



Королевство Бельгия
Директива от 08 декабря 2008 года № 2008/114/ЕС

О европейских критических инфраструктурах и мерах по их защите [рус., англ]

Принята
Советом Европейского Союза

ДИРЕКТИВА N 2008/114/ЕС

СОВЕТА ЕС О ЕВРОПЕЙСКИХ КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

И МЕРАХ ПО ИХ ЗАЩИТЕ <*>

(Брюссель, 8 декабря 2008 года)

(действие Директивы распространяется

на Европейское экономическое пространство)

<*> Перевод Зяблицовой В.А.

<*> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). Опубликовано в Официальном журнале (далее - ОЖ) N L 345, 23.12.2008, стр. 75.

Совет Европейского Союза,

руководствуясь Договором об учреждении Европейского сообщества, и, в частности, статьей 308 Договора,

на основании предложения Европейской комиссии,

руководствуясь Заключением Европейского парламента <*>,

<*> Заключение от 10 июля 2007 г. (еще не опубликовано в ОЖ).

на основании Заключения Европейского центрального банка <*>,

<*> ОЖ N C 116, 26.05.2007, стр. 1.

принимая во внимание следующие обстоятельства:

- 1) В июне 2004 г. Совет ЕС выступил с требованием о подготовке всеобщей стратегии по защите критических инфраструктур. В связи с этим 20 октября 2004 г. Европейская комиссия приняла Сообщение о защите критических инфраструктур в борьбе с терроризмом, в котором выдвинуты предложения относительно тех мер, которые будут способствовать готовности европейских стран к предотвращению и отражению террористических атак, затрагивающих критические инфраструктуры.
- 2) Семнадцатого ноября 2005 г. Европейская комиссия приняла Зеленую книгу Европейской программы по защите критических инфраструктур, предусматривающую стратегические варианты по утверждению программы, а также информационную сеть для предупреждений об угрозах критическим инфраструктурам. В отзывах на содержание Зеленой книги была подчеркнута первостепенная значимость рамок Сообщества по защите критических инфраструктур. Была признана необходимость повышения европейского потенциала к защите критических инфраструктур и содействия снижению их уязвимости. Особое значение было придано принципам субсидиарности, пропорциональности и комплементарности, а также сотрудничеству

заинтересованных субъектов.

- 3) В декабре 2005 г. Европейский совет по правосудию и внутренним делам призвал Европейскую комиссию выступить с предложением о принятии Европейской программы по защите критических инфраструктур ("ERCIP"), указывая, что в основе программы должен быть заложен принцип противостояния всем опасностям в условиях борьбы с угрозами терроризма. Данный принцип предусматривает, что в процессе защиты критических инфраструктур следует принимать во внимание опасности, связанные с деятельностью человека, технологические угрозы и природные катаклизмы, однако приоритетное значение должно быть придано угрозе терроризма.
- 4) В апреле 2007 г. Совет ЕС принял заключение относительно ERCIP, в котором подтвердил, что государства-члены ЕС несут окончательную ответственность за реализацию мер по защите критических инфраструктур в пределах их национальных границ; при этом Совет ЕС одобрил деятельность Европейской комиссии, связанную с усовершенствованием европейской процедуры выявления и установления европейских критических инфраструктур ("ECIs") и проведения оценки необходимости усиления их защиты.
- 5) Настоящая Директива представляет собой первый этап в поэтапном процессе выявления и установления ECIs и проведения оценки необходимости усиления их защиты. Так, объектом внимания настоящей Директивы являются энергетическая и транспортная отрасли, однако Директива должна быть пересмотрена с целью проведения оценки ее влияния и необходимости включения иных отраслей в сферу ее регулирования, *inter alia*, отрасли информационных и коммуникационных технологий ("ICT").
- 6) Основная и конечная ответственность по защите ECIs возлагается на государства-члены ЕС и владельцев/операторов таких инфраструктур.
- 7) В Сообществе существует определенное количество критических инфраструктур, нарушение или уничтожение которых окажет существенное трансграничное влияние. К таковым могут быть отнесены трансграничные межсекторальные последствия, вызванные взаимозависимостью связанных между собой инфраструктур. Такие ECIs должны быть выявлены и установлены в рамках общей процедуры. Оценка требований к безопасности таких инфраструктур должна быть произведена в соответствии с общим минимальным подходом. Двусторонние схемы сотрудничества между государствами-членами ЕС в сфере защиты критических инфраструктур предусматривают надежные и эффективные способы работы с трансграничными критическими инфраструктурами. Такое сотрудничество должно быть положено в основу ERCIP. Информация, связанная с присвоением статуса ECIs конкретной инфраструктуре, должна быть засекречена на соответствующем уровне в соответствии с действующим в Сообществе и государствах-членах ЕС законодательством.
- 8) Поскольку в различных отраслях накоплены специальные знания, опыт, установлены конкретные требования к защите критических инфраструктур, подход Сообщества к защите критических инфраструктур должен совершенствоваться и применяться с учетом отраслевых особенностей и мер защиты, отвечающих специфике существующих отраслей, включая меры, уже существующие в Сообществе, на национальном или региональном уровнях, а также заключенные ранее между владельцами/операторами критических инфраструктур трансграничные соглашения о взаимопомощи. Учитывая значительное участие частного сектора в осуществлении надзора и управлении рисками, планировании непрерывности деловых процессов и восстановлении после стихийных бедствий, подход Сообщества должен быть направлен на поощрение полноценного участия частного сектора.
- 9) Ввиду особенностей энергетической отрасли и, в частности, методов производства и передачи электроэнергии (в отношении электроснабжения), очевидно, что при наличии целесообразности процесс производства электроэнергии может частично включать передачу электроэнергии атомными электростанциями, за исключением отдельных электростанций, подпадающих под действие соответствующего атомного законодательства, в том числе соответствующих договоров и законодательства Сообщества.
- 10) Положения настоящей Директивы дополняют отраслевые меры, существующие на уровне Сообщества и в государствах-членах ЕС. Существующие в Сообществе механизмы должны использоваться и в дальнейшем, способствуя всеобщему применению настоящей Директивы. Следует избегать возникновения дублирования и противоречий между различными актами или положениями.
- 11) Операторские планы обеспечения безопасности ("OSPs") или иные эквивалентные меры, включающие определение наиболее важных активов, оценку степени риска, а также выявление, выбор и установление приоритетных встречных мер, должны присутствовать во всех установленных ECIs. Во избежание излишней работы и дублирования каждое государство-член ЕС должно в первую очередь установить, применяют ли владельцы/операторы установленных ECIs соответствующие OSPs или схожие меры. При отсутствии таких планов каждое государство-член ЕС обязано предпринять необходимые шаги, дабы убедиться, что соответствующие меры вводятся в действие. Каждое государство-член ЕС самостоятельно избирает надлежащую форму деятельности по учреждению OSPs.
- 12) Меры, принципы, руководства, включая меры Сообщества, а также двусторонние и/или многосторонние

