Проект Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" (подготовлен ФСБ России) (не внесен в ГД ФС РФ, текст по состоянию на 08.08.2013)

Проект

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон устанавливает организационные и правовые основы обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях предотвращения компьютерных инцидентов, основные принципы и методы государственного регулирования в указанной сфере, порядок взаимодействия субъектов критической информационной инфраструктуры Российской Федерации с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, определяет полномочия органов государственной власти Российской Федерации, а также права, обязанности и ответственность субъектов критической информационной инфраструктуры Российской Федерации.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации - комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса критически важного объекта;

аккредитация - официальное признание федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации (далее - уполномоченные федеральные органы исполнительной власти) компетентности организации выполнять работы в области оценки защищенности критической информационной инфраструктуры Российской Федерации;

безопасность критической информационной инфраструктуры Российской Федерации - состояние объектов критической информационной инфраструктуры Российской Федерации и критической информационной инфраструктуры Российской Федерации в целом, при котором возникновение на них компьютерных инцидентов не приведет к потере управления экономикой и/или обеспечения обороноспособности, безопасности и правопорядка Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения;

государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - единая централизованная, территориально распределенная система, включающая силы и средства обнаружения и предупреждения компьютерных инцидентов, а также органы государственной власти, в полномочия которых входит обеспечение безопасности объектов критической информационной инфраструктуры Российской Федерации;

информационные ресурсы Российской Федерации - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом;

компьютерная атака - целенаправленное воздействие на информационные ресурсы программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих ресурсах;

компьютерный инцидент - факт нарушения (или прекращения) функционирования объекта критической информационной инфраструктуры Российской Федерации, в том числе вызванный компьютерной атакой;

критически важный объект - объект, нарушение или прекращение функционирования которого может привести к потере управления экономикой Российской Федерации, субъекта Российской Федерации или

административно-территориальной единицы, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения;

критическая информационная инфраструктура Российской Федерации - совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка (далее - объекты критической информационной инфраструктуры Российской Федерации);

нарушение функционирования критической информационной инфраструктуры Российской Федерации - отрицательные последствия целенаправленного и/или случайного воздействия на объекты критической информационной инфраструктуры Российской Федерации, приведшие к утечке, хищению, утрате, подделке, искажению и несанкционированному доступу к информации, а также к отклонению от установленных эксплуатационных пределов и условий функционирования объектов критической информационной инфраструктуры Российской Федерации;

субъекты критической информационной инфраструктуры Российской Федерации - юридические лица, владеющие на праве собственности или ином законном основании объектами критической информационной инфраструктуры Российской Федерации, операторы связи, а также операторы государственных информационных систем, обеспечивающие функционирование и взаимодействие объектов критической информационной инфраструктуры Российской Федерации.

Статья 3. Законодательство о безопасности критической информационной инфраструктуры Российской Федерации

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

2. Если международным договором Российской Федерации установлены иные правила, чем те правила, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора Российской Федерации.

Статья 4. Обеспечение безопасности критической информационной инфраструктуры Российской Федерации

1. Обеспечение безопасности критической информационной инфраструктуры Российской Федерации включает комплекс мер правового, организационного и технического характера по созданию и эксплуатации систем безопасности объектов критической информационной инфраструктуры Российской Федерации и их взаимодействию с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации в целях недопущения нарушения или прекращения функционирования критической информационной инфраструктуры Российской Федерации.

