Объект, знай свою категорию

Издание: RSpectr.com, 6 февраля 2019 г.

Спикер: Михаил Савельев, директор по развитию бизнеса «Информзащиты»

С какими трудностями столкнулись компании, выполняя требования закона о безопасности критической информационной инфраструктуры.

Немногим более года назад — 1 января 2018-го — в России вступил в силу Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Чиновники положительно оценивают первые итоги реализации нормативной правовой базы в этой сфере. Эксперты, в свою очередь, обращают внимание на ее несовершенство, а также указывают на технические, организационные и финансовые сложности, с которыми пришлось столкнуться владельцам критической информационной инфраструктуры (КИИ).

Как идет реализация закона

Принятие базового документа потребовало разработки 18 новых нормативных правовых актов, конкретизирующих его положения. Наиболее важным является постановление правительства № 127, утверждающее критерии значимости объектов КИИ и порядок их категорирования. Оно вступило в силу 8 февраля 2018 года.

Выступая на «Инфофоруме-2019», заместитель директора Федеральной службы по техническому и экспортному контролю (ФСТЭК) России Виталий Лютиков отметил, что в настоящее время уже завершили категорирование и представили сведения во ФСТЭК около 700 организаций.

Более 1 800 владельцев КИИ определили объекты и осуществляют оценку их значимости

В октябре–ноябре 2018 года их было всего 700, уточнил В. Лютиков: «За последние несколько месяцев скачок существенный. Мы видим, что количество организаций, которые приступили к реализации нового закона, неуклонно растет. Около 15% субъектов КИИ находится в наиболее активной стадии. Остальные — на этапе подготовки к внедрению положений законодательства».

Сейчас оценку проходят более 27 тыс. объектов К. И. Как рассказал В. Лютиков, активнее всех ведут работу по категорированию организации из сфер здравоохранения, энергетики и топливно-энергетического комплекса, оборонно-промышленного комплекса, металлургической промышленности
После ряда выступлений на различных площадках представителей Центробанка повысилась интенсивность работы в банковской сфере.

В пресс-службе Сбербанка RSpectr сообщили, что организация своевременно направила ФСТЭК России информацию об объектах КИИ, предусмотренную законодательством, и сейчас проводит категорирование.

Телеком выполняет требования

«Менее активно реализуют положения закона, как ни странно, операторы связи. На сегодняшний момент порядка 40 операторов связи представили соответствующие сведения. Мы полагаем, что это достаточно мало», — заявил В. Лютиков.

Впрочем, опрошенные RSpectr представители операторов связи уверены, что все работы в рамках законодательства о безопасности КИИ будут выполнены.

Пресс-секретарь Группы МТС Алексей Меркутов обращает внимание на то, что в законодательстве не указаны сроки представления перечня объектов КИИ. «МТС ведет работу по определению критических процессов и объектов в установленные законодательством сроки в соответствии с проектом отраслевой Методики категорирования объектов КИИ, которую операторы предоставили во ФСТЭК», — рассказал А. Меркутов.

«МегаФон» утвердил и предоставил во ФСТЭК перечень объектов КИИ в декабре 2018 года, рассказал менеджер по бизнес-коммуникациям корпоративного бизнеса ПАО «МегаФон» Дмитрий Лукьянчиков. «По закону, у операторов есть год на осуществление категорирования. Мы активно принимаем участие в доработках постановления правительства», — добавил представитель оператора.

«Компания провела все необходимые действия, требуемые законодательством в области безопасности К. И. Перечни объектов определены, утверждены и направлены во ФСТЭК и Минкомсвязь России в установленные сроки», — сообщила руководитель пресс-службы ПАО «ВымпелКом» (бренд «Билайн») Анна Айбашева.

В «АКАДО Телеком» (ОАО «КОМКОР») направили во ФСТЭК перечень объектов КИИ, подлежащих категорированию. «Работу по категорированию мы проведем в ближайшее время. Все мероприятия в рамках исполнения закона о КИИ ведутся нами согласно плану», — отметили в пресс-службе.

В Netbynet (ООО «Нэт Бай Нэт Холдинг») подчеркивают, что

инфраструктура операторов связи распределенная и сложная, поэтому сравнивать их по срокам исполнения закона с другими компаниями не совсем корректно

«Спешка в этом деле может привести к пропуску важных систем и узлов связи», — предупредили в пресс-службе компании.

На данный момент в Netbynet осуществлена инвентаризация процессов и систем компании, что позволило подготовить и передать ФСТЭК в установленные сроки перечень объектов К. И. Разработаны локальные нормативные акты, проводится обучение сотрудников и повышение их осведомленности по тематике К. И.

