В федеральном законодательстве создаётся организационно-правовая основа для обеспечения безопасности критической информационной инфраструктуры

27 января 2017 года пакет из трёх законопроектов о безопасности критической информационной инфраструктуры был принят Государственной Думы РФ в первом чтении. Основной законопроект – о безопасности критической информационной инфраструктуры. Ещё два посвящены внесению соответствующих изменений в ряд законодательных актов Российской Федерации, в Уголовный и Уголовно-процессуальный кодексы РФ. Пакет законопроектов был внесён Правительством России 16 декабря 2016 года и рассмотрен Государственной Думой РФ в кратчайшие сроки.

НОВЫЕ УГРОЗЫ НАШЕЙ БЕЗОПАСНОСТИ

Предварительно внесённые Правительством России законопроекты были проработаны и поддержаны профильными комитетами Государственной Думы РФ:

- по информационной политике, информационным технологиям и связи;
- по безопасности и противодействию коррупции;
- по государственному строительству и законодательству;
- по экономической политике, промышленности, инновационному развитию и предпринимательству.

После этого пакет законопроектов об обеспечении безопасности критической информационной инфраструктуры был вынесен на рассмотрение пленарного заседания.

Проблема защиты информации, информационных ресурсов имеет богатую историю. 21 июля 1993 года был принят закон РФ № 5485-I «О государственной тайне», в который потом вносились изменения. Одним из первых федеральных законов в этой сфере, принятых после вступления в силу ныне действующей Конституции России 1993 года, был Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Затем был принят ФЗ-152 от 27 июля 2006 года «О персональных данных» и ряд других отраслевых федеральных законов.

Почему в настоящее время возникла необходимость принятия федерального закона об обеспечении безопасности критической информационной инфраструктуры в России? В последние годы информационные технологии начали массово применяться практически во всех сферах жизни и масштабно расширились на трансграничное пространство. Если в 2011 году было выявлено 4,5 млн компьютерных атак на объекты критической информационной инфраструктуры, то в прошлом, 2016 году их количество возросло до 70 млн. Поэтому проблема зашиты информации вышла на качественно новый уровень.

За последние годы ущерб от вредоносных программ, исходя из различных методик оценки ущерба, составлял от $ 300 млрд до $ 1 трлн, то есть от 0,4% до 1,4% общемирового ежегодного ВВП ? валового внутреннего продукта. Эти показатели имеют тенденцию к неуклонному росту. Информационные технологии используются и для достижения недружественных нашей стране геополитических целей, и террористами, и прочим

криминалитетом.

Компьютерные атаки могут повлечь за собой нарушение важнейших технологических процессов, включая те, что обеспечивают государственную деятельность. Компьютерные атаки могут полностью парализовать критическую информационную инфраструктуру государства, спровоцировать политическую, социальную, финансовую и экологическую катастрофу. Примерами последствий таких воздействий могут послужить остановка центрифуг иранской атомной станции с помощью компьютерного вируса StuxNet в сентябре 2010 года, а также и паралич работы нескольких крупных финансовых учреждений Южной Кореи в марте 2013 года.

Стабильность социально-экономического развития и безопасность нашей страны находятся в прямой зависимости от надежности и безопасности функционирования информационно-телекоммуникационных сетей и информационных систем. Работа по обеспечению безопасности критически важной инфраструктуры велась и раньше. Обеспечение их безопасности регламентируется и другими законами: их физическая защита, в случаях чрезвычайных ситуаций, военных, вооружённых и террористических нападений… Велась работа и по обеспечению информационной безопасности критической информационной инфраструктуры Российской Федерации.

Ярким примером является создание в 2013–2016 годах Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГОССОПКА). Создание этой системы ранее регламентировалось подзаконными актами – Указами Президента России, Постановлениями Правительства РФ и ведомственными нормативными документами, включая Приказы ФСБ России.

