Субъекты КИИ:
торопитесь не торопясь!

Алексей КОМАРОВ,
автор блога ZLONOV.ru

Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» (КИИ) и его подзаконные акты предполагают со стороны субъектов КИИ (владельцев объектов КИИ) ряд определенных шагов, включающих проведение категорирования объектов КИИ, организацию взаимодействия с НКЦКИ, создание системы безопасности значимых объектов КИИ (ЗО КИИ) и т. д. Обобщенный план действий представлен на рис. 1.

Судя по всему, этап категорирования благополучно завершен существенным числом субъектов КИИ. Правда, строго говоря, формально данная процедура должна заканчиваться подачей во ФСТЭК России сведений о результатах категорирования (а еще точнее – получением субъектом КИИ соответствующего уведомления от ФСТЭК России), но на практике на это отводится целый год с момента первоначального направления перечня объектов, подлежащих категорированию, так что далеко не все субъекты КИИ, реально завершившие категорирование, спешат с официальным оформлением этой процедуры. Равно как и не спешат даже с утверждением и подачей перечней – крайний срок (01 сентября 2019 г.) был установлен Постановлением Правительства РФ № 452 от 13.04.2019 только для госорганов и госучреждений, но даже для них ответственность за нарушение этого срока пока не установлена.

Одна из причин, по которой многие не торопятся, состоит в том, что отсчет срока до первой плановой проверки (госконтроля) идет от даты внесения информации о значимом объекте в соответствующий реестр, который ведет ФСТЭК России. Этот срок составляет три года. Так что чем позже субъект КИИ утвердит перечень, тем позже ему надо завершить процедуру категорирования и тем позже в отношении него возможно проведение плановой проверки.

Справедливости ради стоит отметить, что имеющийся запас в четыре года, несмотря на кажущуюся большую продолжительность, для многих, особенно крупных организаций не является таким уж комфортным – длительности бюджетирования и закупочных процедур вносят неизбежные задержки. Да и саму систему безопасности за пару месяцев вряд ли получится построить.

Факторы влияния

Помимо уже обозначенных отсутствия для негосударственных субъектов КИИ конкретных сроков и пока не установленной предметной ответственности даже за полное игнорирование требований № 187-ФЗ среди факторов, отрицательно влияющих на скорейшее выполнение законодательных требований, нельзя не отметить противоречивость и неконкретность самого законодательства в отдельных вопросах.

Конечно, компании, оказывающие консалтинговые услуги в обсуждаемой сфере, уже давно выработали свои методики, а многие из них – даже успешно апробировали их на практике, оказав своим заказчикам помощь в успешном получении от ФСТЭК России уведомлений, подтверждающих корректность выполненной процедуры категорирования.

Однако у тех, кто пока не получил реального опыта и решил выполнить все своими силами, отдельные тонкости могут вызвать затруднения, но вряд ли приведут в тупик. Благо, что открытых источников информации в Интернете предостаточно, да и профессиональное сообщество практически всегда готово прийти на помощь, за что, конечно, многим его активистам нужно сказать отдельное большое спасибо. Так что, в принципе, если загруженность и условная стоимость часа рабочего времени собственных сотрудников позволяют сэкономить на привлечении внешних подрядчиков, выполнить категорирование самостоятельно вполне реально, тем более что по законодательству эту обязанность субъекта КИИ ни на кого другого, даже если этот другой – лицензиат ФСТЭК России, переложить не получится.

Другой вопрос: а есть ли внутренняя готовность у субъекта КИИ к тому, чтобы приступить к выполнению законодательных требований?

