ПРАВИТЕЛЬСТВО
РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственная Дума
Федерального Собрания
Российской Федерации

«06» декабря 2016 г.

№ 9198п-П10

МОСКВА

О внесении проектов федеральных законов "О безопасности критической информационной инфраструктуры Российской Федерации", "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" и "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

В соответствии со статьей 104 Конституции Российской Федерации Правительство Российской Федерации вносит на рассмотрение Государственной Думы Федерального Собрания Российской Федерации проекты федеральных законов "О безопасности критической информационной инфраструктуры Российской Федерации", "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" и "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

Приложение: 1. Текст законопроекта "О безопасности критической информационной инфраструктуры Российской Федерации" на 36 л.
2. Пояснительная записка к проекту федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" на 4 л.

25092341.doc

3. Финансово-экономическое обоснование к проекту федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" на 1 л.
4. Перечень федеральных законов, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", на 3 л.
5. Перечень нормативных правовых актов Президента Российской Федерации, Правительства Российской Федерации и федеральных органов исполнительной власти, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", на 12 л.
6. Текст законопроекта "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" на 3 л.
7. Пояснительная записка к проекту федерального закона "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" на 2 л.
8. Финансово-экономическое обоснование к проекту федерального закона "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" на 1 л.
9. Перечень федеральных законов, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", на 1 л.
10. Перечень нормативных правовых актов Президента Российской Федерации, Правительства Российской

Федерации и федеральных органов исполнительной власти, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", на 1 л.

11. Текст законопроекта "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" на 5 л.
12. Пояснительная записка к проекту федерального закона "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" на 3 л.
13. Финансово-экономическое обоснование к проекту федерального закона "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" на 1 л.
14. Перечень федеральных законов, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", на 1 л.
15. Официальный отзыв Верховного Суда Российской Федерации от 15.05.2015 № 3-ВС-2996/15 (вх. от 21.05.2015 № 2-55470) на 2 л.
16. Перечень нормативных правовых актов Президента Российской Федерации, Правительства Российской Федерации и федеральных органов исполнительной

власти, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", на 1 л.

17. Распоряжение Правительства Российской Федерации по данному вопросу на 1 л.

Председатель Правительства
Российской Федерации Д.Медведев

Вносится Правительством
Российской Федерации

Проект

47577-7

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон устанавливает организационные и правовые основы обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак, основные принципы государственного регулирования в указанной сфере, определяет полномочия органов государственной власти Российской Федерации.

Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

автоматизированная система управления технологическими процессами - комплекс аппаратных и программных средств,

предназначенных для контроля и управления технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными таким технологическим и (или) производственным оборудованием технологическими и (или) производственными процессами;

безопасность критической информационной инфраструктуры Российской Федерации - состояние защищенности критической информационной инфраструктуры Российской Федерации, при котором проведение в отношении нее компьютерных атак не приведет к нарушению (прекращению) функционирования критической информационной инфраструктуры Российской Федерации и (или) значимых ее объектов;

государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак;

значимый объект критической информационной инфраструктуры - объект критической информационной инфраструктуры, которому по

итогам категорирования присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры (далее - реестр);

категорирование - установление соответствия объекта критической информационной инфраструктуры показателям критериев категорирования и их значениям, утвержденным Правительством Российской Федерации, и присвоение этому объекту одной из трех категорий значимости - высокой, средней или низкой либо неприсвоение ему ни одной из таких категорий;

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

компьютерный инцидент - факт нарушения или прекращения функционирования объекта критической информационной инфраструктуры и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе вызванный компьютерной атакой;

критическая информационная инфраструктура Российской Федерации - совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой;

обеспечение безопасности критической информационной инфраструктуры Российской Федерации - комплекс мер правового, организационного, технического и иного характера, обеспечивающих устойчивое функционирование ее объектов в условиях проведения компьютерных атак;

объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности;

силы обнаружения, предупреждения и ликвидации последствий компьютерных атак - подразделения и (или) специально выделенные сотрудники субъектов критической информационной инфраструктуры, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и федерального органа исполнительной власти, уполномоченного в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, в том числе Национального координационного центра по компьютерным инцидентам, на которые в установленном порядке возложена обязанность проводить и участвовать в мероприятиях по обнаружению, предупреждению и ликвидации последствий компьютерных атак;

средства обнаружения, предупреждения и ликвидации последствий компьютерных атак - российские технологии, а также технические, в том числе предназначенные для поиска признаков компьютерных атак в сетях электросвязи, программные, лингвистические, правовые, организационные средства, средства сбора и анализа информации, поддержки принятия управленческих решений (ситуационные центры),

предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак;

субъекты критической информационной инфраструктуры - государственные органы, юридические лица, владеющие на праве собственности или ином законном основании объектами критической информационной инфраструктуры, операторы связи, обеспечивающие взаимодействие объектов критической информационной инфраструктуры между собой.