Однако предстоит еще категорировать объекты КИИ, определенные в перечне, а также модернизировать существующую систему информационной безопасности.

Занижение значимости объектов

Несмотря на то что реализация положений закона о безопасности КИИ сегодня имеет положительную тенденцию, существуют проблемы методологического характера, отметил В. Лютиков.

Одна из самых важных, по его словам, — преднамеренное занижение субъектами КИИ значимости своих объектов. «Пользуясь различными несовершенствами норм, они стараются показать меньшие прогнозируемые последствия от компьютерных атак на инфраструктуру», — заявил В. Лютиков. Представитель ФСТЭК добавил, что законодательство в этой сфере будет дорабатываться — с учетом анализа правоприменительной практики и в диалоге с экспертным сообществом.

Организации, которые последовательно занимались развитием собственных систем информационной безопасности, продолжают это делать, но уже с учетом новых требований, прокомментировал ситуацию по просьбе RSpectr менеджер по развитию бизнеса «Лаборатории Касперского» Алексей Киселев. Те же, кто уклонялся от решения данной проблемы, продолжают это делать, в том числе занижают категории объектов КИИ, ссылаясь на различные юридические нюансы.

Что делать тем, кто уже провел категорирование?

Многие законопослушные субъекты КИИ столкнулись с рядом проблем при реализации закона.

По словам руководителя направления сервиса и аутсорсинга ИБ Центра информационной безопасности компании «Инфосистемы Джет» Екатерины Сюртуковой, основным сдерживающим фактором, помимо технических, организационных и финансовых сложностей (выполнение требований должно осуществляться за счет бюджетов самих субъектов КИИ), стало несовершенство законодательной базы. В документах отсутствуют четкие сроки выполнения требований, очевидные меры наказания. Также нет подзаконных актов, регламентирующих порядок взаимодействия с ГосСОПКА*. Ожидается, что они будут приняты к концу марта.
Несмотря на всю неопределенность, отдельные компании приступили к категорированию, и кто-то даже успел завершить процесс в 2018 году. Однако судьба проделанной работы под вопросом, отмечает Е. Сюртукова, так как сейчас вносятся изменения в правила категорирования. Согласно последней версии изменений в постановление № 127, будут существенно снижены показатели критериев, и теперь большая часть объектов КИИ станут значимыми. «Что делать тем, кто уже провел категорирование, непонятно; будут ли аннулированы результаты — в тексте проекта об этом информации тоже нет», — рассуждает Е. Сюртукова.

Вместе с тем

изменения привнесут ясность по срокам, новый дедлайн по утверждению перечня объектов КИИ — до 1 июня 2019 года

А потом у компаний будет год, чтобы определить значимость каждого объекта.

Затраты на информационную безопасность растут

Руководитель бизнес-направления «Защита АСУТП» ГК InfoWatch Михаил Смирнов отмечает необходимость выделения значительных средств на создание систем безопасности объектов КИИ со стороны собственников.

«Организации сталкиваются с существенными затратами на внедрение систем защиты технологических процессов от киберугроз, если ранее они отсутствовали.

И даже тем предприятиям, где уделялось большое внимание обеспечению информационной безопасности (ИБ), будет необходимо показать контролирующим организациям, что принятые меры для обеспечения безопасности значимого объекта КИИ (организационные, технические и т. д.) соответствуют тем, которые должны быть реализованы для объектов соответствующих категорий. В противном случае потребуются дополнительные средства на доработку систем безопасности», — говорит эксперт.

Немало вопросов возникает и с тем, какие решения по ИБ необходимо рассматривать и пилотировать уже сейчас для приобретения в следующем году, чтобы подойти готовыми к этапам интеграции с ГосСОПКА и создания системы обеспечения безопасности объектов КИИ. «Если на первом этапе –категорирование — большинство организаций может попробовать решить задачу своими силами, то для реализации последующих мы все же настоятельно рекомендуем привлекать ИБ-профессионалов, уже спроецировавших требования закона на предлагаемые решения и готовыми поделиться своей экспертизой», — советует А. Киселев.

С таким мнением солидарен специалист по защите критической инфраструктуры группы компаний Softline Максим Прохоров: «Учитывая высокую конкуренцию среди компаний, предоставляющих услуги по приведению IT-инфраструктуры в соответствие с требованиями регуляторов, важно с особым вниманием подходить к выбору подрядчика. От качества выполнения работ зависит уровень защиты объектов КИИ, а вся ответственность за огрехи исполнителя в случае возникновения инцидентов ляжет на заказчика».