СИСТЕМАТИЗИРУЮЩИЙ ЗАКОНОПРОЕКТ

Однако эффективное правовое регулирование в данной сфере было затруднено из-за отсутствия системообразующих законодательных актов, устанавливающих порядок отношений в сфере обеспечения безопасности критической информационной инфраструктуры в Российской Федерации. Пришла пора обосновать, с учётом зарубежной практики и отечественного опыта, безопасность критической информационной инфраструктуры в России на уровне федерального законодательства.

Пакет законопроектов о безопасности критической информационной инфраструктуры Российской Федерации формирует полноценную правовую основу для развития и функционирования Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Определено, что относится к критической информационной инфраструктуре: информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами в 13 сферах. К ним относятся государственное управление, энергетика, транспорт, связь, кредитно-финансовая сфера, здравоохранение и ряд отраслей промышленности. А именно оборонная, топливная, атомная, ракетно-космическая, горнодобывающая, металлургическая и химическая.

Устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры. Чётко регламентируются полномочия различных органов государственной власти, в том числе различных ведомств и других субъектов отрасли, включая операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

Выстроен порядок их взаимодействия для защиты информационных сетей от компьютерных атак. Вводятся категорирование объектов критической информационной инфраструктуры, порядок их классификации, различия степени защищённости. Оценку степени защищённости смогут проводить организации, аккредитованные уполномоченными государственными органами.

Принятие основного федерального закона – «О безопасности критической информационной инфраструктуры Российской Федерации» требует внесения изменений в ряд действующих законодательных актов. Прежде всего, в Закон РФ № 5485-I «О государственной тайне» ? об отнесении ресурсов обеспечения защиты критической информационной инфраструктуры к категории государственной тайны. В Федеральный закон от 07 июля 2003 года №126-ФЗ «О связи» ? об обязанности операторов телекоммуникаций выполнять требования к технологической оснащённости и обеспечивать сохранность технических средств, задействованных в защите объектов критической информационной инфраструктуры.

Кроме того, вносится норма о защите прав юридических лиц и индивидуальных предпринимателей при проведении профильных контрольно-надзорных мероприятий. Что обусловлено тем, что в основном законопроекте подробно прописаны меры государственного контроля: основания и процедуры проведения проверок, действия по их результатам. Эти правоотношения в отрасли будут регулироваться не Федеральным законом от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», а законом о безопасности критической информационной инфраструктуры.

ОТВЕТСТВЕННОСТЬ СОРАЗМЕРНА ОПАСНОСТИ

Комплекс принимаемых законопроектов вносит изменения и в Уголовный Кодекс РФ. В действующем законодательстве была установлена ответственность за три состава преступлений в сфере компьютерной информации: статьями 272, 273 и 274. Это, во-первых, неправомерный доступ к компьютерной информации, повлекший её изменение, уничтожение или блокирование; во-вторых, производство и распространение вредоносного программного обеспечения; и, в-третьих, нарушение правил эксплуатации компьютеров и компьютерных сетей.

К этим статьям будет добавлена новая, 274-1, конкретизация компьютерных преступлений применительно к объектам критической информационной инфраструктуры, с повышенной ответственностью. Предлагается выделить составы посягательств на критическую информационную инфраструктуру Российской Федерации в отдельную статью Уголовного кодекса ? «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Ответственность предусматривается:

- за создание, распространение компьютерных программ, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру России;
- за неправомерный доступ к охраняемой законом компьютерной информации в критической информационной инфраструктуре;
- за нарушение правил эксплуатации в ней средств хранения, обработки или передачи охраняемой компьютерной информации.

Учитывая высокую общественную опасность таких деяний, санкции за них будут предусматривать, с учётом различных квалифицирующих признаков, наказания в виде штрафа, принудительных работ, лишения свободы на срок до 10 лет, с лишением права занимать определённые должности или заниматься определённой деятельностью. Кроме того, прописываются возможности использования Кодекса административных правонарушений РФ, в котором есть 33 состава проступков в компьютерной сфере. Также применение гражданской ответственности при нанесении ущерба компьютерными атаками.

