КРУГЛЫЙ СТОЛ

Обсуждаем законопроект «О безопасности критической информационной инфраструктуры Российской Федерации»

В круглом столе принимают участие

Дмитрий БУЗЫКИН,
технический директор,
ЗАО «С-Терра СиЭсПи»

Сергей ВИХОРЕВ,
заместитель генерального директора по развитию,
компания «Элвис плюс»

Сергей ГАРБУК,
заместитель генерального директора, Фонд перспективных исследований

Игорь КОРЧАГИН,
специалист по ИБ,
компания ИВК

Алексей КОСИХИН,
руководитель направления по работе с ТЭК Центра информационной безопасности,
компания «Инфосистемы Джет»

Алексей МАЛЬНЕВ,
начальник отдела защиты КСИИ,
«АМТ-ГРУП»

Рустэм ХАЙРЕТДИНОВ,
CEO,
компания Appercut Security

Станислав ШЕВЧЕНКО,
технический директор,
компания SafenSoft

На профильных форумах экспертами неоднократно поднимался вопрос о недостаточной четкости толкования терминологии и базовых понятий. Насколько полно, по вашему мнению, в проекте закона проработаны эти вопросы?

ДМИТРИЙ БУЗЫКИН

Все десять лет своего существования «С-Терра СиЭсПи» наблюдает интерес к данной теме. Однако из всего информационного шума, поднятого в Интернете, через фильтр официального обсуждения законопроекта прошли только шесть (или пять?) обращений. (Почему «шесть» это «пять», видно на стр. 22 сводки предложений, поступивших в ходе общественного обсуждения законопроекта.)

Существует ли конструктивный спор вне стен регуляторов? Да, ФСБ России прикладывает усилия к гармонизации законодательства. Прежде по этой теме уже были законодательные инициативы со стороны как депутатов (2006 г.), так и другого регулятора – ФСТЭК (2012 г.). На текущий момент ориентир процесса задан в «Основных направлениях государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», утвержденных Президентом РФ 12 февраля 2012 г.

На предложения, не касающиеся редакции законопроекта, ФСБ дала первичные ответы. Ответы не исчерпывающие, порой спорные, но ими можно и должно «заниматься более плотно».

СЕРГЕЙ ВИХОРЕВ

Проблема тезауруса очень важна. Однако толкование терминов и базовых понятий – это не сфера закона. Термины должны определяться стандартом. На мой взгляд, ст. 2 перегружена понятиями, которые не используются в самом законе. И приведенные термины не всегда совпадают с уже принятыми в этой области. К примеру, понятие «информационные ресурсы» не совпадает с определением «трехглавого» закона (№ 149-ФЗ). Некоторые термины трактуются слишком широко (понятия «информационный ресурс» или «автоматизированная система управления производственными и технологическими процессами»), что делает неопределенной сферу применения закона. Одно слово «производственные» включает в сферу действия закона практически все информационные системы предприятия, даже систему складского учета. На мой взгляд, эта статья требует доработки.

СЕРГЕЙ ГАРБУК

Проект закона способствует совершенствованию отечественной нормативной базы в сфере безопасности критически важной инфраструктуры Российской Федерации. Некоторое «умножение сущностей» обусловлено понятным стремлением гармонизировать законопроект с соответствующими зарубежными нормативными документами, а противоречивость формулировок – необходимостью обеспечить преемственность с существующей отечественной нормативной правовой базой в этой области, которая сама по себе является весьма противоречивой. Тем не менее некоторые термины требуют уточнения. Так, например, введенное понятие «АСУ производственными и технологическим процессами» противоречит устоявшемуся определению автоматизированной системы по ГОСТ 34.003, согласно которому в состав АС помимо средств автоматизации входит и персонал. Для более точной передачи смысла полезной представляется также замена термина «критическая информационная инфраструктура» на «критически важная информационная инфраструктура». Не вполне оправданно использование кальки «компьютерный инцидент» взамен принятого в серии стандартов ISO/IEC 27000 и ряде других нормативных документов понятия «инцидент информационной безопасности».

