопроса ожидать не стоит.

Александр Баранов. В чем разница требований ФСТЭК и ФСБ? Требования 8 Центра ФСБ техниче-

ские и количественные (вероятностные). А требования ФСТЭК в основном качественные. И попытка заменить качественные на количественные требования приводит к тяжелейшим решениям в оценке. Сертификация будет еще более сложной.

Это пытались сделать почти 20 лет назад, когда мы только начинали разворачивать ИБ. Проблема — ввести количественные характеристики всех требований. Спустя годы, сдвигов на этом направлении не наблюдается. Массовую ИБ надо делать удобной, легкой и масштабируемой, чего нельзя сказать о предлагаемом динамическом подходе.

Вячеслав Бражко. Подводя итоги, отмечу, что в госсекторе все протекает в плановом режиме, но в отдельных случаях хотелось бы сокращения сроков. Иногда госсектор формулирует эксклюзивные решения, требующих быстрых сертификационных мероприятий, часто это напрямую зависит от сформулированных угроз и моделей угроз. И тут важно говорить о сокращении сроков.

Почему я выступаю за идею сертификации производства? Это повысит массовость. Но в определенный момент мы столкнемся с антимонопольным законодательством. Тут нужна осторожность.

Необходимо формирование среды доверия больших платформ, которые позволят по ряду решений отказаться от сертификации определенных элементов. Хороший пример — сертифицированная в определенный момент версия ОС Windows.

ВОПРОС ЧЕТВЕРТЫЙ:

Корреляция между активным регулированием и технологическими возможностями. Пока воплощается замысел, нормы могут измениться. Как найти баланс?

Фёдор Новиков. Да, не всегда проблемы, которые прорабатывались на рабочей группе, на выходе соответствуют замыслу и проделанной работе.

Надо понимать, что государственные институты состоят из разных лиц, которые не всегда общаются с бизнесом. У нас есть практика сопровождения нормативно-правовых актов (НПА) на каждом этапе согласования, это минимизирует процент неожиданностей на выходе. Если со стороны органов власти есть заинтересованность, например, исполнение поручений, то в процессе принятия могут возникнуть сложности, поскольку участники процесса не оценивают все нюансы.

Чтобы в НПА вошли нужные нормы, при выработке решений бизнесу целесообразно создавать экосистему и сообща работать в ней с органами власти. Еще один аспект — участие доверенных лиц при обсуждении НПА, позиционирование бизнеса в госорганах, на мероприятиях, где обсуждаются нормативные акты. Часто в них участвуют одни лица, а претензии после высказывают другие. Необходимо внимательно подходить к тому, кто доносит позицию бизнеса до регулятора.

И делая отсылку ко второму вопросу, скажу, что лучшее регулирование идет после того, как решение сделано. Необходимо идти через механизм экспериментов и пилотных проектов, чтобы максимально комфортно реализовать все при наличии технологической возможности.

Вячеслав Бражко. Нормативные инициативы не могут появляться без технологической возможности. При реализации серьезной задачи сначала стоит вопрос технологической возможности, затем — нормативного регулирования. Иногда это приводит к необоснованному выбору технологических платформ. Но это лучше, чем неисполнение требований.

Как обеспечить корреляцию? Главное, при обсуждении НПА «не выплеснуть ребенка». При появлении технологической возможности необходимо сопровождение НПА, после этого отрасль получает законченное решение.

Регулятор абсолютно открыт, как уже говорили коллеги, есть масса площадок, на которых можно обсуждать. Пример удачного сотрудничества — обсуждение и внесение изменений в Федеральный закон «Об электронной подписи».

Дмитрий Гусев. Необходимо возвращение Госстандартов в рамки НПА и принятие закона «О техническом регулировании». Технологии должны идти впереди регулирования, они должны определять облик будущего законодательства, а не наоборот. Техническое регулирование — вопрос отрасли, а не законодателей.

Это важный момент, на который надо обращать внимание не только в приказах ФСТЭК, но и других регуляторов. Стандарты должны появляться в федеральных законах и подзаконных актах.

ВОПРОС ПЯТЫЙ:

Это вопрос встраивания в глобальное пространство доверия (на уровне стандартов, нормативов, технологий и на организационном уровне). Что мы можем сделать для ускорения этого процесса и повышения его эффективности?

Фёдор Новиков. В чем проблема работы с услугами доверия? По результатам получения услуг необходимо подтвердить деятельность при работе с контрагентами при обращении в суд или в рамках деятельности контрольных органов. В рамках межведомственного и трансграничного взаимодействия мы готовы к тому, что бизнес будет интегрироваться и работать с другими институтами. Мы готовы объяснять всем как работать, почему надо доверять сервисам и услугам. Государство сделало много, теперь бизнесу необходимо применять это на практике.

Константин Дробаденко. Вопрос встраивания в пространство доверия больше политический. А политические течения имеют больше значения, чем вопросы технические. Сегодня по многим направлениям работа ведется в рамках международных контактов, при этом технические вопросы остаются на втором плане. Необходимо выстраивать взаимоприемлемые отношения, разграничивать пространство доверия в рамках действующих договоров. Должна проводиться работа на технологическом уровне. Пример работы ФНС России в этом направлении показывает новые возможности и перспективы развития. Иных универсальных механизмов ускорения процесса нет.

Игорь Качалин. ТК 26 уже более 10 лет занимается международной

стандартизацией и ведет работу по внедрению в международные стандарты российской криптографии. Однако после февраля 2022 г. эта работа была прекращена.

За криптографические стандарты спокоен, но гармонизация стандартов приобрела однобокий характер. Появилась тенденция механического перевода иностранных стандартов, особенно в таких популярных областях как Искусственный интеллект или Интернет вещей, которые внутри содержат отсылки к иностранным стандартам и криптографии, требованиям безопасности без адаптации к российским требованиям. Таких стандартов принимается до сорока в год, очень странно делать их обязательными к применению.

Вячеслав Бражко. Для создания новых путей встраивания в глобальное пространство доверия есть два направления: либо принять чьи-то стандарты, либо заниматься экспансией свободных рынков. Для этого нужно заниматься разработкой и внедрением своих стандартов на свободные рынки, например, на уровне программных продуктов, как это ранее делали иностранные компании. Это можно сделать даже на уровне операционных систем со встроенными российскими криптографическими механизмами.

* * *

Подводя итоги дискуссии, участники отметили, что стратегия развития отрасли всегда есть, даже если она не оформлена на бумаге. Все акторы руководствуются стратегическими соображениями и требованиями регуляторов. При формализации документа необходима стратегия развития сервисов, к которым должны пристраиваться вопросы обеспечения безопасности. При этом стратегия должна быть живой и обсуждаться широким кругом участников. Главное — не возводить ее в ранг догмы, чтобы она не довлела над развитием отрасли.