Тонкости критической инфраструктуры

Антон Свинцицкий, *директор по консалтингу АО "ДиалогНаука"*
Игорь Тарви, *ведущий архитектор систем безопасности АСУ ТП АО "ДиалогНаука"*

Прошло уже полтора года с момента принятия и год со вступления в силу Федерального закона № 187-ФЗ "О безопасности критической информационной инфраструктуры РФ". Постепенно наполняется реестр значимых объектов критической информационной инфраструктуры (КИИ), который находится в ведении ФСТЭК России. На состоявшемся в конце ноября прошлого года SOC-Forum представители ФСТЭК России привели статистику по предоставленным сведениям[1]. Лидерами в категорировании оказались компании, относящиеся к ТЭК, здравоохранению и ОПК.

Тем не менее количество субъектов и объектов, подпадающих под требования закона № 187-ФЗ, значительно больше. Возможно, их владельцы и хотели бы выполнить требования, установленные федеральным законом и подзаконными актами, но не всегда понимают, что от них требуется.

Как же пройти процедуру категорирования? Кажется, что все просто: нужно создать в соответствии с требованиями постановления Правительства РФ № 127-ПП комиссию по категорированию объектов КИИ, провести процедуру, зафиксированную в постановлении, составить акт категорирования и направить, в соответствии с установленной формой, сведения по объекту КИИ в ФСТЭК России для внесения в реестр. Однако процедура категорирования предстала не такой простой, как хотелось бы, и для некоторых отраслей провести ее самостоятельно оказалось затруднительно. Постараемся разобраться в особенностях категорирования и проанализировать первый практический опыт.

Законом № 187-ФЗ определены объекты и субъекты КИИ, но уже в самом определении не совсем понятно, кто именно функционирует в указанных сферах: ИС, ИТС, АСУ или субъекты. При этом ФСТЭК России поясняет, что принадлежность к указанным в законе сферам будет определяться по уставным или другим документам, связанным с компанией, т.е. первичны все-таки субъекты.

Категорирование и его особенности

Законом № 187-ФЗ определены объекты и субъекты КИИ, но уже в самом определении не совсем понятно, кто именно функционирует в указанных сферах: ИС, ИТС, АСУ или субъекты. При этом ФСТЭК России поясняет, что принадлежность к указанным в законе сферам будет определяться по уставным или другим документам, связанным с компанией, т.е. первичны все-таки субъекты. Это означает, что объектами КИИ могут являться некоторые ИС, ИТС и АСУ, принадлежащие юридическим лицам и индивидуальным предпринимателям, работающим в указанных сферах. Из этого предположения можно сделать вывод, что достаточно вывести ИС, ИТС и АСУ в отдельную компанию, например, с говорящим названием "ИТ Сервисы", и покупать у них облачные ИТ-услуги в соответствии с модной тенденцией "инфраструктура как сервис". Теоретически в этом случае процесс категорирования будет очень коротким: основная компания не имеет ИС, ИТС и АСУ на балансе (категорирование завершено!), а дополнительная компания не работает в критической сфере, она предоставляет облачные ИТ-услуги, которые вроде бы не относятся к критическим сферам.

Первый этап выполнения требований закона связан с присвоением объекту КИИ категории значимости, этот процесс называется категорированием. Его определяет постановление Правительства РФ № 127-ПП. Беда только в том, что ни в действующей версии постановления, ни в самом законе не указываются сроки, в которые необходимо провести категорирование и приведение систем в соответствие требованиям. В законе указана только дата его вступления в силу – 1 января 2018 г., а в постановлении дополнительно определен срок проведения категорирования – не более одного года с момента утверждения субъектом КИИ перечня объектов. Однако непонятно, как скоро нужно было заняться разработкой этого перечня, от которого отсчитывается один год. Эта неопределенность дала компаниям возможность отсрочки категорирования. И хотя в случае успешной хакерской атаки и причинения ущерба после 1 января 2018 г. руководитель объекта может получить уголовный срок, большинство рассчитывает, что пронесет или удастся списать на форс-мажор.

В п. 3 постановления о процедуре категорирования сказано следующее: "Категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ". Далее идет описание процесса категорирования.

Тут возникает вопрос о том, что считать "процессом в рамках выполнения функций (полномочий)". Например, как оценивать ущерб для телекоммуникационных компаний, которые в соответствии с законом "О связи" могут не знать, в каких процессах используются их сети, а следовательно не могут рассчитать ущерб от прекращения деятельности. В частности, при передаче клиентом по сетям оператора конфиденциальной информации, естественно, с соблюдением всех требований по защите, оператор не может

[1] *От 660 субъектов были направлены сведения о более чем 25 тыс. объектах КИИ. Более 60 объектов КИИ зарегистрированы в реестре как значимые. Материалы еще по 600 объектам КИИ были отправлены заявителям на доработку.*

знать о содержании передаваемой информации и о возможном ущербе в случае ее недоставки в срок. Возможно, именно поэтому телекоммуникационные компании не торопятся проводить категорирование, поскольку не до конца понимают, как посчитать ущерб от временного прерывания функционирования их ИТС, т.к. ущерб наносится не им, но клиентам. Схожие проблемы существуют и в транспортной отрасли: компании, осуществляющие перевозки, не всегда могут оценить экономический ущерб клиенту в случае недоставки в срок из-за хакерской атаки угля для доменной печи непрерывного цикла.