ИГОРЬ КОРЧАГИН

Действительно, к терминологии, используемой в законопроекте, у многих специалистов и экспертов имеются замечания, которые, в частности, были представлены на публичном обсуждении законопроекта. Наибольшее количество вопросов вызывают такие определения, как «автоматизированная система управления производственными и технологическими процессами», «компьютерная атака», «компьютерный инцидент». В первую очередь это вызвано несогласованностью с терминологией существующих ГОСТов. Практически ни одно представленное замечание не было учтено разработчиками законопроекта, которые ссылаются на преемственность с «Основными направлениями государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации».

АЛЕКСЕЙ КОСИХИН

Большинство терминов, определений и базовых понятий законопроекта заимствовано из документов, распоряжений, указов и т. п., изданных ранее. Степень четкости и понятности толкования того или иного термина либо базового понятия каждый для себя определяет самостоятельно, и скорее всего, всегда будут те, кто недопонял, иначе истолковал и т. д. Чтобы этого избежать, законопроект и был выставлен на публичное обсуждение. Само принятие законопроекта (если это произойдет) может расцениваться как серьезный шаг к обеспечению безопасности в той области, которой до недавнего времени в нашей стране уделяли очень мало внимания.

РУСТЭМ ХАЙРЕТДИНОВ

Идеальные законы – редкость, а первая версия закона и не может быть идеальной. Попытки охватить все аспекты проблемы привели к размытости формулировок, однако ценность закона не в этом. В областях, где от регулирования зависят жизни людей, нельзя действовать по банковским схемам: мол, накопим статистику инцидентов, тогда и будем регулировать. Само появление закона привлекло внимание к проблеме, а формулировки будут оттачиваться, в том числе и при участии экспертного сообщества.

СТАНИСЛАВ ШЕВЧЕНКО

Как сказано в первых строках проекта, закон устанавливает основы обеспечения безопасности информационной инфраструктуры. «Информационная инфраструктура» – технический термин, для однозначного понимания он должен рассматриваться как определение, не терпящее двусмысленностей. Технический подход к рассмотрению инфраструктуры предполагает перечень и спецификацию всех входящих в эту инфраструктуру сущностей. В проекте четко не определен объектный состав критической информационной инфраструктуры (КИИ), подобная неточность может позволить произвольно относить объекты к подпадающим или не подпадающим под действие закона. С учетом динамики информатизации имеет смысл периодически определять точный перечень объектов критической информационной структуры РФ.

В пункте 4.1 сказано, что обеспечение безопасности подразумевает недопущение нарушения или прекращения функционирования КИИ РФ. Но наиболее распространенным деструктивным воздействием на системы является хищение или подмена данных, не приводящие к нарушению или прекращению функционирования атакуемой системы, однако при этом несущие в себе серьезную опасность для КИИ в целом.

В пункте 4.4 целесообразно определить и точно расписать, какие федеральные органы какими компетенциями обладают.

В документе используются термины «высокая категория опасности», «средняя категория опасности» и «низкая категория опасности», но в тексте они не определены. В статье 11 отсутствуют требования к базам данных.

В проекте закона прописаны критерии, по которым должно осуществляться категорирование объектов. Насколько необходимым и достаточным является этот перечень? Какова степень измеряемости и сопоставимости приведенных критериев?

ДМИТРИЙ БУЗЫКИН

В законопроекте использован не перечневый, а критериальный подход к отнесению объектов информационной инфраструктуры к критическим. Критерии установлены в ч. 2 ст. 8 законопроекта. Полагаем, что список значимых критериев не может быть закрытым и тем более рейтинговым («деньги или жизнь», «экология или оборона»). Показатели критериев, в соответствии с которыми владельцы объектов КИИ смогут относить их к той или иной категории опасности, должны быть определены в подзаконных актах с возможностью их судебного обжалования.