Стадия обсуждения корректировок

Число запросов, связанных с защитой автоматизированных систем управления технологическими процессами (АСУТП) и защитой ИБ на объектах КИИ, в Softline выросло за последний год примерно на 30% и будет расти дальше, прогнозируют в компании.

М. Прохоров уверен, что

несомненно, проекты в области защиты КИИ стали трендом 2018 года в области ИБ и останутся таковыми в следующие несколько лет

Есть определенные сложности, связанные с методологией и интерпретацией законодательства, резюмирует руководитель направления Защиты АСУ ТП компании «Ростелеком-Solar» Владимир Карантаев. При этом он отмечает, что ФСТЭК ведет работу в этом направлении и в последние годы занимает очень открытую позицию. На старте принятия подзаконных нормативных актов практически со всеми представителями отраслей были проведены консультации, что, безусловно, положительно повлияло на итоговые положения закона.

На основе этой наработанной практики сейчас также проводятся обсуждения корректировок и изменений в постановление № 127, рассказал В. Карантаев.

«Понятно, что при формировании новых регуляторных требований всегда возникают разногласия экспертов, отношение объектов регулирования к закону может быть разным. Но все же 187-ФЗ появился очень своевременно — на старте цифровой трансформации.

То, что практически все 12 отраслей, перечисленных в законе о безопасности КИИ, будут затронуты глобальными процессами цифровой трансформации, — это факт.
И о безопасности нужно думать именно сейчас, на старте, а не после внедрения новых систем», — подчеркнул В. Карантаев.

СПРАВКА

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» определяет основные понятия и принципы обеспечения безопасности КИИ для ее устойчивой работы во время компьютерных атак. В законе прописаны полномочия государственных органов, а также права, обязанности и ответственность организаций, работающих в этой сфере.

Объекты КИИ и сети связи для взаимодействия между ними составляют понятие критической информационной инфраструктуры.

Требования закона затрагивают государственные и частные организации, которые владеют объектами КИИ или арендуют их (субъекты КИИ).

Закон содержит требование к владельцам КИИ о подключении объектов к системе ГосСОПКА, созданной Федеральной службой безопасности (ФСБ) по поручению президента.

Контроль и регулирование в области обеспечения безопасности объектов КИИ, включая регулирование, возложены на ФСБ и ФСТЭК, которая также ведет реестр таких объектов.

Вместе с принятием закона в УК РФ была добавлена статья 274.1, которая устанавливает уголовную ответственность:

• за создание, распространение и (или) использование компьютерных программ, заведомо предназначенных для неправомерного воздействия на КИИ РФ;
• за неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ;

• за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ.

Мнение эксперта

Михаил Савельев,

директор по развитию бизнеса компании «Информзащита:

— Такие масштабные законы, как 187-ФЗ, обычно проходят так называемые типовые стадии принятия неизбежного. За 2018 год, по моему мнению, сообществу удалось преодолеть фазы «отрицания» и «гнева».

Под этим я подразумеваю то, что практически весь год мы потратили на убеждение друг друга в принадлежности к множеству «субъектов КИИ», разбирали неизбежные погрешности нового закона, ждали, жадно читали и обсуждали нюансы подзаконных актов, «гневно» цепляясь за любые шероховатости и «завышенные» требования.

Неопределенность со сроками выполнения первого этапа пути по приведению себя в соответствие требованиям закона (я говорю о составлении перечня объектов), которые появились из-за того, что из постановления правительства были исключены упоминания конкретных временных рамок, а также отсутствие прямой ответственности за непредставление сведений немного затянули эти фазы.

В конце 2018 года мы начали переходить на стадию «торга». Это выражается в том, что субъекты начинают задумываться, как выполнить закон с минимальными затратами. Кто-то ищет способы снизить категорию значимости своих объектов, кто-то переживает, что зря включил в уже поданный список объекты, которые не являются значимыми. Задумываясь о выполнении требований, связанных с подключением к ГосСОПКА, субъекты начинают торговаться о том, что должен отсылать в НКЦКИ** обслуживающий их центр. При отсутствии практики работы многие опасаются, что любая отправленная информация об инцидентах повлечет внеплановые проверки со стороны регуляторов.

Мне хочется верить, что мы сможем быстро проскочить фазу «депрессии», которая может выражаться в затягивании сроков защитных мер, и скорее приступим к реальным шагам по обеспечению безопасности критической инфраструктуры.

___

** ГосСОПКА — Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак.*

*** НКЦКИ — Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Был создан в сентябре 2018 года приказом директора ФСБ Александра Бортникова. Задачей НКЦКИ является обеспечение координации деятельности субъектов КИИ РФ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.*

Подробнее: https://rspectr.com/articles/483/obekt-znaj-svoyu-kategoriyu