Собственно, в постановлении есть и терминологические сложности. С одной стороны, категория присваивается объекту – ИС, АСУ и ИТС, но и фактически процессу, в результате приостановки которого считается ущерб. А кто должен отвечать за категорирование: владелец объекта или процесса? Ведь владелец вычислительной системы (объекта) может не совпадать с владельцем процесса, выполнение которого обеспечивает ИС. Это, в частности, популярные нынче облачные технологии, которые приводят к подобному расслоению ответственности: облака не передаются клиенту даже на правах аренды, но обеспечивают ему функционирование процессов.

Планы изменения

Уже известно, что в постановление № 127-ПП будут вноситься изменения, об этом заявили представители ФСТЭК России на том же SOC-Forum. На публичное обсуждение был вынесен проект измененного постановления, в котором присутствует ряд серьезных изменений, которые, возможно, потребуют пересмотра результатов уже завершившихся проектов по категорированию. Рассмотрим их подробнее и обсудим возможное влияние на существующие сложности закона.

Существенным изменением, которое планируется внести в постановление № 127-ПП, является четкое определение сроков. В новой редакции планируется указать срок подготовки и регистрации перечня объектов к 1 июня 2019 г. При этом сокращается срок проведения процедуры категорирования с года до шести месяцев. Если эти поправки будут приняты, то категорирование объектов должно быть завершено к концу этого года. Срок не очень большой, но об этом предупреждали ранее, и в распоряжении субъектов был весь предыдущий год.

Кроме того, комиссии по категорированию должны стать постоянно действующими, их расформирование предусмотрено в двух случаях:

а) субъект КИИ перестал быть субъектом КИИ;

б) субъект КИИ ликвидирован или реорганизован.

Также указывается, что в них могут участвовать самые разные специалисты, в том числе и финансово-экономические. А компаниям с разветвленной сетью филиалов разрешается создавать комиссии по категорированию в филиалах с передачей в центр координирующей функции.

В случае зависимости одного объекта КИИ от другого предполагается оценивать ущерб совместно. Сформулировано это так: "В случае если критический процесс зависит от иных критических процессов субъекта КИИ … оценка проводится по совокупному масштабу возможных последствий от нарушения или прекращения функционирования всех взаимозависимых критических процессов". То есть ущерб по-прежнему оценивается в рамках одного субъекта, хотя вполне возможна ситуация, когда ИС, например, транспортной компании зависит от функционирования ИТС мобильного оператора. Обе компании являются субъектами КИИ, но каждая будет оценивать ущерб только для своей инфраструктуры.

Новый вариант постановления также указывает на необходимость категорирования вновь создаваемых объектов КИИ, при этом включение таких объектов в первоначальный перечень, направляемый в ФСТЭК России, не требуется. Расширяется набор сведений, которые необходимо передавать в ФСТЭК России по результатам категорирования: кроме самих категорий, придется передавать сведения и об обосновании присвоения категорий, и даже информацию о неприменимости показателей к объекту КИИ, с обоснованием вывода. Эти сведения будут использоваться для проверки выводов комиссии о присвоении той или иной категории значимости объектам КИИ.

Изменены и критерии значимости. В показателях, характеризующих территорию (группа показателей социальной значимости), из оценки удалены муниципальные образования численностью до 2 тыс. человек для транспорта и до 3 тыс. человек для связи, однако порог попадания в значимые объекты снижен для этих отраслей. При расчете снижения уровня дохода субъектов КИИ используется усредненный за предыдущие пять лет годовой доход (вместо прогнозируемого), расширен диапазон значений показателей по категориям значимости. В связи с этим компаниям, в которых процедура категорирования уже была проведена, скорее всего, придется пересматривать категории значимости. Правда, если данные уже попали в реестр ФСТЭК России, то пересмотр показателей значимости предусмотрен только через пять лет; за это время, видимо, можно не пересматривать показатели, поскольку закон обратной силы не имеет.

Заключение

Первые результаты категорирования показали различные сложности в реализации этой процедуры, особенно в сложных холдинговых структурах, которые характерны для российского бизнеса. Кроме того, границы объекта КИИ не позволяют оценивать ущерб, который может быть нанесен критической инфраструктуре других компаний и ведомств. Оценка выполняется экспертами субъекта и может оказаться сильно заниженной: пока объективных и проверяемых показателей, к счастью, нет, поскольку точно их посчитать можно лишь на реальных инцидентах. Тем не менее компаниям придется в этом году как минимум завершить процесс категорирования по таким размытым критериям. Лучше всего с такой задачей справятся сторонние консультанты, которые имеют опыт в реализации проектов, проведении процедуры категорирования и оценки потенциального ущерба в компаниях из разных сфер экономической деятельности и могут посмотреть на картину со стороны.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Как оценивать ущерб для телекоммуникационных компаний, которые в соответствии с законом "О связи" могут не знать, в каких процессах используются их сети, а следовательно не могут рассчитать ущерб от прекращения деятельности. В частности, при передаче клиентом по сетям оператора конфиденциальной информации, естественно, с соблюдением всех требований по защите, оператор не может знать о содержании передаваемой информации и о возможном ущербе в случае ее недоставки в срок. Возможно, именно поэтому телекоммуникационные компании не торопятся проводить категорирование, поскольку не до конца понимают, как посчитать ущерб от временного прерывания функционирования их ИТС, т.к. ущерб наносится не им, но клиентам. Схожие проблемы существуют и в транспортной отрасли: компании, осуществляющие перевозки, не всегда могут оценить экономический ущерб клиенту в случае недоставки в срок из-за хакерской атаки угля для доменной печи непрерывного цикла.