2. Основными направлениями обеспечения безопасности критической информационной инфраструктуры Российской Федерации являются:

1) нормативное правовое регулирование деятельности по обеспечению безопасности критической информационной инфраструктуры Российской Федерации;

2) определение уполномоченных федеральных органов исполнительной власти, осуществляющих мероприятия по обеспечению безопасности критической информационной инфраструктуры Российской Федерации;

3) разработка и реализация федеральных целевых программ обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

4) установление обязательных требований по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации, их технической защищенности, в том числе при создании, вводе в эксплуатацию, эксплуатации и модернизации (на всех этапах жизненного цикла);

5) категорирование объектов критической информационной инфраструктуры Российской Федерации;

6) оценка защищенности объектов критической информационной инфраструктуры Российской Федерации;

7) создание и обеспечение функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

8) государственный контроль (надзор) в области безопасности критической информационной инфраструктуры Российской Федерации;

9) информационно-аналитическое, материально-техническое и научно-техническое обеспечение безопасности критической информационной инфраструктуры Российской Федерации;

10) выявление угроз безопасности критической информационной инфраструктуры Российской Федерации;

11) обнаружение, предупреждение и ликвидация последствий компьютерных атак на информационные ресурсы Российской Федерации.

3. Разработка мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации осуществляется уполномоченными федеральными органами исполнительной власти и субъектами критической информационной инфраструктуры Российской Федерации на основе проведенного категорирования объектов критической информационной инфраструктуры Российской Федерации в соответствии с требованиями настоящего Федерального закона и принятыми в соответствии с ним нормативными правовыми актами.

4. Уполномоченные федеральные органы исполнительной власти в пределах своей компетенции принимают участие в международном сотрудничестве в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, участвуют в работе международных организаций, совещаний и конференций по вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации, а также в соответствии с международными договорами осуществляют обмен информацией на взаимной основе с органами иностранных государств и международными организациями о возможных угрозах безопасности и выявленных компьютерных инцидентах.

Глава 2. ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 5. Цель и принципы обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. Целью обеспечения безопасности критической информационной инфраструктуры Российской Федерации является ее устойчивое и безопасное функционирование, обеспечивающее защиту интересов личности, общества и государства в информационной сфере.

2. Основными 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;

5) эффективное взаимодействие уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры Российской Федерации;

6) приоритет предупреждения компьютерных инцидентов в критической информационной инфраструктуре Российской Федерации.

Статья 6. Полномочия органов государственной власти в сфере обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. Президент Российской Федерации:

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

2) определяет порядок создания и принципы построения государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

3) определяет случаи использования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации для решения задач, не связанных с обеспечением безопасности объектов критической инфраструктуры Российской Федерации.

2. Правительство Российской Федерации

организует обеспечение федеральных органов исполнительной власти средствами и ресурсами, необходимыми для выполнения задач в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

3. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности:

1) осуществляет реализацию государственной политики в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

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

3) координирует деятельность субъектов критической информационной инфраструктуры Российской Федерации в области обнаружения, предупреждения и ликвидации компьютерных инцидентов;

4) по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации вносит предложения о совершенствовании нормативного правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации Президенту Российской Федерации и в Правительство Российской Федерации;

5) проводит оценку защищенности объектов критической информационной инфраструктуры Российской Федерации для объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности;

6) проводит проверку на достоверность и правильность отнесения объектов критической информационной инфраструктуры Российской Федерации к высокой категории опасности;

7) ведет реестр объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности, утверждает форму указанного реестра и правила его ведения;

8) проводит аккредитацию организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности;

9) осуществляет государственный контроль (надзор) в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности, а также устанавливает порядок его осуществления;

10) совместно с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, разрабатывает и утверждает показатели критериев категорирования объектов критической информационной инфраструктуры Российской Федерации;

11) устанавливает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, требования к обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности;

12) осуществляет иные предусмотренные настоящим Федеральным законом полномочия.

4. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации:

1) осуществляет реализацию государственной политики в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

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

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

4) проводит оценку защищенности объектов критической информационной инфраструктуры Российской Федерации для объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности;

5) проводит проверку на достоверность и правильность отнесения объектов критической информационной инфраструктуры Российской Федерации к средней и низкой категориям опасности;

6) ведет реестр объектов критической информационной инфраструктуры Российской Федерации

средней и низкой категорий опасности, утверждает форму указанного реестра и правила его ведения;

7) проводит аккредитацию организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности;

8) осуществляет государственный контроль (надзор) в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности, а также устанавливает порядок его осуществления;

7) совместно с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности разрабатывает и утверждает показатели критериев категорирования объектов критической информационной инфраструктуры Российской Федерации;

8) устанавливает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, требования к обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации низкой и средней категории опасности;

9) осуществляет иные предусмотренные настоящим Федеральным законом полномочия.