СЕРГЕЙ ВИХОРЕВ

В части критериев отнесения объектов к критическим в законопроекте ничего нового нет. Еще в 2005 г. Совбез России определил эти критерии. Основным признаком принадлежности объекта к критически важным Совбез назвал наличие на объекте экологически опасного или социально значимого производства либо технологического процесса, нарушение штатного режима которого приводит к чрезвычайной ситуации. Если посмотреть внимательно, приведенные в законе критерии как раз и описывают этот признак. Только сами по себе они действовать не будут. Тем более что категорировать будут сами субъекты. Здесь нужны четкие методики определения критериев. Только тогда эти критерии будут сопоставимы и измеряемы. Только тогда их можно будет проверить и избежать излишних трат, ведь некоторые руководители захотят отнести свои объекты к критическим только из амбиций или для получения дополнительного финансирования. Будем надеяться, что такие методики появятся.

СЕРГЕЙ ГАРБУК

Общепринятый подход к категорированию объектов по критериям безопасности подразумевает оценку рисков, связанных с реализацией угроз безопасности. В случае с информационными системами критически важных объектов риски от нарушения или прекращения функционирования этих информационных систем должны оцениваться не столько на уровне объектов информационной инфраструктуры, сколько на уровне самих критически важных объектов. Таким образом, категория объекта КИИ должна принципиальным образом зависеть от категории соответствующего критически важного объекта. В то же время в законопроекте не учтена нормативно закрепленная практика, сложившаяся в области категорирования объектов различных критически важных инфраструктур, в частности топливно-энергетической (в соответствии с № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса») и транспортной (№ 16-ФЗ «О транспортной безопасности»). Это приведет к избыточной нормативной нагрузке на субъекты информационных инфраструктур и затруднит учет отраслевой специфики при оценивании возможных рисков. Можно предположить, что критерии категорирования объекта КИИ должны включать единственный критерий, характеризующий тяжесть возможных последствий на соответствующем критически важном объекте, а также совокупность критериев, характеризующих потенциальную уязвимость объекта информационной инфраструктуры с учетом актуальной модели угроз.

ИГОРЬ КОРЧАГИН

Необходимость всех представленных в законопроекте критериев не вызывает сомнений. Но судить об их достаточности сложно, так как однозначно не определено, кто подпадет под понятие КВО. Стоит отметить, что в данном перечне не учитывались влияния друг на друга различных инфраструктур, что могло бы тоже стать одним из критериев категорирования КВО.

Еще более сложным является объективное измерение перечисленных критериев, особенно когда они носят качественный характер. Только после предоставления регуляторами показателей критериев категорирования

можно будет оценить адекватность данных критериев по отношению к реальным условиям функционирования АСУ производственными и технологическими процессами КВО и обеспечения их безопасности.

АЛЕКСЕЙ КОСИХИН

В законопроекте прописаны семь критериев. Исходя из нашего опыта, каждые критичная система или объект КИИ будут обладать признаками от трех до пяти критериев, которые вполне можно сопоставить. А вот их измеримость – другой вопрос. Надо дождаться нормативных правовых актов, изданных во исполнение закона, в которых это должно быть прописано. Тут опять ожидается огромное количество споров. Как, например, измерить ущерб, который понесет государство по критерию социальной значимости? Или по критерию значимости для национальной безопасности? Эти вопросы пока остаются открытыми.

СТАНИСЛАВ ШЕВЧЕНКО

В статье 1 говорится о том, что закон определяет порядок обнаружения, предупреждения и ликвидации возможных последствий, однако упущена такая сфера, как расследование совершенных атак. Без четко прописанного порядка расследования инцидентов вероятность успешной реализации такой практики снижается. Желательно законодательно обязать иметь всю информацию о произошедшем инциденте с установлением авторства и мотивов совершения атаки. В связи с этим стоит также дополнить словами «расследовании атак» п. 4.2.7 и 4.2.11.

В законопроекте указаны три категории критически важных объектов (КВО). Каким вам представляется сам механизм категорирования, т. е. отнесения КВО к конкретной категории? На каких принципах должен базироваться этот механизм?

ДМИТРИЙ БУЗЫКИН

Перечень критически важных областей можно указать в нормативном документе уровня постановления Правительства с ежегодным пересмотром, в частности с учетом международных обязательств Российской Федерации. Вводить ли не трех-, а пяти- или N-балльную систему, можно будет определить на последующих этапах законотворческой деятельности с учетом разграничения полномочий между федеральными органами власти и органами власти субъектов РФ.

