Особенности режима безопасности критической информационной инфраструктуры РФ

26 июля 2017 года Президентом Российской Федерации подписана серия Федеральных законов, касающихся обеспечения безопасности критической информационной инфраструктуры Российской Федерации, включая следующие законы:
1) Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – 187-ФЗ) – закон, регулирующий отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак;
2) Федеральный закон от 26 июля 2017 г. № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – 193-ФЗ) – закон, вносящий изменения в Федеральный закон от 21 июля 1993 года № 5485-1 «О государственной тайне» (сведения о мерах по обеспечению безопасности критической информационной инфраструктуры (далее – КИИ) добавляются в перечень сведений, составляющих государственную тайну), Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» (необходимость обеспечения установленного 187-ФЗ порядка, технических условий установки и эксплуатации средств, предназначенных для поиска компьютерных атак в сетях электросвязи) и Федеральный закон от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля (исключение государственного контроля в области обеспечения безопасности КИИ из-под действия 294-ФЗ);
3) Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – 194-ФЗ) – закон, добавляющий в УК РФ отдельную статью № 274 «Неправомерное воздействие на критическую информационную инфраструктуру» и устанавливающий ответственность за данное деяние.

Следует отметить ряд важных особенностей, присущих законодательству РФ в области безопасности КИИ в его текущем воплощении.

Во-первых, законодательство на текущий момент недостаточно для полноценного выполнения обязанностей, возложенных на субъектов КИИ, в силу отсутствия ряда ключевых подзаконных актов и указов Президента РФ.

Так, на данный момент не назначен орган, уполномоченный в области безопасности КИИ. Такой орган предстоит назначить Президенту РФ. Готовится проект указа Президента РФ «О федеральном органе исполнительной власти, уполномоченном в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации». Этот орган будет определять ключевые особенности классификации и построения систем защиты для объектов КИИ. С учетом специализации федеральных органов исполнительной власти России и по предположению ряда профильных экспертов, таким органом может стать ФСТЭК России или ФСБ России. В случае, если Президентом в качестве органа, уполномоченного в области безопасности КИИ, будет утвержден ФСТЭК России, следует ожидать преемственности формируемых данным органом требований на основе ранее выпущенного этим органом Приказа ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» и комплекта документов о защите ключевых систем информационной инфраструктуры Российской Федерации. В случае, если уполномоченным в области безопасности КИИ будет назначена ФСБ России, возможно, предстоит существенный пересмотр защитных механизмов КИИ по сравнению с Приказом №31. Однако при этом следует ожидать более гармоничной интеграции с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Кроме того, сложившийся на данный момент понятийный аппарат содержит в себе ряд нестыковок и противоречий. Например, 187-ФЗ и Стратегии развития информационного общества Российской Федерации на 2017 – 2030 годы (утв. Указом Президента РФ от 09 мая 2017 г. № 203) по-разному вводят само понятие «Критическая информационная инфраструктура», в чем читатель может убедиться самостоятельно. Однако и в том, и в другом случае КИИ определяется не через степень возможных негативных последствий от нарушения функционирования соответствующих объектов, а через принадлежность фиксированному набору отраслей экономики, полнота которого неочевидна.

Во-вторых, в качестве области действия задан перечень отраслей экономики, в которых используемые информационные технологии для автоматизации бизнес-процессов существенно различаются. Так, для компаний финансовой сферы и для производственных предприятий актуальны совершенно разные подходы и требования по обеспечению информационной безопасности. Существенно различаться будет и методика оценки воздействия рисков информационной безопасности для объектов КИИ из разных отраслей экономики. Мировой опыт (в том числе, опыт Соединенных Штатов Америки) говорит о целесообразности специализации требований по отраслям экономики, тем самым обеспечив максимальную вовлеченность соответствующих министерств и органов исполнительной власти, определяющих развитие данной отрасли в масштабах страны.

Обеспечение вовлеченности профильных экспертов при формировании конкретных мероприятий и требований по обеспечению безопасности КИИ является хорошей практикой, которая, хочется верить, позволит сформировать мероприятия и требования по обеспечению безопасности КИИ в максимально эффективном, управляемом и исполнимом виде применительно к каждой отрасли, в рамках которой функционируют КИИ.

В-третьих, 193-ФЗ добавляет в перечень сведений, составляющих государственную тайну, любые сведения о мерах защиты объектов КИИ. С учетом этого рынок услуг в области обеспечения безопасности КИИ может стать весьма специфическим.

Объекты КИИ должны быть устойчивы как к целенаправленным атакам, так и к опасным последствиям непреднамеренных и неквалифицированных действий персонала, включая действия, предпринимаемые персоналом в нарушение действующих политик. Кроме того, должна быть предусмотрена устойчивость к угрозам природного и техногенного характера.

С учетом сложности объектов КИИ задача обеспечения их безопасности всегда находится на стыке дисциплин, связанных с безопасностью, включая, как минимум, следующие: информационная безопасность, технологическая и промышленная безопасность, пожарная безопасность, социальная безопасность и так далее. Эффективная система обеспечения безопасности объекта КИИ должна строиться с учётом факторов, характерных для всех этих дисциплин.

В связи с проникновением цифровых технологий практически на все уровни технологических процессов и унификацией технологий и протоколов взаимодействия, обеспечение безопасности объектов КИИ требует комплексного подхода. Процессы реагирования на инциденты, связанные с безопасностью, как и процессы обеспечения непрерывности бизнеса и восстановления после аварий, должны быть сквозными и включать информационную, промышленную и технологическую, пожарную, социальную и иные сферы безопасности.

Вышеперечисленные особенности серии законов, направленных на обеспечение безопасности критической информационной инфраструктуры Российской Федерации, подписанных Президентом Российской Федерации 26 июля 2017 г., рекомендуется учитывать при выполнении мероприятий владельцами информационных систем.

безопасность критической информационной инфраструктуры, аналитика