Статья 7. Финансирование мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации

1. Финансирование мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации осуществляется за счет средств субъектов, которым объекты критической информационной инфраструктуры Российской Федерации принадлежат на праве собственности или ином законном основании, а также средств федерального бюджета, выделенных уполномоченным федеральным органам исполнительной власти на осуществление таких мероприятий.

2. Финансирование организации и функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов на информационные ресурсы Российской Федерации осуществляется за счет средств федерального бюджета.

3. Финансирование мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации за счет иных источников средств осуществляется в соответствии с законодательством Российской Федерации.

Глава 3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 8. Категорирование объектов критической информационной инфраструктуры Российской Федерации

1. Для установления дифференцированных требований обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации с учетом возможных последствий нарушения или прекращения их функционирования проводится категорирование объектов на основе критериев, установленных частью 2 настоящей статьи.

2. Категорирование объектов критической информационной инфраструктуры Российской Федерации осуществляется исходя из следующих критериев:

критерий экономической значимости;

критерий экологической значимости;

критерий значимости для обеспечения обороноспособности;

критерий значимости для национальной безопасности;

критерий социальной значимости;

критерий важности объекта критической информационной инфраструктуры Российской Федерации в части реализации управленческой функции;

критерий важности объекта критической информационной инфраструктуры Российской Федерации в части предоставления значительного объема информационных услуг.

3. С учетом указанных в части 2 настоящей статьи критериев устанавливаются следующие категории объектов критической информационной инфраструктуры Российской Федерации:

1) объекты критической информационной инфраструктуры Российской Федерации высокой категории опасности;

2) объекты критической информационной инфраструктуры Российской Федерации средней категории опасности;

3) объекты критической информационной инфраструктуры Российской Федерации низкой категории опасности.

4. Субъекты критической информационной инфраструктуры Российской Федерации на основании установленных частью 2 настоящей статьи критериев и в соответствии с утвержденными показателями этих критериев, осуществляют отнесение принадлежащих им на праве собственности или ином законном основании объектов критической информационной инфраструктуры Российской Федерации к установленным категориям.

5. Сведения о результатах проведенного категорирования субъекты критической информационной инфраструктуры Российской Федерации направляют:

- в отношении объектов высокой категории опасности - в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, по утвержденной им форме;

- в отношении объектов средней и низкой категории опасности - в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, по утвержденной им форме.

6. Полученные сведения о результатах проведенного категорирования подлежат проверке на достоверность и правильность отнесения объекта критической информационной инфраструктуры Российской Федерации к определенной категории.

7. При несоответствии предоставленных сведений утвержденным показателям критериев либо при несоблюдении формы предоставления этих сведений уполномоченный федеральный орган исполнительной власти возвращает субъекту критической информационной инфраструктуры Российской Федерации предоставленные им документы на доработку с мотивированным обоснованием причин возврата.

8. При соответствии предоставленных сведений утвержденным показателям критериев и форме предоставления этих сведений объекты критической информационной инфраструктуры Российской Федерации высокой категории опасности включаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности в реестр объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности, а объекты критической информационной инфраструктуры Российской Федерации средней и низкой категории опасности включаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, в реестр объектов критической информационной инфраструктуры Российской Федерации средней и низкой категории опасности.

9. Пересмотр категории объекта критической информационной инфраструктуры Российской Федерации может производиться в порядке категорирования, предусмотренном пунктами 4 - 6 настоящей статьи, по инициативе субъекта критической информационной инфраструктуры Российской Федерации или по обоснованному решению уполномоченного федерального органа исполнительной власти, в том числе по результатам проведенной оценки защищенности этого объекта.

