Приложение 1

Предложения
по реализации Федерального закона от 26.07.2017 № 187- ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее ФЗ-187) является основой, задающей базовые понятия и принципы обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее - КИИ).

Эффективность практической реализации (1)3-187 будет зависеть от качества подзаконных нормативных правовых актов (далее-НПА), завершение принятия которых ожидается в первом полугодии 2018 года.

Поддерживая усилия государственных органов, направленные на обеспечение безопасности КИИ, полагаем, что при принятии на уровне НПА решений о способах обеспечения безопасности КИИ необходимо избежать введения избыточных обязанностей, запретов и ограничений, а также положений, способствующих возникновению необоснованных расходов в сфере предпринимательской деятельности.

Для реализации требований ФЗ-187 осуществляется подготовка и принятие ряда НПА, большая часть которых уже принята с выборочным привлечением к обсуждению представителей бизнес-сообщества, но не все замечания бизнеса учтены. Опыт показывает, что требования, разработанные без участия бизнеса, часто являются завышенными, труднореализуемыми технически, не учитывающими реальные процессы бизнес-планирования и бюджетирования. Поэтому такие проекты долго согласовываются, приводят к срыву сроков, неэффективным затратам и в итоге оказываются неоптимальными ни для бизнеса, ни для государства.

В этой связи предлагается:

1. Министерствам и ведомствам Российской Федерации, ответственным за разработку НПА (ФСТЭК России, ФСБ России, Минкомсвязь России) обеспечить привлечение к подготовке проектов НПА, в том числе о внесении изменений в принятые НПА, экспертов-представителей российского бизнеса (отраслевые рабочие группы по вопросам реализации требований ФЗ-187).

Использовать РСПП как консолидированную площадку для взаимодействия органов государственной власти и бизнеса при разработке проектов нормативных правовых актов, регулярной оценки правоприменительной практики при реализации ФЗ-187.

2. В НПА по реализации ФЗ-187 необходимо учитывать отраслевые особенности субъекта КИИ.

В этой связи предлагается:

- ФСТЭК России оказать методическую помощь субъектам КИИ в проведении категорирования объектов КИИ с учетом отраслевых особенностей;

- Правительству РФ рассмотреть возможность создания отраслевых Центров мониторинга и реагирования на компьютерные инциденты (с привлечением к деятельности таких Центров представителей ФСТЭК России, ФСБ России).

Задачами таких Центров могут стать: сосредоточение отраслевых компетенций и оказание субъектам КИИ методологической помощи по обеспечению безопасного и устойчивого функционирования объектов КИИ;

распространение передового опыта защиты объектов КИИ, в том числе путем организации взаимодействия с аналогичными международными центрами; подготовка предложений по эффективной реализации регуляторных инициатив в сфере безопасности КИИ с учетом особенностей каждой отрасли; своевременное информирование субъектов КИИ по актуальным вопросам информационной безопасности.

3. Реализация ФЗ-187 потребует от бизнеса значительных дополнительных затрат, которые по существу не будут являться инвестициями в бизнес, что затормозит его развитие.

Вместе с тем, для повышения эффективности разработки мер по обеспечению безопасности КИИ представляется целесообразным стимулировать бизнес к сотрудничеству с соответствующими органами государственной власти в вопросах выявления уязвимостей защиты КИИ.

В этой связи предлагается Правительству РФ рассмотреть возможность:

- стимулирования субъектов КИИ в части обеспечения безопасности объектов КИИ: налоговые льготы, субсидии и прочее;
- поощрения положительной деятельности субъектов КИИ, организаций или частных лиц в отношении поиска уязвимостей программного обеспечения или аппаратных средств защиты КИИ и передачи результатов указанной деятельности соответствующим государственным органам.

4. Требования НПА, направленные на реализацию ФЗ-187, не должны необоснованно ограничивать выбор технических средств защиты КИИ и возможных поставщиков продуктов и услуг (интеграторов). Это может привести к снижению уровня конкуренции, росту итоговой стоимости внедрения и владения техническими средствами защиты КИИ.