СЕРГЕЙ ВИХОРЕВ

Механизм прописан в законе: субъект критической инфраструктуры проводит оценку показателей по каждому установленному критерию, выбирает соответствующую категорию КВО; уполномоченный госорган проверяет правильность категорирования, если надо, поправляет субъекта и после устранения замечаний вносит в реестр. Схема вполне рабочая, если учесть, что многие КВО находятся в ведении самостоятельных хозяйствующих субъектов и даже не относятся к какой-то отрасли. А принцип должен быть один: оценка возможных последствий (вреда) для гражданина, общества, государства в результате чрезвычайных ситуаций по каждому из критериев, приведенных в законе. И здесь без четких методик не обойтись.

СЕРГЕЙ ГАРБУК

Как уже было отмечено, механизмы категорирования объектов по критериям безопасности достаточно детально отработаны и в международной, и в отечественной практике. Обычно решение об отнесении критически важного объекта к той или иной категории принимается на основании двух интегральных критериев, один из которых характеризует потенциальный материальный ущерб, а другой – опасность для жизни и здоровья людей. В принципе, все критерии, перечисленные в ч. 2 ст. 8 законопроекта, являются промежуточными и могут быть сведены к этим двум интегральным критериям. При этом конкретные критериальные параметры для отдельных категорий опасности могут быть определены в соответствующих подзаконных актах.

АЛЕКСЕЙ МАЛЬНЕВ

Категорирование является ключевым вопросом в контексте решаемых задач. Ни с экономической, ни с практической точек зрения было бы некорректно регламентировать одни и те же меры защиты для объектов разных категорий важности. Но еще более важны организация и контроль процесса категоризации. Не секрет, что субъекты критической инфраструктуры зачастую заинтересованы иметь категоризацию минимального уровня для снижения издержек. В главе 3 ст. 8 регламентирована самостоятельная категоризация субъектом критической инфраструктуры с последующим направлением результатов в федеральные органы исполнительной власти. На этом этапе большое значение имеет экспертный подход соответствующих подразделений органов исполнительной власти (ФСБ и ФСТЭК) для исключения попыток и возможности необъективного занижения категории опасности объекта. В целом, на наш взгляд, для законодательного уровня градаций по критериям достаточно. Важно корректное исполнение данных требований.

Законопроект предусматривает введение в случае необходимости дополнительных требований отраслевыми регуляторами. Какие отрасли/сферы регулирования требуют более «тонкой» настройки? Готовы ли, на ваш взгляд, соответствующие ведомства к подобной работе?

СЕРГЕЙ ВИХОРЕВ

Объекты каждой отрасли уникальны по-своему, уникальны и применяемые там АСУ ТП. Конечно же, «тонкая» настройка нужна.

Готовы ли ведомства к такой работе? Пока, наверное, не все. Поэтому

и норма закона, позволяющая вводить дополнительные требования, не является императивной (все-таки последнее слово за ФСТЭК и ФСБ). Однако к этому надо стремиться. Ведомствам виднее, где слабые места. Думаю, здесь пойдет итерационный процесс: ФСТЭК и ФСБ выдвинут основные общие требования, отрасли по ним поживут, увидят нерешенные вопросы, накопят опыт и дополнят общие требования своей спецификой. Если закон предписывает заниматься этой проблемой, то со временем и в отраслях появятся грамотные специалисты.

СЕРГЕЙ ГАРБУК

Вовлечение отраслевых регуляторов в работу по нормативному регулированию вопросов обеспечения безопасности объектов КИИ целесообразно, по крайней мере при оценивании возможных последствий от реализации угроз, а также при определении допустимости применения различных мер организационного и технического характера на конкретных инфраструктурных объектах. В большинстве отраслей подобная работа уже ведется, и необходимо, чтобы разрабатываемый законопроект способствовал интеграции этих усилий.