Статья 9. Оценка защищенности критической информационной инфраструктуры Российской Федерации

1. Оценка защищенности критической информационной инфраструктуры Российской Федерации проводится на основе оценки защищенности ее объектов, анализа данных, получаемых при использовании технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, информации о признаках компьютерных атак в сетях электросвязи, а также иной информации, получаемой в соответствии с законодательством Российской Федерации.

2. В целях реализации части 1 настоящей статьи федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, устанавливает в сетях электросвязи технические средства, предназначенные для поиска признаков компьютерных атак в сообщениях электросвязи.

3. Технические условия, порядок установки и эксплуатации технических средств, указанных в частях 1 и 2 настоящей статьи, определяются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

4. Оценка защищенности объектов критической информационной инфраструктуры Российской Федерации проводится в целях определения состояния их защищенности, соответствующей определенной категории объектов критической информационной инфраструктуры Российской Федерации, от потенциальных угроз возникновения компьютерных инцидентов.

5. Порядок проведения оценки защищенности Российской Федерации устанавливается:

- в отношении объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности - федеральным органом исполнительной власти, уполномоченным в области

обеспечения безопасности;

- в отношении объектов критической информационной инфраструктуры Российской Федерации средней и низкой категориям опасности - федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации.

КонсультантПлюс: примечание.
Нумерация пунктов дана в соответствии с официальным текстом документа.

---

7. При проведении оценки защищенности объектов критической информационной инфраструктуры Российской Федерации могут привлекаться аккредитованные для этих целей в установленном порядке организации.

8. На основе проведенной оценки защищенности объектов критической информационной инфраструктуры Российской Федерации уполномоченным федеральным органом исполнительной власти составляется акт, который содержит результаты проведенной оценки защищенности, а также, в необходимых случаях, предписание субъекту критической информационной инфраструктуры Российской Федерации в отношении мер, которые необходимо дополнительно включить в систему безопасности объекта критической информационной инфраструктуры Российской Федерации.

9. Сведения, полученные в ходе проведения оценки защищенности, раскрывающие уязвимость объекта критической информационной инфраструктуры Российской Федерации, относятся к информации ограниченного доступа. Если федеральным законом такие сведения отнесены к сведениям, составляющим государственную тайну, они подлежат защите в соответствии с законодательством Российской Федерации о государственной тайне.

Статья 10. Аккредитация организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации

1. Аккредитация организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации проводится на добровольной основе. Аккредитация организаций проводится на срок пять лет, если более короткий срок не указан в заявлении организации.

2. Аккредитация организаций проводится при условии выполнения ими следующих требований:

- наличие лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну;

- наличие средств, предназначенных для оценки защищенности объектов критической информационной инфраструктуры Российской Федерации и получивших подтверждение соответствия требованиям, установленным в соответствии с частью 7 статьи 13 настоящего Федерального закона;

- наличие в штате организации не менее трех работников, непосредственно осуществляющих деятельность по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации, имеющих высшее профессиональное образование в области информационной безопасности.

3. Аттестат аккредитации выдается на основании представленных заявителем заявления о предоставлении аттестата аккредитации и документов, подтверждающих соответствие заявителя требованиям аккредитации. Исчерпывающий перечень таких документов содержится в порядке проведения аккредитации, установленном уполномоченным федеральным органом исполнительной власти.

4. Основанием отказа в предоставлении аттестата аккредитации является:

- наличие в представленных заявителем заявлении о предоставлении аттестата аккредитации и (или) прилагаемых к нему документах недостоверной или искаженной информации;

- установленное при проведении документарной проверки несоответствие заявителя требованиям аккредитации.

5. Основаниями для досрочного аннулирования аттестата аккредитации являются:

- обращение организации о прекращении деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации;

- прекращение действия лицензии на осуществление работ, связанных с использованием сведений, составляющих государственную тайну, выданной организации.

6. Критерии аккредитации и порядок ее проведения устанавливаются:

- в отношении организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности - федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности;

- в отношении организаций для осуществления ими деятельности по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации средней и низкой категорий опасности - федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации.