В этой связи ФАС России предлагается взять под контроль вопрос обеспечения формирования конкурентной среды при реализации ФЗ-187.

5. Одной из важнейших составных частей в обеспечении безопасности КИИ является государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА, отв. ФСБ России). В указанную систему должна стекаться информация, в том числе, об инцидентах в сфере информационной безопасности, от всех субъектов КИИ.

На базе указанной информации может быть выстроена мощная платформа для проведения анализа с целью выработки мер противодействия угрозам, подготовки рекомендаций, создания единой базы знаний, подготовки аналитических отчетов, в том числе, отраслевыми Центрами мониторинга и реагирования на компьютерные инциденты и т.п.

6. В настоящее время организации и предприятия, которые являются субъектами КИИ при закупке программных продуктов у зарубежных компаний-разработчиков требуют проведения сертификации в рамках системы сертификации средств защиты информации по требованиям безопасности информации. При этом доступ экспертам аккредитованной организации к исходному тексту и\или коду программного обеспечения предоставляется в лабораториях вне России без ограничений и в требуемое время с соблюдением установленных правил

безопасности и заключением соответствующего соглашения о конфиденциальности.

Существует озабоченность, что при введении в действие 187-ФЗ, будут ужесточены требования по сертификации программных продуктов, которые включают функции безопасности, что существенно затруднит продвижение решений международных компаний на российском рынке и поставит под угрозу дальнейшую модернизацию уже развернутых систем.

В этой связи Правительству РФ при реализации 187-ФЗ предлагается сохранить существующий порядок, позволяющий осуществлять контроль исходного текста и\или кода программного обеспечения, для целей проведения его сертификации по требованиям информационной безопасности на территории стран-разработчиков с соблюдением установленных требований по безопасности и заключением соответствующего соглашения о конфиденциальности.

7. В соответствии с постановлением Правительства РФ от 08.02.2018 № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" к значимым объектам КИИ может быть отнесена существенная часть информационных систем, а также существует вероятность отнесения к значимым объектам КИИ сетей связи операторов, входящих в состав сети связи общего пользования (далее - ССОП). При этом к объектам КИИ могут быть отнесены объекты ССОП, для которых установленные законодательством требования к защите информации не могут быть в полной мере реализованы технически и с приемлемыми для бизнеса затратами.

В этой связи ФСТЭК России предлагается:

- инициировать внесение поправок в ФЗ-187 с целью определения, что сети связи операторов связи, входящие в ССОП, не являются объектами КИИ (на сегодняшний день существует неопределенность, что нужно отнести к понятию ИТКС).

Критерии и методика должны обеспечивать отнесение к значимым только объектов с высоким (катастрофическим) потенциальным ущербом в случае нарушения безопасности информации. Все меры защиты объектов КИИ должны быть реализованы на защищаемых объектах КИИ, при этом ССОП должны функционировать в обычном режиме без реализации дополнительных мер защиты.

8. Особое внимание следует уделить ФЗ-187 как инструменту противодействия рискам, которые могут возникнуть в результате угроз внешнего воздействия на элементы КИИ, построенные на импортных технологиях и оборудовании.

В этой связи предлагается:

- провести, с привлечением специалистов РАН, МО РФ, РИСИ, ВШЭ, заинтересованных структур научно-исследовательские работы по созданию модели угроз, возникающих в результате возможного проведения западными странами воздействия на импортозависимые информационные системы, технологии и оборудование, входящие в состав объектов КИИ. Подготовить предложения по оптимальному парированию этих угроз с детализацией по отраслям и видам оборудования.

- организовать обучающие мероприятия для специалистов субъектов КИИ. направленные на их подготовку К реализации ФЗ-187.

9. Обеспокоенность бизнес-сообщества вызывают следующие вопросы:

9.1. Неопределенность в вопросе возможности отнесения сведений о предпринимаемых мерах по обеспечению безопасности объектов КИИ к государственной тайне.