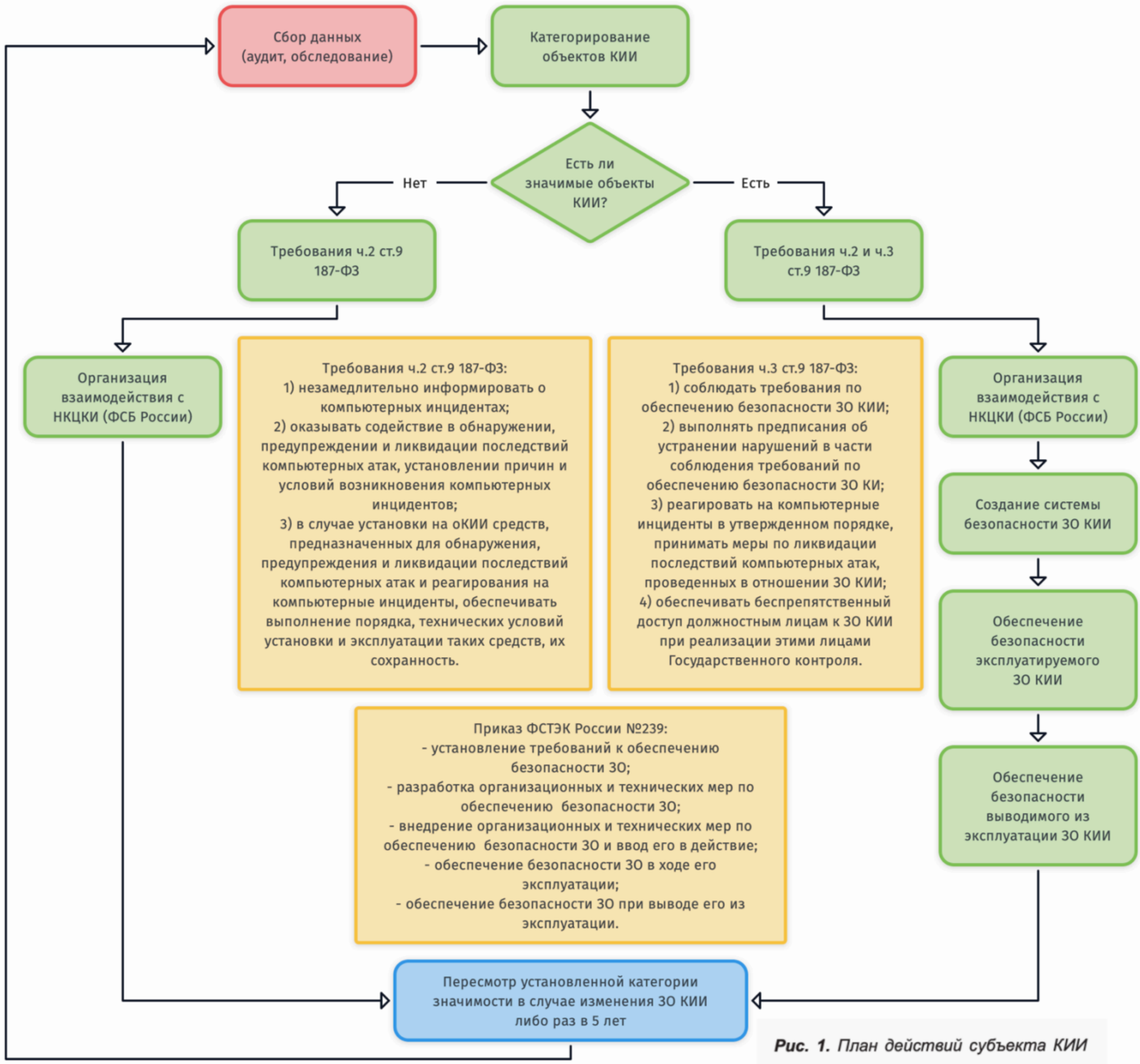

Рис. 1. *План действий субъекта КИИ*

Готовность заказчиков

На публичных мероприятиях представители регуляторов не один раз за прошедшие с момента принятия Федерального закона № 187-ФЗ годы недвусмысленно давали понять, что в случае игнорирования субъектами КИИ, особенно владельцами значимых объектов, требований законодательства более строгие сроки и штрафы для уклоняющихся не заставят себя ждать.

Судя по тому, что строгие меры все еще зафиксированы лишь в проектах документов, выбранная тактика диалога и мягкого принуждения оказалась эффективной. Ведь не нужно забывать, что новые обязанности появились не только у субъектов КИИ, но и у соответствующих федеральных органов исполнительной власти.

Полученные от субъектов КИИ результаты категорирования (в терминах законодательства – «сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий») необходимо проверить, выдать при наличии обоснованные замечания («возвращает их в письменном виде субъекту критической информационной инфраструктуры с мотивированным обоснованием причин возврата») либо соответствующим уведомлением фактически подтвердить их отсутствие, да еще и сделать это в установленные законодательством сроки. При этом, разумеется, не сказано, что если в один день поступили сведения

от, допустим, тысячи субъектов, то успеть ответить надо только первым ста.

Так что все участники процесса персонально заинтересованы в постепенном эволюционном росте числа субъектов, вступивших на путь выполнения требований законодательства о безопасности КИИ.

В связи с этим позиция тех, кто не сильно торопится, выигрышна, но лишь отчасти. Нарастив необходимые ресурсы и получив достаточный опыт, регулятор может перестать быть лояльным к тем, кто затянул решение вопроса до последнего. Вряд ли можно посоветовать какому-либо субъекту КИИ оказаться в числе крайних в своей отрасли. Тем более что выполнение законодательных требований даже в полном объеме вовсе не предполагает существенных и/или бессмысленных трат. Требования законодательства о безопасности критической информационной инфраструктуры не содержат откровенных глупостей или никому не нужных формальностей, не влияющих на реальную безопасность.

Приказы ФСТЭК России яркое тому подтверждение: реализация изложенных в них подходов мало чем отличается от тех рекомендаций, что обычно излагаются в «лучших практиках» или «дорожных картах по повышению уровня информационной безопасности», разрабатываемых профессиональными специалистами. Да, конечно, надо аккуратно и грамотно оформить соответствующую сопроводительную документацию, но сами предлагаемые подходы, повторюсь, отторжения не вызывают.

При этом даже в условиях непростой геополитической ситуации каких-то жестких ограничений, например, по использованию исключительно сертифицированных и/или отечественных решений, в приказах ФСТЭК России не содержится. Да, сейчас много говорят о планах по закручиванию гаек в этой части, но такова уж политическая повестка дня, а вопросов политики в рамках данной статьи касаться не хотелось бы.