Статья 11. Требования по обеспечению безопасности объекта критической информационной инфраструктуры Российской Федерации

1. Требования по обеспечению безопасности объекта критической информационной инфраструктуры Российской Федерации включают:

организационные вопросы безопасности;

требования к персоналу, непосредственно обеспечивающему функционирование и безопасность объектов критической информационной инфраструктуры Российской Федерации;

требования к защите от вредоносного программного обеспечения и от компьютерных атак;

требования безопасности при взаимодействии с сетями связи общего пользования;

требования к обеспечению безопасности информационных технологий в ходе эксплуатации информационно-телекоммуникационных систем.

2. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, могут устанавливать дополнительные требования по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации, исходя из специфики этих объектов, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, - в отношении объектов критической информационной инфраструктуры Российской Федерации высокой категории опасности или с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, - в отношении объектов критической информационной инфраструктуры Российской Федерации средней и низкой категории опасности.

Статья 12. Права и обязанности субъектов критической информационной инфраструктуры Российской Федерации

1. Субъекты критической информационной инфраструктуры Российской Федерации имеют право:

1) в установленном порядке получать от уполномоченных федеральных органов исполнительной власти информацию, касающуюся обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации, принадлежащих им на праве собственности или ином законном основании;

2) самостоятельно разрабатывать мероприятия по обеспечению безопасности объекта критической информационной инфраструктуры Российской Федерации, не противоречащие требованиям настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов.

2. Субъекты критической информационной инфраструктуры Российской Федерации обязаны:

1) обеспечивать защиту, в том числе физическую, объектов критической информационной инфраструктуры Российской Федерации, принадлежащих им на праве собственности или ином законном основании;

2) направлять сведения о выполнении мероприятий, содержащихся в предписании по результатам проведенной оценки защищенности объектов критической информационной инфраструктуры Российской Федерации в уполномоченный федеральный орган исполнительной власти, определенный частью 7 статьи 9 настоящего Федерального закона;

3) незамедлительно информировать в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, о компьютерных инцидентах, произошедших на объектах критической информационной инфраструктуры Российской Федерации, принадлежащих им на праве собственности или ином законном основании;

4) выполнять предписания, представления должностных лиц уполномоченных федеральных органов исполнительной власти об устранении нарушений требований по обеспечению безопасности объекта критической информационной инфраструктуры Российской Федерации и об устранении причин и условий, способствующих реализации угроз безопасности Российской Федерации;

5) обеспечивать беспрепятственный доступ должностных лиц уполномоченных федеральных органов исполнительной власти к объекту критической информационной инфраструктуры Российской Федерации,

при реализации ими полномочий, предусмотренных настоящим Федеральным законом;

6) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, в выявлении, предупреждении и пресечении компьютерных инцидентов, а также в ликвидации их последствий, установлении причин и условий их совершения;

7) обеспечивать выполнение технических условий, порядка установки и эксплуатации, а также сохранность технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

8) обеспечивать выполнение технических условий, порядка установки и эксплуатации, а также сохранность технических средств, предназначенных для поиска признаков компьютерных атак в сообщениях электросвязи.

Статья 13. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации обеспечивает:

- организацию защиты информационных ресурсов Российской Федерации от компьютерных атак;
- выявление признаков проведения компьютерных атак, определение их источников, методов осуществления и направленности;
- организацию и осуществление взаимодействия на национальном и межгосударственном уровнях в области обнаружения компьютерных атак и установления их источников;
- научные исследования в области создания средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- сбор и анализ информации о компьютерных инцидентах в информационном пространстве Российской Федерации, а также о компьютерных инцидентах в информационном пространстве других стран, в которые вовлечены информационные ресурсы Российской Федерации;
- осуществление мероприятий по оперативному реагированию на компьютерные инциденты;
- организацию и осуществление взаимодействия с субъектами критической информационной инфраструктуры Российской Федерации, правоохранительными органами и другими заинтересованными органами и организациями по вопросам реагирования на компьютерные инциденты;
- сбор и анализ сведений о выявляемых уязвимостях программного обеспечения и оборудования, а также средствах и способах проведения компьютерных атак;
- организацию и осуществление международного обмена информацией о выявленных угрозах, обмене лучшими практиками выявления и устранения уязвимостей и реагирования на компьютерные инциденты;
- оценку реального уровня защищенности информационных систем и информационно-телекоммуникационных сетей;
- поиск и выявление компьютерных атак, а также ликвидация последствий компьютерных инцидентов.