Статья 3. **Законодательство Российской Федерации о безопасности критической информационной инфраструктуры Российской Федерации**

Законодательство Российской Федерации о безопасности критической информационной инфраструктуры Российской Федерации основывается на Конституции Российской Федерации, общепризнанных принципах и нормах международного права и состоит из настоящего Федерального закона, других федеральных законов и принимаемых в соответствии с ними иных нормативных правовых актов Российской Федерации.

Особенности применения настоящего Федерального закона к сетям связи общего пользования определяются Федеральным законом "О связи"

и принимаемыми в соответствии с ним нормативными правовыми актами Российской Федерации.

Статья 4. **Принципы обеспечения безопасности критической информационной инфраструктуры Российской Федерации**

Принципами обеспечения безопасности критической информационной инфраструктуры Российской Федерации являются:

1) законность;

2) соблюдение баланса интересов личности, общества и государства;

3) взаимная ответственность личности, общества и государства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

4) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры Российской Федерации, достигаемые в том числе за счет эффективного взаимодействия между уполномоченными федеральными органами исполнительной власти и субъектами критической информационной инфраструктуры;

5) приоритет предотвращения компьютерных инцидентов перед устранением их последствий.

Статья 5. Полномочия органов государственной власти в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. Президент Российской Федерации определяет:

1) основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

2) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

3) федеральный орган исполнительной власти, уполномоченный в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования;

4) принципы построения, задачи, порядок создания и использования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2. Правительство Российской Федерации:

1) утверждает показатели критериев категорирования и значения таких показателей, а также порядок категорирования;

2) устанавливает порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

3) устанавливает порядок подготовки и использования ресурсов единой сети электросвязи для обеспечения функционирования значимых объектов критической информационной инфраструктуры.

3. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации:

1) осуществляет научно-исследовательскую деятельность в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

2) вносит в установленном порядке предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации Президенту Российской Федерации и в Правительство Российской Федерации;

3) утверждает правила ведения реестра, в том числе его форму, и ведет реестр;

4) проводит проверку правильности категорирования;

5) устанавливает требования по обеспечению безопасности для каждой категории значимых объектов критической информационной инфраструктуры, за исключением объектов связи и информационно-телекоммуникационных сетей;

6) осуществляет во взаимодействии с уполномоченными органами государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

7) осуществляет иные предусмотренные настоящим Федеральным законом полномочия.

4. Федеральный орган исполнительной власти, уполномоченный в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования:

1) участвует в научно-исследовательской деятельности в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

2) по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, вносит в установленном порядке предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации Президенту Российской Федерации и в Правительство Российской Федерации;

3) координирует деятельность субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

4) организует и проводит оценку состояния защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

5) утверждает порядок реагирования на компьютерные инциденты и порядок ликвидации последствий компьютерных атак на значимых объектах критической информационной инфраструктуры;

6) утверждает порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной

инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными и неправительственными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты;

7) обеспечивает установку на значимых объектах критической информационной инфраструктуры и в сетях электросвязи технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

8) устанавливает требования к техническим средствам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

9) осуществляет иные предусмотренные настоящим Федеральным законом полномочия.

5. Федеральный орган исполнительной власти, уполномоченный в области связи:

1) устанавливает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения

безопасности критической информационной инфраструктуры Российской Федерации, требования по обеспечению безопасности для каждой категории значимых объектов связи и информационно-телекоммуникационных сетей;

2) утверждает по согласованию с федеральным органом исполнительной власти, уполномоченным в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, порядок и технические условия установки и эксплуатации технических средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи.

Статья 6. **Категорирование объектов критической информационной инфраструктуры**

1. Категорирование осуществляется исходя из следующих критериев:

1) социальная значимость, выражающаяся в том числе в оценке ущерба здоровью людей, возможности прекращения (нарушения) функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимального

времени недоступности государственной услуги для определенного количества получателей такой услуги;

2) политическая значимость, выражающаяся в оценке ущерба интересам Российской Федерации во внутриполитической и внешнеполитической сферах;

3) экономическая значимость, выражающаяся в оценке снижения экономических показателей, прямых и косвенных финансовых потерь Российской Федерации;

4) экологическая значимость, выражающаяся в оценке вреда, причиняемого окружающей среде;

5) значимость для обеспечения обороноспособности, безопасности государства и правопорядка.

2. Каждый объект критической информационной инфраструктуры подлежит категорированию в соответствии с утвержденными Правительством Российской Федерации показателями критериев категорирования и их значениями, а также порядком категорирования.

