Babr24.com

Автор: Виктория Федосеенко © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 10662
29.01.2017, 16:42 10

Закон о критической информационной инфраструктуре. Главное

27 января 2017 года Госдума приняла в первом чтении пакет правительственных законопроектов, которые касаются критической информационной инфраструктуры РФ. Пакет вводит уголовное наказание за киберпреступления, предполагает создание госсистемы предупреждения и ликвидации кибератак, а также реестра объектов критической информационной инфраструктуры. SmartBabr выбрал главное из многостраничного документа.

Законопроект был внесен в Госдуму 6 декабря 2016 года комитетом по информационной политике, информационным технологиям и связи. Все документы опубликованы на сайте федерального собрания. В пояснительной записке к законопроекту сказано:

> «Стабильность социально-экономического развития Российской Федерации и ее безопасность, по сути, поставлены в прямую зависимость от надежности и безопасности функционирования информационно-телекоммуникационных сетей и информационных систем (...). Принятие законопроекта позволит создать правовую и организационную основу для эффективного функционирования системы безопасности (...) а также существенно снизит общественно-политические, финансовые и иные негативные последствия для Российской Федерации в случае проведения против нее компьютерных атак».

Законопроект вводит несколько новых понятий. Среди них:

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ – «единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак».

Компьютерная атака – «целенаправленное воздействие программными средствами на информационные системы, информационно-телекоммуникационные сети, средства связи и автоматизированные системы управления технологическими процессами, осуществляемое в целях нарушения их функционирования и (или) нарушения безопасности обрабатываемой ими информации»;

Критическая информационная инфраструктура РФ – «совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической инфраструктуры между собой».

Объекты критической информационной инфраструктуры – «информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированые системы управления технологическими процессами, функционирующие *в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности и химической промышленности*».

Согласно законопроекту, на значимых объектах критической информационной инфраструктуры и в сетях электросвязи должны быть установлены технические средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Категории значимости

Всем объектам критической информационной инфраструктуры будет присвоена категория значимости – высокая, средняя или низкая.

Категории будут присваиваться исходя из социальной значимости (ущерб здоровью людей, влияние на работу объектов жизнеобеспечения, транспортной инфраструктуры и т.д.), а также исходя из политической, экономической и экологической значимости. Критерии устанавливаются Правительством Российской Федерации.

Для каждой категории федеральный орган должен установить требования по обеспечению безопасности.

Реестр критической информационной инфраструктуры

Закон также предполагает создание реестра критической информационной инфраструктуры, куда, в частности, будут вноситься сведения о программном обеспечении объекта, мерах и средствах, применяемых для обеспечения его безопасности.

Субъекты этого реестра, должны, помимо прочего, обеспечивать «беспрепятственный доступ должностных лиц федерального органа исполнительной власти (...) к значимому объекту критической информационной инфраструктуры».

Ответственность за нарушение безопасности информационных систем

Законопроект вводит уголовную, административную, гражданско-правовую и дисциплинарную ответственность за нарушение законодательства в области безопасности критической информационной инфраструктуры.

За создание программ для атак на объекты информационной инфраструктуры– штраф от пятисот тысяч до миллиона рублей либо принудительные работы или лишение свободы на срок до пяти лет;

За неправомерный доступ к охраняемой информации (с причинением вреда инфраструктуре)– штраф от одного до двух миллионов рублей или лишение свободы на срок до шести лет со штрафом от пятисот тысяч до одного миллиона рублей.

За нарушение правил эксплуатации технических средств критических систем– принудительные работы на срок до пяти лет с лишением права занимать определенные должности на срок до трех лет, либо лишение свободы на срок до шести лет.

Если совершение всех правонарушений повлекло тяжелые последствия или «создало угрозу их наступления» – оно наказывается лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности на срок до пяти лет.

Согласно проекту, закон должен был вступить в силу 1 января 2017 года. Отдельные статьи закона – 1 января 2018 года. Новые сроки вступления закона в силу пока неизвестны.

На фото: центральный пульт управления Иркутской ГЭС – одним из критически важных объектов города. Понятие критический объект было определено в законодательстве РФ в 1994 году

Автор: Виктория Федосеенко
© SmartBabr

Порекомендовать текст

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:
- *Телеграм*
- *ВКонтакте*

Связаться с редакцией Бабра:
newsbabr@gmail.com

Автор текста: **Виктория Федосеенко**, журналист.

На сайте опубликовано **1158** текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта