Дмитрий КОСТРОВ: «Требования к средствам защиты КИИ должны быть согласованы с Минкомсвязи»

Интервью с заместителем директора департамента Министерства связи и массовых коммуникаций РФ

– Сейчас готовится законопроект «О безопасности критической информационной инфраструктуры Российской Федерации». Что будет означать принятие такого закона для отрасли связи?

– Законопроект в его нынешнем виде вызывает у нас очень много вопросов, в нем немало неясностей и недоговоренностей именно для отрасли связи. Вот лишь некоторые из них.

В законопроекте есть понятия объекта критической информационной инфраструктуры (КИИ) и субъекта критической информационной инфраструктуры – владельца КИИ. Субъект сам решает, относится ли его объект к КИИ, он вполне может решить, что нет, и не подавать сведений в реестр. Однако при этом предусмотрена весьма жесткая ответственность владельца за нарушение безопасности КИИ, вплоть до длительного тюремного заключения.

Операторы связи в законопроекте прямо называются субъектами КИИ. Но к какой категории оператору относить свою инфраструктуру? На базе одной и той же сети могут оказываться разные услуги различным категориям заказчиков. Если к сети оператора подключена АСУ ТП критически важного объекта первой категории, то по логике сеть тоже должна быть отнесена к первой категории. Но вопрос: сеть целиком или только ее часть с ближайшим узлом связи? Это нигде не объясняется. А что делать, если в рамках одного производственного цикла работают несколько территориально разнесенных предприятий? В обеспечение связи между ними могут быть вовлечены несколько операторов, в том числе те, чья инфраструктура не имеет непосредственного подключения к АСУ ТП. Как они должны категорировать свои объекты?

Скорее всего, федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности, будут требовать, чтобы все операторские инфраструктуры считались объектами КИИ. Необходимо четко прописать (желательно на уровне постановления Правительства РФ) порядок взаимодействия операторов с органами исполнительной власти, а также требования к техническим средствам, как это сделано для СОРМ. Оператор должен хорошо понимать, где чья сфера ответственности и во что ему обойдется обслуживание КВО. Продумать эти вещи нужно заранее. Принять закон, чтобы потом разбираться, как его выполнять, – не лучший подход.

– В законопроекте сказано, что регуляторы могут устанавливать дополнительные требования по обеспечению безопасности объектов КИИ исходя из их специфики. Будет ли Минкомсвязи как отраслевой регулятор вести такую работу?

– Как регулятор отрасли Минкомсвязи отвечает за устойчивость, целостность, безопасность сети связи общего пользования. Но, к сожалению, мы не видим в законопроекте отражения роли министерства.

Мы считаем, что приказы, определяющие требования к техническим средствам защиты КИИ, а также технические условия их установки должны согласовываться с Минкомсвязи. Иначе мы не сможем гарантировать устойчивость связи. Для согласования нам даже не нужно знать детали работы того или иного устройства, пусть его соответствие подтверждается сертификатом. Нас прежде всего интересует интерфейсная часть – мы должны понимать, что устройство не нарушит работу сети.

– Каковы сегодня угрозы и риски для клиента со стороны инфраструктуры связи? Существует ли модель угроз? От чего должны операторы защищать клиентов?

– Любое внешнее подключение создает риски. Но в зависимости от технологии подключения, оказываемых услуг меняется модель угроз. Одно дело, если мы имеем оптоволоконный канал «точка – точка», и совсем другое, если используем виртуальные сети; одно дело статическая маршрутизация, другое – динамическая и т. д. Поэтому в каждом случае вероятные угрозы нужно оценивать индивидуально.

В общем виде модели угроз, требований по безопасности к оператору связи (какие существуют в банковском секторе) нет. Возможно, они должны быть, но вопрос, кто должен определять эти требования. Скорее всего, клиент. Если он владеет критически важным объектом, то при наличии выбора

поинтересуется у оператора, есть ли у того модель нарушителя, готов ли он обеспечивать дополнительные меры защиты и т. п.