3. Субъекты критической информационной инфраструктуры на основании критериев, предусмотренных частью 1 настоящей статьи, в соответствии с утвержденными Правительством Российской Федерации показателями критериев и их значениями, а также порядком

категорирования, осуществляют категорирование принадлежащих им на праве собственности или ином законном основании объектов критической информационной инфраструктуры. Деятельность по категорированию осуществляется субъектами критической информационной инфраструктуры самостоятельно либо с привлечением организаций, имеющих лицензии на осуществление деятельности по технической защите конфиденциальной информации.

4. Сведения о результатах проведенного категорирования субъекты критической информационной инфраструктуры в письменном виде в десятидневный срок со дня принятия решения о присвоении объекту критической информационной инфраструктуры одной из категорий значимости направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной этим органом форме.

5. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в трехмесячный срок со дня поступления сведений о результатах категорирования проверяет

соблюдение процедур категорирования и правильность отнесения указанного объекта к одной из категорий значимости.

6. В целях осуществления учета значимых объектов критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, ведет реестр. О каждом значимом объекте критической информационной инфраструктуры в реестр вносятся следующие сведения:

1) наименование значимого объекта критической информационной инфраструктуры;

2) наименование субъекта критической информационной инфраструктуры, владеющего на праве собственности или ином законном основании значимым объектом критической информационной инфраструктуры;

3) основание для создания значимого объекта критической информационной инфраструктуры;

4) тип значимого объекта критической информационной инфраструктуры;

5) сведения о разработчике (проектировщике) значимого объекта критической информационной инфраструктуры;

6) сведения об операторе, эксплуатирующем значимый объект критической информационной инфраструктуры;

7) категория значимости, которая присвоена объекту критической информационной инфраструктуры;

8) сведения об аппаратном и программном обеспечении, используемом на значимом объекте критической информационной инфраструктуры;

9) меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры;

10) средства, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры.

7. При соблюдении субъектом критической информационной инфраструктуры процедуры категорирования и правильном присвоении категории значимости объекту критической информационной инфраструктуры, а также при соблюдении установленной формы представления этих сведений федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, вносит сведения об этом объекте критической информационной инфраструктуры

в реестр, о чем в десятидневный срок информируется субъект критической информационной инфраструктуры, направивший сведения.

8. При несоблюдении субъектом критической информационной инфраструктуры процедуры категорирования или неправильности присвоения категории значимости объекту критической информационной инфраструктуры, а также в случае несоблюдения установленной формы предоставления этих сведений федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, возвращает в письменном виде субъекту критической информационной инфраструктуры указанные сведения с мотивированным обоснованием причин возврата.

9. Субъект критической информационной инфраструктуры после получения им мотивированного обоснования причин возврата направленных им сведений об объекте критической информационной инфраструктуры устраняет отмеченные недостатки (в случае возможности их устранения) и повторно направляет их в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

10. Изменение категории значимости, к которой отнесен объект критической информационной инфраструктуры, производится в порядке, предусмотренном для категорирования, в следующих случаях:

1) по мотивированному решению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, принятому по результатам проверки, проведенной в рамках осуществления государственного контроля;

2) в результате изменений значимого объекта критической информационной инфраструктуры, следствием которых такой объект перестал соответствовать показателям критериев категорирования и их значениям, на основании которых ему была присвоена категория значимости.

Статья 7. **Права и обязанности субъектов критической информационной инфраструктуры**

1. Субъекты критической информационной инфраструктуры имеют право:

1) в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, получать от указанного органа информацию, необходимую для

обеспечения безопасности значимых объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры на праве собственности или ином законном основании, в том числе об угрозах безопасности информации и уязвимостях программного обеспечения, оборудования и технологий;

2) в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их обнаружения и предупреждения;

3) в дополнение к положениям, предусмотренным настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, самостоятельно либо с привлечением организаций, имеющих лицензии на осуществление деятельности по технической защите конфиденциальной информации, разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта критической информационной инфраструктуры;

4) по согласованию с федеральным органом исполнительной власти, уполномоченным в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, за свой счет приобретать и устанавливать средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2. Субъекты критической информационной инфраструктуры обязаны:

1) информировать в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, о компьютерных инцидентах;

2) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

Российской Федерации и обеспечения ее функционирования, в обнаружении и предупреждении компьютерных атак, а также в ликвидации их последствий, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах критической информационной инфраструктуры технических средств, предназначенных для поиска признаков компьютерных атак, обеспечивать выполнение технических условий установки и эксплуатации технических средств, порядка установки и эксплуатации таких технических средств и их сохранность.

3. Субъекты критической информационной инфраструктуры, владеющие на праве собственности либо ином законном основании значимыми объектами критической информационной инфраструктуры, помимо выполнения обязанностей, предусмотренных частью 2 настоящей статьи, также обязаны:

1) соблюдать требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) выполнять предписания должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, об устранении нарушений требований по обеспечению

безопасности значимого объекта критической информационной инфраструктуры, выданные с соблюдением установленных требований и в пределах их компетенции;

3) принимать меры по ликвидации последствий компьютерных атак, осуществленных в отношении принадлежащих субъектам критической информационной инфраструктуры значимых объектов критической информационной инфраструктуры;

4) обеспечивать беспрепятственный доступ должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, к значимому объекту критической информационной инфраструктуры при реализации должностными лицами полномочий, предусмотренных статьей 13 настоящего Федерального закона.

Статья 8. **Система безопасности значимого объекта критической информационной инфраструктуры**

1. В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической

информационной инфраструктуры Российской Федерации, создает систему безопасности такого объекта и обеспечивает ее функционирование.

2. Система безопасности значимого объекта критической информационной инфраструктуры должна обеспечивать:

1) предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения информации на значимом объекте критической инфраструктуры;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено или прекращено функционирование значимого объекта критической информационной инфраструктуры;

3) обнаружение и предупреждение компьютерных атак;

4) восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемое в том числе за счет создания и хранения резервных копий необходимой для этого информации;

5) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

6) сбор, анализ и хранение сведений о проведенных в отношении значимого объекта критической информационной инфраструктуры компьютерных атаках.

Статья 9. **Требования по обеспечению безопасности значимого объекта критической информационной инфраструктуры**

1. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в отношении организации деятельности по обеспечению безопасности таких объектов, информационных систем, автоматизированных систем управления технологическими процессами, а в части информационно-телекоммуникационных сетей - федеральным органом исполнительной власти, уполномоченным

в области связи по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

2. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, могут устанавливать своими нормативными правовыми актами требования, дополняющие требования, установленные принятыми в соответствии с настоящим Федеральным законом нормативными правовыми актами, исходя из особенностей функционирования значимых объектов критической информационной инфраструктуры в установленной сфере деятельности.

Статья 10. **Координация деятельности субъектов критической информационной инфраструктуры в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты**

1. Координацию деятельности субъектов критической информационной инфраструктуры в области обнаружения,

предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, а также организацию и осуществление обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными и неправительственными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, осуществляет Национальный координационный центр по компьютерным инцидентам.

Статья 11. **Порядок предоставления, обработки и распространения информации в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации**

1. В государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации поступает информация от технических средств этой системы, в том числе технических средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи.

2. Сведения, указанные в части 4 настоящей статьи, представляются в государственную систему обнаружения, предупреждения и ликвидации

последствий компьютерных атак на информационные ресурсы Российской Федерации:

1) субъектами критической информационной инфраструктуры;

2) федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

3. Сведения, указанные в части 4 настоящей статьи, могут быть представлены в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

1) государственными органами и органами местного самоуправления, не являющимися субъектами критической информационной инфраструктуры;

2) организациями, привлекаемыми субъектами критической информационной инфраструктуры к разработке и осуществлению мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

3) иными организациями и лицами, не являющимися субъектами критической информационной инфраструктуры.

4. Перечень сведений, представляемых в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и порядок их представления устанавливает федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

5. Сведения, содержащиеся в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, относятся к информации ограниченного доступа.

6. Порядок доступа к информации, содержащейся в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, определяется федеральным органом исполнительной власти, уполномоченным в области создания и обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Статья 12. **Оценка состояния защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак**

1. Оценка состояния защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак осуществляется федеральным органом исполнительной власти, уполномоченным в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, в целях прогнозирования ситуации в области обеспечения информационной безопасности Российской Федерации и принятия мер по повышению защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак.

2. Оценка состояния защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак осуществляется на основании:

1) анализа данных, получаемых при использовании технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные

ресурсы Российской Федерации, в том числе информации о признаках компьютерных атак в сетях электросвязи;

2) сведений, полученных по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры о нарушениях требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, в результате которых создаются предпосылки возникновения компьютерных инцидентов;

3) иной информации, получаемой в соответствии с законодательством Российской Федерации.

3. Для реализации положений, предусмотренных частями 1 и 2 настоящей статьи, федеральный орган исполнительной власти, уполномоченный в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, устанавливает в сетях электросвязи технические средства, предназначенные для поиска признаков компьютерных атак в сетях электросвязи.

4. Технические условия установки и эксплуатации технических средств, предназначенных для поиска признаков компьютерных атак, за

исключением технических средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, утверждаются федеральным органом исполнительной власти, уполномоченным в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования.

5. В целях выработки мер по совершенствованию систем безопасности значимых объектов критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и обеспечения ее функционирования, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, сведения, содержащие результаты оценки состояния защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак.