КонсультантПлюс: примечание.

Нумерация пунктов дана в соответствии с официальным текстом документа.

---

4. В рамках государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации функционирует Национальный координационный центр по компьютерным инцидентам, обеспечение деятельности которого осуществляет федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

5. Представление информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации осуществляют:

субъекты критической информационной инфраструктуры Российской Федерации;

уполномоченные федеральные органы исполнительной власти, в том числе с использованием технических средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

иные органы государственной власти;

аккредитованные организации, осуществляющие деятельность по оценке защищенности объектов критической информационной инфраструктуры Российской Федерации.

Перечень сведений, подлежащих представлению в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов на информационные ресурсы

Российской Федерации, и порядок их предоставления устанавливает федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

6. Сведения, содержащиеся в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, относятся к информации ограниченного доступа. Если федеральным законом такие сведения отнесены к сведениям, составляющим государственную тайну, они подлежат защите в соответствии с законодательством Российской Федерации о государственной тайне.

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 обеспечения безопасности.

7. Требования к техническим средствам, обеспечивающим взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к техническим средствам, предназначенным для поиска признаков компьютерных атак в сообщениях электросвязи, устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности.

8. Субъектами критической информационной инфраструктуры Российской Федерации в незамедлительном порядке принимаются меры по ликвидации последствий компьютерных инцидентов. Порядок реагирования на компьютерные инциденты и ликвидации их последствий на объектах критической информационной инфраструктуры Российской Федерации определяется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

9. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации может использоваться для решения задач, не связанных с обеспечением безопасности объектов критической инфраструктуры Российской Федерации, в случаях, определенных в соответствии с частью первой статьи 6 настоящего Федерального закона.

Статья 14. Обеспечение безопасности объекта критической информационной инфраструктуры Российской Федерации

1. В целях обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации субъекты критической информационной инфраструктуры Российской Федерации создают на них системы безопасности и обеспечивают их функционирование.

2. Система безопасности объекта критической информационной инфраструктуры Российской Федерации должна обеспечивать:

1) предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения информации, а также совершения иных противоправных действий по отношению к информации, обеспечивающей управление и контроль за технологическими процессами критически важных объектов;

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

3) реагирование на компьютерные инциденты;

4) возможность незамедлительного восстановления информации и функционирования объекта критической информационной инфраструктуры Российской Федерации;

5) создание и хранение резервных копий информации, обеспечивающей управление и контроль за технологическими процессами критически важных объектов;

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

3. Обеспечение физической защиты объекта критической информационной инфраструктуры Российской Федерации осуществляется в соответствии с законодательством Российской Федерации.

Глава 4. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА И ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЕГО ТРЕБОВАНИЙ

Статья 15. Государственный контроль (надзор) за соблюдением требований настоящего

Федерального закона

1. Государственный контроль (надзор) в области безопасности критической информационной инфраструктуры Российской Федерации осуществляется в целях реализации принципов, установленных настоящим Федеральным законом.

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

1) категорирования объекта критической информационной инфраструктуры Российской Федерации;

2) окончания проведения последней плановой проверки.