Но на сегодня оператор связи обязан оказывать только те услуги, которые прописаны в законе «О связи» и лицензии. Услуги связи могут оказываться в целях обеспечения безопасности государства и граждан, но о защищенности самой связи речь в законе не идет. Клиент может затребовать у оператора дополнительные услуги в рамках договора, тем более что защититься от некоторых видов атак (например, DDoS) без участия оператора весьма затруднительно. Однако будет ли выгодно оператору брать на себя нагрузку в виде дополнительных требований по безопасности со стороны владельцев КВО? Если закон обяжет оператора это делать, ему придется доказывать, что он способен это сделать. Но опять же вопрос: доказывать кому? И как? Эти вещи необходимо продумать до принятия закона.

– Как сами операторы относятся к перспективе стать владельцами объектов КИИ?

– В эту категорию попадут как минимум несколько ключевых операторов – хотя бы в силу охвата территории и социальной значимости своих услуг. Конечно, они это понимают. Все крупные операторы и отраслевые ассоциации направили свои замечания по законопроекту. Операторы сильно обеспокоены ситуацией, прежде всего потому, что не понимают, как выполнять требования будущего закона. Минкомсвязи как регулятор должно уметь им это разъяснить. Однако на данный момент у нас немало вопросов к самому законопроекту – в законопроекте слишком много неясностей, и сейчас мы активно обсуждаем это с разработчиком. Разработчик не всегда хорошо знает специфику отрасли, поэтому участие Минкомсвязи в доработке законопроекта необходимо. Если неопределенные места нельзя разъяснить в самом законе, нужно сделать это в подзаконных актах – в постановлении Правительства либо в совместном приказе Минкомсвязи и органов безопасности (но обязательно утвержденном в Минюсте, чтобы это был полноценный юридический документ). Нужен документ, разъясняющий, как категорировать объекты КИИ, находящиеся в собственности операторов связи. Вероятно, это может быть некий внутриведомственный документ.

> Оператор должен хорошо понимать, где чья сфера ответственности и во что ему обойдется обслуживание КВО. Продумать эти вещи нужно заранее. Принять закон, чтобы потом разбираться, как его выполнять, — не лучший подход.

> В общем виде модели угроз, требований по безопасности к оператору связи (какие существуют в банковском секторе) нет. Возможно, они должны быть, но вопрос, кто должен определять эти требования.

– Мы говорили о безопасности инфраструктуры связи для клиента оператора. А как насчет самого оператора? Ведь у него есть свои системы управления связью, АСУ. Их тоже надо защищать. Как с этим обстоит дело?

– Мы это называем технологическими сетями операторов связи. Конечно, их тоже надо защищать. Но соответствующих требований пока нет (если не считать приказа Минсвязи РФ № 113 «Об утверждении Правил ввода в эксплуатацию сооружений связи» и некоторых статей закона «О связи»). Вопросы обеспечения безопасности систем мониторинга и управления сетью, OSS/BSS решаются каждым оператором по-своему. Часто поддержка этих систем отдается на аутсорсинг, например зарубежному вендору. Так оказывается проще, поскольку продукты постоянно обновляются, а у операторов связи, как правило, нет своих достаточно квалифицированных специалистов. При этом создается канал удаленного управления… О какой технологической безопасности можно после этого говорить?

– Кто будет внедрять технические средства для защиты сетей электросвязи? Какие компетенции потребуются от исполнителей?

– Внедрять средства защиты будут, конечно, интеграторы – лицензиаты ФСТЭК и ФСБ. Прежде всего от них потребуется понимание технологий связи, особенностей протоколов, принципов работы современного оборудования от различных производителей. Такой интегратор обязательно должен иметь у себя сетевое подразделение. Классическая ИТ-безопасность и сетевая безопасность – не одно и то же, обеспечение безопасности сети операторского класса требует особых компетенций. ■