Статья 13. **Государственный контроль обеспечения безопасности значимых объектов критической информационной инфраструктуры**

1. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры осуществляется в целях проверки соблюдения субъектами критической информационной инфраструктуры, владеющими на праве собственности либо ином законном основании значимыми объектами критической информационной инфраструктуры, требований, установленных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Государственный контроль осуществляется путем проведения плановых либо внеплановых проверок.

2. Основаниями для проведения плановой проверки является истечение трех лет со дня:

1) внесения сведений об объекте критической информационной инфраструктуры в реестр;

2) окончания проведения последней плановой проверки в отношении значимого объекта критической информационной инфраструктуры.

3. Основаниями для проведения внеплановой проверки является:

1) истечение срока исполнения субъектом критической информационной инфраструктуры выданного уполномоченным федеральным органом исполнительной власти в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации предписания об устранении выявленного нарушения требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) возникновение компьютерного инцидента на значимом объекте критической информационной инфраструктуры;

3) поручение Президента Российской Федерации, Правительства Российской Федерации или требование прокурора о проведении внеплановой проверки в рамках осуществляемого им прокурорского надзора за исполнением законов.

4. По итогам проведенной проверки федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, составляется акт по утвержденной им форме, который содержит ее результаты.

5. На основании акта в случаях выявления нарушения требований обеспечения безопасности значимого объекта критической

информационной инфраструктуры, установленных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, выдает субъекту критической информационной инфраструктуры предписание об устранении нарушений этих требований, содержащее обязательные к исполнению указания по устранению выявленных нарушений и сроки их устранения.

6. Сведения, полученные в ходе проведения государственного контроля и содержащие информацию об уязвимостях программного обеспечения и оборудования значимого объекта критической информационной инфраструктуры, являются информацией ограниченного доступа.

Статья 14. **Ответственность за нарушение законодательства Российской Федерации в области безопасности критической информационной инфраструктуры Российской Федерации**

Граждане Российской Федерации, иностранные граждане и лица без гражданства за нарушение законодательства Российской Федерации в области безопасности критической информационной инфраструктуры Российской Федерации несут уголовную, административную,

гражданско-правовую и дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Статья 15. **Вступление в силу настоящего Федерального закона**

1. Настоящий Федеральный закон вступает в силу с 1 января 2017 года, за исключением статей 6 - 8, 13 и 14 настоящего Федерального закона.

2. Статьи 6 - 8, 13 и 14 настоящего Федерального закона вступают в силу с 1 января 2018 года.

Президент
Российской Федерации

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к проекту федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

Осуществляемый в настоящее время в Российской Федерации переход к информационному обществу приводит к тому, что подавляющее большинство систем принятия решений и бизнес-процессов в ключевых отраслях экономики и сфере государственного управления реализуются или планируются к реализации с использованием информационных технологий. В различных информационных системах уже сейчас хранятся и обрабатываются значительные объемы информации, в том числе касающейся вопросов государственной политики и обороны, финансовой и научно-технической сферы, частной жизни граждан.

Одновременно информационные технологии повсеместно внедряются при построении автоматизированных систем управления производственными и технологическими процессами, используемых в топливно-энергетическом, финансовом, транспортном и других секторах критической инфраструктуры Российской Федерации.

Глобализация современных информационно-коммуникационных сетей и информационных систем, вынужденное применение при их построении иностранного оборудования и заимствованного программного обеспечения, имеющего уязвимости, а также существенное увеличение количества автоматизированных систем управления производственными и технологическими процессами в сочетании с интенсивным совершенствованием средств и методов применения информационных и коммуникационных технологий в противоправных целях формируют новые угрозы безопасности Российской Федерации.

Нанесение ущерба критической информационной инфраструктуре может привести к катастрофическим последствиям, а учитывая, что она является связующим звеном между другими секторами национальной инфраструктуры, неизбежно нанесет ущерб и этим секторам. Переход информационных и коммуникационных технологий на систему цифровых сигналов упростил и частично автоматизировал управление процессами, но, в то же время, сделал их более уязвимыми перед компьютерными атаками. Вредоносная программа, направленная на внесение изменений в бинарный код программы (алгоритм программы, записанный в двоичной системе исчисления) способна вывести из

строя любое оборудование, работающее с использованием бинарного кода. При этом равную опасность могут представлять атаки, совершаемые в преступных, террористических и разведывательных целях со стороны отдельных лиц, сообществ, иностранных специальных служб и организаций.

По данным за последние годы, исходя из различных методик оценки ущерба от вредоносных программ, он составлял от трехсот миллиардов до одного триллиона долларов, то есть от 0,4% до 1,4% общемирового ежегодного ВВП, и эти показатели имеют тенденцию к неуклонному росту.

При развитии событий по наихудшему сценарию компьютерная атака способна полностью парализовать критическую информационную инфраструктуру государства и вызвать социальную, финансовую и/или экологическую катастрофу.