РУСТЭМ ХАЙРЕТДИНОВ

Пока регуляторы не обладают требуемой отраслевой компетенцией. Однако профессиональным сообществом, профильными министерствами и СРО накоплен достаточный опыт применения стандартов. Если регуляторы учтут этот опыт и смогут распространить лучшие практики на всю отрасль, регулирование пойдет на пользу защищенности критически важных объектов.

В проекте прописывается обязанность субъектов информировать регулятора о компьютерных инцидентах, затрагивающих безопасность КВО. Не секрет, что для отечественного бизнеса не характерно «выносить сор из избы», более того, распространение информации сотрудниками об инцидентах зачастую жестко пресекается. Насколько готовы, по вашим наблюдениям, отечественные предприятия и компании к подобной практике? Какова степень готовности самого регулятора такую практику насаждать?

СЕРГЕЙ ВИХОРЕВ

За рубежом такая практика является нормой. Только большая статистика позволяет провести объективный анализ и выработать адекватные меры. И здесь общественные интересы должны превалировать над корпоративными. Тем более что речь идет не об инцидентах вообще, а об инцидентах на критически важных объектах. Да, это чувствительная информация и относиться к ней надо с осторожностью, но делиться ею необходимо – это поможет другим.

А проводить такую политику регулятор, конечно, будет, даже «силовыми» (но законными) методами.

СЕРГЕЙ ГАРБУК

В законопроекте однозначно указывается, что сведения, полученные в ходе проведения оценки защищенности, раскрывающие уязвимость объекта КИИ, а также сведения, содержащиеся в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, относятся к информации ограниченного доступа. Обязательность выполнения требований по обеспечению конфиденциальности подобных сведений в сочетании с пониманием субъектами КИИ целесообразности выполнения требований по информированию регуляторов об инцидентах информационной безопасности обеспечит эффективность данной регулирующей нормы.

ИГОРЬ КОРЧАГИН

Вероятно, не все отечественные предприятия готовы уведомлять регулятора о компьютерных инцидентах по причине нежелания допускать вмешательство сторонних лиц на свою «кухню». А с учетом того, что в соответствии с законопроектом информация о компьютерном инциденте может стать основанием для внеплановой проверки, субъекты КИИ, вероятно, будут пытаться ее скрывать. Конечно, вероятность такого сценария зависит от масштабов произошедших событий и их последствий.

АЛЕКСЕЙ КОСИХИН

Действительно, данная обязанность порождает огромное число вопросов. Например, в каком виде следует передавать информацию? Допустим, это будет «универсальная карточка инцидента», содержащая информацию об источнике угрозы, объекте атаки, оцененных последствиях атаки, предпринятых мерах по нейтрализации, мерах, направленных на недопущение инцидентов в дальнейшем. По каким каналам передавать информацию? Как регулятор будет ее хранить? Как обеспечить ее безопасное хранение? Какова ответственность в случае утечки или разглашения? Это же масса рисков как для субъектов, передающих информацию о своих уязвимостях, так и для регуляторов, которые ее аккумулируют. Поэтому, скорее всего, субъект десять раз подумает, передавать информацию или нет, а если передавать, то по каким инцидентам. А регулятор, в свою очередь, не будет настаивать на 100%-ной передаче информации (тем более что проконтролировать ее достоверность он, скорее всего, не сможет).

АЛЕКСЕЙ МАЛЬНЕВ

Ни предприятия, ни регуляторы к такой практике пока не готовы. Тут есть проблемы организационного и технического характера.

Во-первых, предполагается, что единая государственная система обнаружения, предупреждения и

ликвидации последствий компьютерных атак станет ключевым элементом регулирования и оценки состояния информационной безопасности на объектах критической инфраструктуры. Технически это вполне реализуемо. Но надо понимать, что задача примет поистине глобальный характер. Более того, для полноценной работы указанной системы нужно на каждом объекте критической инфраструктуры внедрить эффективные организационные и технические меры информационной безопасности.

Во-вторых, следует определить механизм информирования об инцидентах. Очевидно, что регулятор не может назначить квоты по получаемым инцидентам. Необходимо, чтобы отсутствие серьезных инцидентов трактовалось как признак эффективной работы системы информационной безопасности, а не наоборот.

