КЛАСТЕР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
cs.raec.ru

Заключение на законопроект, разработанный Федеральной службой безопасности Российской Федерации «О безопасности критической информационной инфраструктуры Российской Федерации»[1]

Проект ФЗ «О безопасности критической информационной инфраструктуры РФ» содержит положения и подходы к обеспечению безопасности, в целом соответствующие положениям и задачам Доктрины информационной безопасности РФ от 06.12.2016[2], Основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ от 2012 г.[3], Указа Президента РФ 31с от 15.01.2013 г. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[4]. Актуальная версия законопроекта также учитывает и развивает положения Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утверждена Президентом РФ 12.12.2014, № К 1274[5].

Законопроект обеспечивает преемственность и последовательность развития государственной политики в сфере регулирования и защиты АСУ ТП и КИИ. Законопроект также предлагает комплексную модель разграничения полномочий и ведомственных компетенций в области обеспечения безопасности КИИ между ФСБ РФ (в качестве ФОИВ, уполномоченного в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ и обеспечения ее функционирования) и ФСТЭК РФ (в качестве ФОИВ, уполномоченного в области обеспечения безопасности КИИ РФ). Такая модель позволяет минимизировать риск дублирования компетенций, конфликта интересов

[1] (ID 00/04-5890/08-13/20-13-4, адрес: http://regulation.gov.ru/projects#npa=5971), внесён в Государственную Думу ФС РФ, http://asozd2.duma.gov.ru/addwork/scans.nsf/ID/EBE024490F4C5851432580810054D3AC/$File/47571-7_06122016_47571-7.PDF?OpenElement (последнее посещение 29.01.2017).

[2] Доктрина информационной безопасности Российской Федерации, Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646, Российская газета, https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (последнее посещение 29.01.2017).

[3] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803), Совет Безопасности Российской Федерации, http://www.scrf.gov.ru/documents/6/113.html (последнее посещение 29.01.2017).

[4] Указ Президента Российской Федерации от 15 января 2013 г. N 31с г. Москва «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Выписка), Российская Газета, 18 января 2013 г., https://rg.ru/2013/01/18/komp-ataki-site-dok.html (последнее посещение 29.01.2017).

[5] Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Концепция утверждена Президентом РФ 12.12.2014, № К 1274), ФСБ РФ, http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf (последнее посещение 29.01.2017).

между теми или иными уполномоченными ФОИВ, а также появления функций и объектов КИИ, выпадающих из сферы компетенций и ответственности уполномоченных ФОИВ.

Законопроект вводит внутренне непротиворечивую систему понятий и определений, позволяя уточнить накопившиеся с середины 2000-х гг. терминологические противоречия (в том числе в отношении терминов КИИ, КВО, КСИИ), и таким образом способствует уточнению предмета деятельности и функций государственных ведомств в сфере защиты критической инфраструктуры. Кроме того, законопроект предлагает системный и унифицированный методологический аппарат для определения объектов, идентификации задач и определения приоритетов в области обеспечения безопасности КИИ, включая:

- Систему категорирования объектов КИИ по ряду критериев (значимость для национальной безопасности и обороноспособности, социальная, политическая, экономическая и экологическая значимость).
- Классификацию объектов КИИ по классам значимости/опасности (с вытекающим из него разведением функций ФСБ и ФСТЭК в зависимости от класса объекта КИИ).
- Систему функций государственных регуляторов, требований к защите объектов КИИ, прав и обязанностей субъектов КИИ, мер государственного контроля обеспечения безопасности значимых объектов КИИ и проч.

Законопроект не ограничивается каким-либо отдельным сектором или отраслью КИИ и обеспечивает организационно-нормативную основу государственной политики в области защиты информационной инфраструктуры по всем отраслям и секторам, включая отрасль связи. Подобный подход необходим для обеспечения внутренней непротиворечивости государственной политики и предотвращения риска развития разнонаправленных моделей регулирования на отраслевом уровне и нарушения межведомственного взаимодействия в данной сфере. Межотраслевой охват законопроекта принципиально важен, поскольку российская инфраструктура электросвязи обеспечивает функционирование КИИ в большинстве отраслей и секторов экономики и потому не может рассматриваться в качестве объекта регулирования по отдельности, вне связи с остальными секторами и отраслями.

Вместе с тем, законопроект учитывает особенности обеспечения безопасности КИИ применительно к сектору связи и, в частности, сетям связи общего пользования. Это позволяет снизить риск избыточных административных и финансово-материальных издержек операторов связи сетей общего пользования в связи с исполнением обязанностей и требований к субъектам КИИ, обеспечивающим взаимодействие объектов КИИ между собой. В этой связи важной задачей в рамках внесения изменений в НПА Президента РФ, Правительства РФ и ФОИВ в связи с проектом рассматриваемого ФЗ представляется доработка разработанного Минкомсвязи РФ проекта изменений в ФЗ «О связи» [6] с целью приведения его в соответствие с принципами и методологией регулирования, изложенных в рассматриваемом законопроекте, в том числе в части терминологии и критериев для системы категорирования объектов КИИ.

[6] Федеральный закон «О внесении изменений в Федеральный закон «О связи» (Проект), 01/05/11-16/00058851, Федеральный портал проектов нормативных правовых актов, http://regulation.gov.ru/projects#npa=58851 (последнее посещение 29.01.2017).