Характерными примерами последствий негативного воздействия компьютерных атак на критическую инфраструктуру государства могут послужить остановка центрифуг иранской атомной станции с помощью компьютерного вируса StuxNet в сентябре 2010 г. и паралич работы нескольких крупных финансовых учреждений Южной Кореи в марте 2013 г.

Таким образом, 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.

В настоящее время эффективное правовое регулирование в данной сфере затруднено из-за отсутствия системообразующих законодательных актов, устанавливающих порядок отношений в сфере обеспечения безопасности критической информационной инфраструктуры в Российской Федерации.

Законопроектом устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры, полномочия государственных органов Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами критической информационной инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

В соответствии с законопроектом безопасность критической информационной инфраструктуры Российской Федерации и ее объектов обеспечивается за счет:

- определения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

- разработки критериев категорирования объектов критической информационной инфраструктуры, показателей этих критериев и порядка категорирования объектов критической информационной инфраструктуры;

- категорирования объектов критической информационной инфраструктуры в соответствии с указанными критериями, показателями и порядком;

- ведения реестра значимых объектов критической информационной инфраструктуры;

- установления требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры с учетом их категорий;

- создания систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечение их функционирования;

- обеспечения взаимодействия этих систем с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, созданной в соответствии с Указом Президента Российской Федерации от 15 января 2013 г. № 31с;

- осуществления оценки состояния защищенности критической информационной инфраструктуры Российской Федерации;

- осуществления государственного контроля в области безопасности критической информационной инфраструктуры Российской Федерации.

Реализация мероприятий на указанных направлениях позволит обеспечить комплексность и непрерывность обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Результаты анализа опыта правового регулирования безопасности критической информационной инфраструктуры стран с развитой информационной инфраструктурой, таких как Германия, США, Великобритания, Япония и Южная Корея, а также международных правовых актов в данной области, показывают, что обеспечение безопасности критической информационной инфраструктуры Российской Федерации исключительно силами и средствами государства невозможно. Существенная часть объектов критической информационной инфраструктуры в этих странах, как и в Российской Федерации, не находится в собственности государства.

Исходя из этого, законопроектом предусматриваются дополнительные обременения, налагаемые на лиц, владеющих значимыми объектами критической информационной инфраструктуры на праве собственности или ином законном основании, касающиеся категорирования, создания и обеспечения функционирования систем безопасности этих объектов, а также обеспечения их взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Принятие законопроекта позволит создать правовую и организационную основу для эффективного функционирования системы безопасности критической информационной инфраструктуры Российской Федерации, направленной в первую очередь на предупреждение возникновения компьютерных инцидентов на ее объектах, а также существенно снизит общественно-политические, финансовые и иные негативные последствия для Российской Федерации в случае проведения против нее компьютерных атак.

ФИНАНСОВО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ

к проекту федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

Принятие федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" не потребует дополнительных расходов из федерального бюджета и не повлечет финансовых обязательств государства.

ПЕРЕЧЕНЬ

федеральных законов, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

Принятие федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" потребует внесения изменений в следующие федеральные законы:

1. Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации.

Обоснование: высокая общественная опасность деяний, причиняющих вред безопасности критической информационной инфраструктуры Российской Федерации или создающих угрозу его причинения.

Краткое описание.

Дополнение Уголовного кодекса Российской Федерации статьей 274.1, устанавливающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, в том числе за:

создание и (или) распространение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации;

неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации;

нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации.

Внесение изменения в пункт 2 части второй статьи 151 Уголовно-процессуального кодекса Российской Федерации (определение прямой подследственности органов федеральной службы безопасности по составам преступлений, предусмотренных статьей 274.1 Уголовного кодекса Российской Федерации), а также в часть пятую статьи 151 Уголовно-процессуального кодекса Российской Федерации (определение альтернативной подследственности по составам преступлений, предусмотренных статьей 274.1

Уголовного кодекса Российской Федерации, иных органов, уполномоченных проводить предварительное расследование).

2. Закон Российской Федерации "О государственной тайне".

Обоснование: необходимость защиты сведений о мерах, предпринимаемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации высокой и средней категорий опасности, а также сведений об оценке степени защищенности критической информационной инфраструктуры Российской Федерации.

Краткое описание.

Дополнение пункта 4 статьи 5 (сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму) новыми абзацами. Таким образом, сведения о мерах, предпринимаемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, а также об оценке степени защищенности критической информационной инфраструктуры Российской Федерации будут отнесены к сведениям, составляющим государственную тайну.

3. Федеральный закон "О связи".

Обоснование: необходимость обеспечения технических условий для функционирования технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также создание условий для обеспечения сохранности данных технических средств.

Краткое описание.