3. Основанием для проведения внеплановой проверки является:

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

2) поступление в уполномоченные органы исполнительной власти обращений и заявлений граждан, индивидуальных предпринимателей, юридических лиц, информации от органов государственной власти (в том числе должностных лиц уполномоченных органов исполнительной власти), органов местного самоуправления, из средств массовой информации и оперативных источников об угрозах возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры Российской Федерации;

3) возникновение компьютерного инцидента на объекте критической информационной инфраструктуры Российской Федерации, повлекшего за собой нарушение или прекращение функционирования этого объекта;

4) наличие приказа (распоряжения) руководителя уполномоченного федерального органа исполнительной власти, изданного в соответствии с поручениями Президента Российской Федерации, Правительства Российской Федерации и на основании требования прокурора о проведении внеплановой проверки в рамках надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Статья 16. Ответственность за нарушение настоящего Федерального закона

За нарушение законодательства о безопасности критической информационной инфраструктуры Российской Федерации виновные лица несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Глава 5. ЗАКЛЮЧИТЕЛЬНЫЕ И ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

Статья 17. Вступление в силу настоящего Федерального закона

Настоящий Федеральный закон вступает в силу с 1 января 2015 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 в ближайшем будущем 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 критически важных объектов инфраструктуры Российской Федерации (далее - АСУ КВО), используемых в топливно-энергетической, финансовой, транспортной 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 доли территориально распределенных АСУ КВО, взаимодействие которых зачастую осуществляется посредством сетей связи общего пользования, в сочетании с интенсивным совершенствованием средств и методов применения информационных и коммуникационных технологий в противоправных целях, формируют новые угрозы безопасности Российской Федерации.

Ущерб критической информационной инфраструктуре может привести к катастрофическим последствиям, так как информационная инфраструктура является связующим звеном между другими секторами национальной инфраструктуры и неизбежно повлечет ущерб 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 инцидентами, включая компьютерные атаки. 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 и иностранных специальных служб. При наихудшем развитии сценария компьютерная атака способна полностью парализовать критическую информационную инфраструктуру государства и вызвать социальную, финансовую и/или экологическую катастрофу.

Характерными примерами негативного воздействия компьютерных атак на критическую инфраструктуру государства могут послужить остановка центрифуг иранской атомной станции с помощью компьютерного вируса StuxNet в сентябре 2010 года и массированные компьютерные атаки, парализовавшие работу нескольких крупных финансовых учреждений Южной Кореи в марте 2013 года.

Таким образом, стабильность социально-экономического развития Российской Федерации и ее безопасность, по сути, поставлены в прямую зависимость от надежности и безопасности функционирования информационно-коммуникационных сетей и информационных систем.

В настоящее время системообразующие законодательные акты, регулирующие отношения в сфере безопасности критической информационной инфраструктуры в Российской Федерации, отсутствуют, что приводит к несогласованности и недостаточной эффективности правового регулирования в данной сфере.

Законопроектом устанавливаются основные направления и 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 объектами критической информационной инфраструктуры, операторов связи, операторов государственных информационных систем, обеспечивающих функционирование и взаимодействие этих объектов.

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

- разработки критериев отнесения объектов критической информационной инфраструктуры к различным категориям опасности;

- категорирования объектов критической информационной инфраструктуры в соответствии с указанными критериями;

- ведения реестров объектов критической информационной инфраструктуры с учетом их категории опасности;

- установления требований к системам безопасности объектов критической информационной инфраструктуры с учетом их категории опасности;

- 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. N 31с;

- осуществления оценки защищенности критической информационной инфраструктуры Российской Федерации и ее объектов;

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

Указанные направления деятельности позволят обеспечить комплексность и непрерывность

обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Анализ 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 показывает, что обеспечение безопасности критической информационной инфраструктуры Российской Федерации исключительно силами и средствами государства невозможно. Существенная часть объектов критической информационной инфраструктуры в данных странах, как и в Российской Федерации, не находится в собственности государства. Исходя из этого, законопроектом предусматриваются дополнительные обременения, накладываемые на лиц, владеющих объектами критической информационной инфраструктуры на праве собственности, 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 позволит существенно снизить их общественно-политические, финансовые и иные негативные последствия для Российской Федерации.