Возвращаясь к вопросу стоимости реализации требований, нельзя не отметить активность поставщиков средств защиты – статьи, вебинары, листовки и прочие маркетинговые материалы были быстро отредактированы и адаптированы под ставшую модной тематику.

Готовность поставщиков

Сами решения поставщиков при этом, понятно, не изменились: нет каких-то специальных средств защиты информации от несанкционированного доступа (СЗИ НСД) или электронных замков исключительно для значимых объектов КИИ.

Да, есть требования по глубине (назовем это так) сертификации, но, во-первых, это все та же процедура сертификации и межсетевой экран определенного класса защиты может успешно защищать как ЗО КИИ, так и персональные данные (ПДн). Во-вторых, само по себе требование по наличию оценки на соответствие

Рис. 2. *Слайд из презентации Елены Борисовны Торбенко, ФСТЭК России*

требованиям по безопасности в форме обязательной сертификации, как уже отмечалось, не является обязательным: «В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации» (приказ ФСТЭК России № 239 от 25 декабря 2017 г.).

Однако здравый смысл и статистика из публичных выступлений представителей ФСТЭК России (рис. 2) подсказывают, что среди значимых объектов, для которых и надо реализовывать существенную часть законодательных требований, доминируют объекты КИИ, являющиеся автоматизированными системами управления.

В силу особенностей АСУ (и более узко – АСУ ТП) как объектов защиты некоторое время назад специализированных решений и даже подходов для них не существовало. Ситуация начала меняться, когда стало понятно, что без наложенных средств защиты не обойтись из-за отсутствия у применяемых в АСУ ТП программного обеспечения и аппаратных средств необходимых встроенных (штатных) функций безопасности.

Модернизация оборудования и систем управления для успешно работающего технологического процесса экономически не оправдано, а офисные (корпоративные, классические, ИТ-) решения в промышленности не просто неэффективны, но и порой даже опасны. И пусть рассказ о том, что однажды использование сканера уязвимостей для технологической сети остановило производство воспринимается как «городская легенда», когда речь заходит о дорогостоящем оборудовании и жестких требованиях по непрерывности, без тестирования совместимости средств защиты с АСУ ТП проекты по внедрению просто не реализуются.

При этом каждый поставщик выбирает свой вариант тестирования совместимости: кто-то «обвешивается» максимально общими, без конкретики (например, даже без указания версии протестированного решения) заключениями и сертификатами о совместимости, как новогодняя елка огоньками, кто-то обосновывает отсутствие влияния на технологический процесс за счет применения однонаправленной передачи данных, а кто-то выполняет тестирование внедряемого решения для конкретного объекта непосредственно на месте. Хотя на практике чаще используется, конечно, комбинированный подход.

В любом случае нельзя не отметить общее повышение зрелости специализированных решений для промышленных систем и стремление поставщиков на теперь уже сильно конкурентном рынке действительно повысить качество предлагаемых решений и оказываемых сопутствующих услуг. Кстати, принято считать, что конкуренция оказывает существенное влияние и на стоимость.

Завершая мысль про поставщиков, стоит отметить, что не всегда предлагаемое комплексное многокомпонентное решение является самым правильным выбором – часто можно обойтись теми же штатными средствами, организационными мерами или внешними техническими решениями, но не по заоблачной цене.

Резюме

В целом тема обеспечения безопасности критической информационной инфраструктуры с нами надолго. Ожидать, что будут послабления со стороны регуляторов, не приходится – скорее даже наоборот.

Любители «продавать страх» в связи с темой КИИ часто упоминают принятую вместе с Федеральным законом № 187-ФЗ новую статью Уголовного Кодекса РФ 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Данная статья на самом деле напрямую не касается вопросов категорирования и построения систем безопасности, но, поскольку правоприменительная практика по частям 1 и 4 становится все обширнее, счет публикациям о возбужденных уголовных делах и вынесенных приговорах идет уже на десятки, это означает, что сам термин «критическая информационная инфраструктура» становится в судебно-прокурорской среде все более привычным.

При этом стоит напомнить, что упомянутая статья содержит, в частности, и довольно «неприятную» часть 3: «Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации… либо правил доступа…, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации», судебную практику по которой в части трактовок можно пока только предполагать.

Так что для минимизации рисков уголовных последствий вполне разумным представляется построение системы безопасности ЗО КИИ, которая позволит снизить вероятность «причинения вреда КИИ РФ», тем более что и для устойчивости бизнеса наличие грамотно выстроенной и экономически оптимально реализованной системы безопасности – это благо.

Таких проблем, как раньше, в самом начале становления темы, у субъектов КИИ в настоящее время не наблюдается – понятно, что делать с процедурной точки зрения, и недостатка в выборе подходящих организационных и технических мер тоже нет. Стратегия откладывания вопроса «на потом» становится все менее оправданной, что, видимо, неизбежно повлечет рост числа субъектов КИИ, выполняющих требования законодательства во все большем объеме. ■