Дополнение части 1 статьи 46 Федерального закона "О связи" новым абзацем. Таким образом, операторы связи будут обязаны в случае установки в сетях электросвязи технических средств, предназначенных для поиска признаков компьютерных атак, обеспечивать выполнение утвержденных в соответствии с законодательством Российской Федерации о безопасности критической информационной инфраструктуры Российской Федерации технических условий установки и эксплуатации технических средств, порядка установки и эксплуатации таких технических средств, а также сохранность этих технических средств.

4. Федеральный закон "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

Обоснование: соблюдение принципа непрерывности и комплексности обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Краткое описание.

Дополнение части 3.1 статьи 1 пунктом 22. Тем самым положения указанного Федерального закона, устанавливающие порядок организации и проведения проверок, не будут применяться при осуществлении государственного контроля (надзора) в области безопасности критической информационной инфраструктуры Российской Федерации.

Подготовка проектов федеральных законов "О внесении изменений в законодательные акты Российской Федерации в связи с принятием федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" и "О внесении изменений в Уголовный кодекс Российской Федерации и в Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации", предусматривающих внесение указанных изменений, осуществляется одновременно с проектом федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

Головной исполнитель - ФСБ России.

Соисполнители: Минкомсвязь России, МВД России, ФСО России, ФСТЭК России, Минэкономразвития России, Минпромторг России.

П Е Р Е Ч Е Н Ь

нормативных правовых актов Президента Российской Федерации, Правительства Российской Федерации и федеральных органов исполнительной власти, подлежащих признанию утратившими силу, приостановлению, изменению или принятию в связи с проектом федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
	Нормативные правовые акты Президента Российской Федерации			
1.	Проект указа Президента Российской Федерации "О федеральном органе исполнительной власти, уполномоченном в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации"	Реализация пункта 2 части 1 статьи 5 законопроекта. Указом будет определен федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее - КИИ)	В течение 6 месяцев после принятия закона	ФСТЭК России ФСБ России

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
		Нормативные правовые акты Правительства Российской Федерации		
2.	Проект постановления Правительства Российской Федерации "Об утверждении показателей критериев категорирования объектов критической информационной инфраструктуры Российской Федерации, значений таких показателей, а также порядка категорирования объектов критической информационной инфраструктуры Российской Федерации"	Реализация пункта 1 части 2 статьи 5 законопроекта. Постановлением будут утверждены конкретные показатели и их значения следующих критериев категорирования объектов КИИ: - социальной значимости; - политической значимости; - экономической значимости; - экологической значимости; - значимости для обеспечения обороноспособности, безопасности государства и правопорядка. Руководствуясь данными показателями, субъекты КИИ будут осуществлять отнесение своих объектов КИИ к низкой, средней или высокой категориям значимости.	В течение 6 месяцев после определения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации	Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации ФСБ России Федеральные органы исполнительной власти в соответствии с компетенцией

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
		Постановлением будет утвержден порядок, в соответствии с которым субъекты КИИ будут проводить категорирование своих объектов КИИ		
3.	Проект постановления Правительства Российской Федерации "Об утверждении порядка осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской федерации	Реализация пункта 2 части 2 статьи 5 законопроекта. Постановлением будет утвержден порядок организации и проведения проверок соблюдения требований по обеспечению безопасности значимых объектов КИИ	В течение 6 месяцев после определения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации	Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации Федеральные органы исполнительной власти в соответствии с компетенцией

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
4.	Проект постановления Правительства Российской Федерации "Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи для обеспечения функционирования значимых объектов критической информационной инфраструктуры Российской Федерации"	Реализация пункта 3 части 2 статьи 5 законопроекта. Постановлением будет утвержден порядок подготовки и использования ресурсов единой сети электросвязи для обеспечения функционирования значимых объектов КИИ, регламентирующий правила предоставления услуг связи операторами связи для таких объектов	В течение 6 месяцев после принятия закона	Минкомсвязь России ФСБ России
	Нормативные правовые акты федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации			
5.	Проект приказа федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской	Реализация части 4 статьи 6 законопроекта. Приказом будут утверждены формы предоставления субъектами КИИ сведений о проведенном	В течение 6 месяцев после определения федерального органа исполнительной власти, уполномоченного в	Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
	Федерации "Об утверждении формы предоставления сведений о проведенном категорировании"	категорировании для их проверки федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ	области обеспечения безопасности критической информационной инфраструктуры Российской Федерации	информационной инфраструктуры Российской Федерации
6.	Проект приказа федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации "Об утверждении формы реестра объектов критической информационной инфраструктуры Российской Федерации и правил его ведения"	Реализация пункта 3 части 3 статьи 5 законопроекта. Приказом будут утверждены форма реестра объектов КИИ и правила его ведения, включающие порядок подготовки, утверждения и внесения изменений в реестр значимых объектов КИИ	В течение 6 месяцев после определения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации	Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
7.	Проект приказа федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"	Реализация пункта 5 части 3 статьи 5 и части 1 статьи 9 законопроекта. Приказом будут утверждены требования по обеспечению безопасности для каждой категории значимых объектов КИИ, включающие в себя требования: - к организации деятельности по обеспечению безопасности таких объектов; - для информационных систем; - для автоматизированных систем управления технологическими процессами	В течение 6 месяцев после определения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации	Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации ФСБ России