Обременение предприятий, не связанных с обеспечением обороноспособности государства, вопросами организации работ в рамках режима государственной тайны представляется излишним.

В этой связи представляется необходимым министерствам и ведомствам Российской Федерации при разработке НПА избежать отнесения сведений о мерах по обеспечению безопасности объектов КИИ к государственной тайне.

9.2. Наличие уголовной ответственности (введена новая статья 274.1 УК РФ) за преступные действия, связанные с созданием, распространением и/или использованием компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру РФ; неправомерным доступом к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ; нарушением правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ в виде лишения свободы на срок до 10 лет.

Это повлечет отток специалистов из области обеспечения информационной безопасности КИИ либо потребует значительного повышения фонда оплаты труда таких специалистов.

9.3. В настоящее время ч. 3 ст. 274.1 УК РФ за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда КИИ, предусмотрено наказание принудительными работами на срок до пяти лет либо лишением свободы на срок до шести лет.

Дифференциация наказания в зависимости от общественной опасности последствий указанных нарушений не предусмотрена.

Это положение не соответствует проводимому руководством РФ курсу на либерализацию уголовного законодательства для формирования благоприятных условий для ведения бизнеса и создает неоправданно высокие риски. Вызывает опасения также то, что для определения общественно-опасных деяний используются признаки только субъективно-оценочного характера (причинение вреда КИИ), что может привести к трудностям в правоприменении и в совокупности с беспрецедентно строгим наказанием может стать катализатором коррупции.

В этой связи Правительству Российской Федерации предлагается разработать законопроект, предусматривающий дифференцированную ответственность, включая административную, в зависимости от общественной опасности соответствующих деяний.

10. Поэтапное внедрение решения по обеспечению информационной безопасности.

В связи с тем, что во многих компаниях уже внедрены и эффективно используются те или иные решения по обеспечению информационной безопасности, во избежание их существенной переработки и/или обязательного использования сертифицированных средств (что влечет значительную дополнительную финансовую нагрузку на бизнес) предоставить федеральным органам исполнительной власти, ответственным за разработку и внесение изменений в НПА, следующие варианты приведения в соответствие:

1. Вновь реализуемые проекты и решения должны соответствовать утвержденным требованиям.

2. Для уже существующих решений ввести «переходный период» с учетом того, что уже закупленное и смонтированное оборудование должно выработать свой ресурс.

3. Завершенные решения и решения, реализованные более чем на 20%, оставить неизменными в том случае, если они удовлетворяют требованиям по защите, но не удовлетворяют в полной мере требованиям по наличию сертификатов и т.д.

11. Конкретизация терминологии для категорирования объектов.

В связи с тем, что использование терминов «транспорт», «сети», «системы управления» и т.п. не позволяют однозначно определить круг субъектов и объектов, на которых распространяется предмет регулирования ФЗ-187, а тем более определить перечень объектов регулирования, которые подлежат категорированию в соответствии с ФЗ-187, необходимо при разработке нормативных правовых актов конкретизировать терминологию, в том числе в части ИТКС.

12. Формулировки в части хранения информации требуют детализации.

Необходимо детализировать в проекте «Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты», утверждаемый приказом ФСБ России (размещался на общественное обсуждение в феврале 2018г.) ряд используемых понятий в части объемов и времени хранения информации. На данный момент отсутствие детализации может привести к значительным финансовым и инфраструктурным нагрузкам для бизнеса, по аналогии с «Законом Яровой».

13. Использование механизмов саморегулирования для принятия оперативных решений.

С целью унификации стандартов, снижения рисков неисполнения требований закона, повышения ответственности участников рынка, необходимых для реализации ФЗ-187, рассмотреть передачу части контролирующих функций, требующих максимальной оперативности принятия решений от государства, профессиональному сообществу.

Предлагается Правительству Российской Федерации и Государственной Думе Российской Федерации рассмотреть возможность использования механизмов саморегулирования (СРО).