В-третьих, для внедрения и эксплуатации государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак понадобится внушительный штат специалистов на всех уровнях – от предприятия до отрасли и государственных регуляторов. Централизация функций мониторинга и обнаружения атак является необходимой мерой. Специалисты на местах должны быть способны принимать решения и контролировать процессы ИБ самостоятельно. Поэтому следует принимать меры для тотального повышения квалификации специалистов ИБ, причем обязательно с учетом специфики предприятий. Исходя из масштабов задачи к этому вопросу нужно подходить системно.

РУСТЭМ ХАЙРЕТДИНОВ

Действительно, информационная открытость – не самая сильная сторона российской бизнес-традиции. Но опыт других регуляторов, например Банка России, показывает, что настойчивое постепенное внедрение регулятором отчетности по инцидентам с непрерывным разъяснением пользы такой отчетности для самих предприятий дает положительный результат.

В рассматриваемом документе нет прямых указаний на возможные меры наказания и ответственность субъекта, владеющего КВО, есть лишь отсылки к прочим нормам и законам. Насколько, на ваш взгляд, это скажется на его исполнении?

ДМИТРИЙ БУЗЫКИН

Вопросы уголовного и уголовно-процессуального права, равно как и исполнения уголовного или административного наказания, не являются предметом правового регулирования законопроекта. Хотя, например, тема введения специализированных общественно полезных работ как возможной меры наказания за правонарушения и преступления в рассматриваемой сфере выглядит спекулятивно привлекательно (категоризированная ИТ-шарашка поколения Next).

СЕРГЕЙ ВИХОРЕВ

А в Правилах дорожного движения разве прописаны меры наказания? И разве от этого наказания за их нарушения стали менее жесткими? Форма и мера наказания определяются КоАП РФ, ГК РФ, УК РФ. Если существующих мер недостаточно, то надо вносить изменения и дополнения в кодексы, а не прописывать их в каждом специальном законе. Это, кстати, исключит волюнтаризм и самодурство при определении степени вины и выборе наказания. И конечно, надо нарабатывать судебную практику. Право и правоприменение у нас в стране, к сожалению, не всегда одно и то же.

СЕРГЕЙ ГАРБУК

До настоящего времени адекватная ответственность должностных лиц в основном предусматривалась лишь в тех случаях, когда невыполнение требований закона уже привело к негативным последствиям. Однако все чаще тяжесть наказания устанавливается соразмерно тяжести потенциальных последствий. Следует ожидать, что эффективность исполнения разработанного закона будет зависеть и от этого правоприменительного тренда.

АЛЕКСЕЙ КОСИХИН

Пока не будет прописана серьезная ответственность субъектов, многие из них будут подходить к исполнению требований закона формально. Необходима, как минимум, более серьезная система штрафов, возрастающих при повторении инцидентов. Матрицу таких штрафов можно привязать, например, к величине ущерба, понесенного по каждому из критериев. Надеюсь, в подзаконных актах этому будет уделено самое пристальное внимание.

АЛЕКСЕЙ МАЛЬНЕВ

Практика западных государств (например, США) показывает, что четкая политика штрафных санкций, которая однозначно определяет прямые финансовые потери предприятия в результате несоблюдения правил, оказывает большое влияние на решения, принимаемые руководством предприятий. Для энергетических компаний в США существует четкая матрица штрафов за несоблюдение тех или иных пунктов национального стандарта безопасности NERC. Причем значения штрафов пропорциональны размеру предприятия. В результате штрафные санкции становятся одними из лучших мотивирующих факторов для соблюдения отраслевых стандартов ИБ на предприятиях.

СТАНИСЛАВ ШЕВЧЕНКО

Прежде чем переходить к мерам наказания и ответственности, нужно определить, что считать предосудительными действиями, заслуживающими наказания. Имеет смысл предусмотреть не только умышленное вмешательство в систему, но и ошибки, которые могут возникать в связи со сложностью самой системы и процессов ее эксплуатации. ■