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
8.	Проект приказа федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации "Об утверждении формы акта по результатам проведенной проверки в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"	Реализация части 4 статьи 13 законопроекта. Приказом будет утверждена форма акта по результатам проведенной проверки в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ	В течение 6 месяцев после определения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации	Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
		Нормативные правовые акты ФСБ России		
9.	Проект приказа ФСБ России "Об утверждении порядка реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак	Реализация пункта 5 части 4 статьи 5 законопроекта. Приказом будет утвержден порядок реагирования на компьютерные инциденты и	В течение 9 месяцев после принятия закона	ФСБ России

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
	на значимых объектах критической информационной инфраструктуры Российской Федерации"	ликвидации последствий компьютерных атак на значимые объекты КИИ		
10.	Проект приказа ФСБ России "Об утверждении перечня сведений, предоставляемых в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и порядка их предоставления"	Реализация части 4 статьи 11 законопроекта. Приказом будут утверждены перечень сведений, предоставляемых в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также порядок их предоставления субъектами КИИ	В течение 9 месяцев после принятия закона	ФСБ России

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
11.	Проект приказа ФСБ России "Об утверждении порядка доступа к информации, содержащейся в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"	Реализация части 6 статьи 11 законопроекта. Приказом будет утвержден порядок доступа к информации, содержащейся в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	В течение 9 месяцев после принятия закона	ФСБ России
12.	Проект приказа ФСБ России "Об утверждении требований к техническим средствам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"	Реализация пункта 8 части 4 статьи 5 законопроекта. Приказом будут утверждены требования к техническим средствам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	В течение 9 месяцев после принятия закона	ФСБ России Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
13.	Проект приказа ФСБ России "Об утверждении технических условий установки и эксплуатации технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"	Реализация части 4 статьи 12 законопроекта. Приказом будут утверждены технические условия установки и эксплуатации устанавливаемых на объектах КИИ технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	В течение 9 месяцев после принятия закона	ФСБ России Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
14.	Проект приказа ФСБ России "Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам"	Реализация статьи 10, пункта 1 части 2 статьи 7 и пункта 6 части 4 статьи 5 законопроекта. Приказом будут утверждены Положение о Национальном координационном центре по компьютерным инцидентам, включающее в себя порядок информирования субъектами	В течение 9 месяцев после принятия закона	ФСБ России

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
		критической информационной инфраструктуры Российской Федерации о компьютерных инцидентах, произошедших на объектах КИИ, принадлежащих им на праве собственности или ином законном основании, порядок обмена информацией о компьютерных инцидентах субъектов КИИ между собой, а также с уполномоченными органами иностранных государств, международными и неправительственными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты		

№ п/п	Наименование проекта нормативного правового акта	Обоснование необходимости подготовки, краткое описание	Срок подготовки	Исполнители
		Нормативные правовые акты Минкомсвязи России		
15.	Проект приказа Минкомсвязи России "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"	Реализация пункта 1 части 5 статьи 5 и части 1 статьи 9 законопроекта. Приказом будут утверждены требования по обеспечению безопасности для каждой категории значимых объектов КИИ, включающие в себя требования: - для объектов связи; - для информационно-телекоммуникационных сетей	В течение 6 месяцев после определения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации	Минкомсвязь России Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации
16.	Проект приказа Минкомсвязи России "Об утверждении порядка и технических условий установки и эксплуатации для операторов связи устанавливаемых в сетях электросвязи технических средств, предназначенных для поиска признаков компьютерных атак"	Реализация пункта 2 части 5 статьи 5 законопроекта. Приказом будут утверждены порядок и технические условия установки и эксплуатации технических средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи	В течение 9 месяцев после принятия закона	Минкомсвязь России ФСБ России

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 5 декабря 2016 г. № 2589-р

МОСКВА

1. Внести в Государственную Думу Федерального Собрания Российской Федерации проекты федеральных законов "О безопасности критической информационной инфраструктуры Российской Федерации", "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" и "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

2. Назначить статс-секретаря - заместителя директора Федеральной службы безопасности Российской Федерации Шалькова Дмитрия Владиславовича официальным представителем Правительства Российской Федерации при рассмотрении палатами Федерального Собрания Российской Федерации проектов федеральных законов "О безопасности критической информационной инфраструктуры Российской Федерации", "О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" и "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

Председатель Правительства
Российской Федерации Д.Медведев

3137239