Общественное обсуждение этих вопросов проводилось на самых разнообразных площадках, в частности, на Национальном форуме информационной безопасности «Инфофорум – 2017», проходившем 2?3 февраля 2017 года. Вопросы защиты объектов критической информационной инфраструктуры в финансовой сфере рассматривались на IX Уральском форуме «Информационная безопасность финансовой сферы», проведённого 13–17 февраля этого года. Разработчиками законопроекта учтены более 300 замечаний, поступивших от представителей более 60 регионов страны.

Можно достаточно уверенно прогнозировать социальные, экономические, экологические, политические – внешние и внутренние, а также иные негативные последствия, которые могут наступить в результате атак на те или иные объекты критической информационной инфраструктуры. Исходя из такого прогнозирования, на основе принятого пакета законопроектов Правительство России своими нормативными документами может определять требования по обеспечению её безопасности к каждой из сфер, отраслей.

Элементы критической информационной инфраструктуры включаются в государственный реестр значимых объектов, им на основании определённых критериев может присваиваться одна из трёх категорий значимости ? высокая, средняя или низкая. Присвоенным категориям должна соответствовать степень защищённости, которую должны обеспечивать собственники, владельцы, управляющие этими объектами. Что такое системы безопасности объектов критической информационной инфраструктуры, какими они должны быть, ? в законопроекте прописано подробно.

ФАКТОР МЕЖДУНАРОДНОЙ ОБСТАНОВКИ

Что касается технического обеспечения, то, по оценкам экспертов, наша страна способна самостоятельно обеспечить выполнение принимаемых законопроектов, и аппаратное, и программное. Дело в том, чтобы этими техническими средствами оснастить все требующие защиты объекты критической информационной инфраструктуры. Согласно финансово-экономическому обоснованию, сопровождающему законопроект, дополнительных финансовых затрат из государственного бюджета, федерального и региональных, его реализация не требует. Потому что создание ГОССОПКА было начато четыре года назад.

Сейчас ГОССОПКА работает как централизованная территориально распределённая система, полноценно обеспечивает защиту объектов критической информационной инфраструктуры. Принимаемый законопроект просто развивает регламентацию её работы, переносит её с подзаконных нормативных актов на новый правовой уровень – федерального

законодательства.

Затраты на организационно-техническое обеспечение реализации законопроекта и их источники уже были определены ранее. Как из государственного бюджета, так и негосударственных собственников объектов критической информационной инфраструктуры. Обеспечение безопасности, конечно, требует затрат, но такие расходы необходимы. Существенного их возрастания в связи с принятием законопроектов, о которых идёт речь, ожидать не приходится.

Разработчики законопроектов учитывали зарубежный опыт и практику противодействия информационным атакам на объекты критической инфраструктуры. Были учтены все международные обязательства Российской Федерации в этой области. Подытожен опыт правового регулирования безопасности критической информационной инфраструктуры стран с развитой информационной инфраструктурой, таких как Германия, США, Великобритания, Япония и Южная Корея.

Даже то, что в последнее время в некоторых странах чаще стали использоваться политические спекуляции вокруг компьютерных атак, не препятствует международному взаимодействию для противодействия киберпреступности. В ряде сфер, взять хотя бы атомную промышленность, компьютерные атаки могут нанести огромный международный ущерб. Поэтому выполняются, на паритетных началах, существующие договорные отношения о привлечении к уголовной ответственности тех виновных в компьютерных преступлениях, кто находится за рубежом.

Следует отметить, что компьютерные атаки иностранных государственных структур, совершаемые, например, в разведывательных целях, не подпадают под российское уголовное законодательство, которое распространяется на физические, а не на юридические лица. Проблемы со странами, изобличёнными в подобных действиях, должны решаться политическими способами.

Принятие пакета законопроектов создаст организационно-правовую основу для эффективной работы системы безопасности критической информационной инфраструктуры Российской Федерации. В первую очередь для предупреждения компьютерных инцидентов, а также для существенного снижения общественно-политических, финансовых и иных негативных последствий компьютерных атак.