Законопроект также отвечает ряду принципов и практик, изложенных в рекомендациях международных организаций, в том числе Рекомендациях Совета ОЭСР по защите КИИ от 2008 г.[7] – в том числе, в части:

- выработки определения критических информационных инфраструктур;
- определения четких целей политики по обеспечению безопасности КИИ на высшем уровне, определения круга ответственных за ее реализацию регуляторов и иных структур;
- принятия мер по повышению уровня безопасности компонентов информационных систем и сетей, из которых состоят объекты КИИ.

Законопроект отвечает рекомендательным мерам доверия, сформулированным в пунктах 15-16 Решения № 1202 «Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования ИКТ» от 10 марта 2016 г.[8] Так, предлагаемые в рамках законопроекта нормы могут способствовать поощрению и облегчению регионального и субрегионального взаимодействия между законно уполномоченными органами власти, отвечающими за безопасность критически важной инфраструктуры, включая обмен информацией об угрозах, связанных с КИИ; разработку мер реагирования на вызовы, включая процедуры регулирования кризиса в случае широкомасштабного или транснационального сбоя в функционировании КИИ; повышение безопасности национальной и транснациональной КИИ, включая обеспечение ее целостности на региональном и субрегиональном уровнях; повышение осведомленности о важности защиты систем управления производственными процессами и о проблемах, касающихся их безопасности, связанной с ИКТ, а также о необходимости разработки процессов и механизмов реагирования на эти проблемы.

Отдельные положения законопроекта демонстрируют близость принципам и передовым практикам регулирования КИИ в ряде зарубежных государств – например, в части формулировки критерия социальной значимости объекта КИИ, включающей доступ к государственной услуге определенного количества ее получателей (интерпретация критической значимости через функцию оказания услуг гражданам). Приведенный в законопроекте перечень секторов экономики, управления и отраслей промышленности, в которых функционируют объекты КИИ, в целом соответствует международному опыту и передовым практикам развитых государств и интеграционных объединений.

Соответствие международным практикам и рекомендациям представляется существенным условием для обеспечения эффективности государственной политики в области обеспечения безопасности КИИ с учетом необходимости международного сотрудничества и иных трансграничных взаимодействий.

Отдельные положения законопроекта представляются требующими доработки с учетом экспертных отзывов, либо разъяснений со стороны инициаторов и разработчиков законопроекта. На этапе рассмотрения и обсуждения законопроекта в Госдуме РФ актуальна гармонизация ключевых понятий (в частности, КИИ РФ, АСУ ТП, ГосСОПКА) с нормативными и доктринальными документами, принятыми Советом Безопасности РФ, ФСТЭК РФ, президентом РФ и проч. в 2012-2016 гг., в том числе приравнивание понятия

[7] OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures, https://www.oecd.org/sti/40825404.pdf (последнее посещение 29.01.2017).

[8] Решение № 1202 меры укрепления доверия в рамках обсе с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий в решении № 1039 Постоянного совета (26 апреля 2012 года), Организация по безопасности и сотрудничеству в Европе 10 March 2016, PC.DEC/1202, http://www.osce.org/ru/pc/228521?download=true (последнее посещение 29.01.2017).

КИИ к понятию «ключевые системы информационной инфраструктуры (КСИИ) РФ» с целью обеспечения преемственности наработок ФСТЭК в области категорирования и ведения реестра объектов КИИ. Актуальна может быть доработка перечня секторов и отраслей, в которых функционируют КИИ РФ, в частности включение в них сектора водоснабжения и гидротехнической промышленности, а также пищевой промышленности.

Для того, чтобы избежать избыточной регуляторной нагрузки на организации финансово-кредитного сектора РФ по аналогии с имеющейся в проекте ФЗ нормой по особенностям его применения к сетям связи общего пользования возможно введение подобной нормы для финансово-кредитного сектора, который уже охвачен системой ФЗ и иных НПА, в том числе документами Центрального Банка РФ.

Отдельные нормы законопроекта могут требовать соотнесения с антитеррористическим законодательством РФ (в части разведения понятий ««оценка состояния защищенности от компьютерных атак» и «оценка антитеррористической защищенности»), а также комплексной гармонизации с отраслевыми нормами федерального законодательства РФ в области безопасности, включая следующие отрасли:

- Промышленная безопасность, в том числе промышленная безопасность опасных производственных объектов
- Гидротехнические сооружения, а также промышленные объекты повышенной опасности.
- Транспортная безопасность, включая безопасность воздушного, водного, железнодорожного и автомобильного транспорта.
- Безопасность объектов ТЭК.
- Безопасность объектов атомной энергетики.

Отдельные положения законопроекта также могут требовать уточнения в части требований к персоналу, допущенному к работе на значимых объектах КИИ, закрепления роли субъектов КИИ в определении угроз своим объектам и формировании частных моделей таких угроз, уточнения возможностей субъектов КИИ в части доступа к механизмам обмена информацией о компьютерных инцидентах за рамками НКЦКИ (в том числе неправительственным, частным и международным группам реагирования на компьютерные инциденты (CSIRT/CERT)). Также может быть востребован пересмотр норм, относящих к сведениям, составляющим государственную тайну, информацию о мерах, принимаемых для обеспечения безопасности значимых объектов КИИ РФ средней и высокой категорий опасности и об оценке степени защищенности КИИ РФ.

Несмотря на это, принятие законопроекта представляется положительным и давно востребованным решением, отражающим потребности государства и общества в области обеспечения безопасности КИИ в ключевых секторах национальной экономики и государственной деятельности в условиях стабильного роста количества и масштаба компьютерных инцидентов, связанных с целенаправленными компьютерными атаками на объекты информационной инфраструктуры РФ, включая объекты КИИ.