схемы сотрудничества, предусматривающие план, эквивалентный или схожий с OSP, или предусматривающие назначение специалиста по обеспечению безопасности связи или эквивалентного специалиста, должны быть расценены как отвечающие требованиям настоящей Директивы в отношении OSP или специалистов по обеспечению безопасности связи соответственно.

- 13) Специалисты по обеспечению безопасности связи должны быть назначены во всех установленных ECIs в целях содействия сотрудничеству и обмену данными между соответствующими национальными органами власти по защите критических инфраструктур. Во избежание излишней работы и дублирования каждое государство-член ЕС должно в первую очередь установить, обладают ли владельцы/операторы установленных ECIs специалистами по обеспечению безопасности связи или эквивалентными специалистами. При отсутствии таких специалистов по обеспечению безопасности связи каждое государство-член ЕС обязано предпринять необходимые шаги, чтобы убедиться, что соответствующие меры вводятся в действие. Каждое государство-член ЕС самостоятельно избирает надлежащую форму деятельности по назначению специалиста по обеспечению безопасности связи.
- 14) Эффективное выявление рисков, угроз и уязвимых мест в отдельных отраслях требует осуществления взаимодействия между владельцами/операторами ECIs и государствами-членами ЕС, а также между государствами-членами ЕС и Европейской комиссией. Каждое государство-член ЕС должно вести учет сведений о ECIs, расположенных на его территории. Европейская комиссия должна получать от государств-членов ЕС общие сведения, касающиеся рисков, угроз и уязвимых мест в отраслях, где выявлены ECIs, включая соответствующую информацию о возможностях усовершенствования ECIs и межотраслевых взаимозависимостей; при необходимости такие сведения могут являться основой для разработки Европейской комиссией специальных предложений по совершенствованию защиты ECIs.
- 15) В целях содействия усилению защиты ECIs могут быть разработаны общие методики идентификации и классификации рисков, угроз и уязвимых мест в активах инфраструктуры.
- 16) Владелец/оператор ECIs должен быть предоставлен доступ в первую очередь соответствующими органами государства-члена ЕС, к наилучшим методикам и практикам работы по защите критических инфраструктур.
- 17) Эффективная защита ECIs требует взаимодействия, координации и сотрудничества на национальном уровне и внутри Сообщества. Наилучшим образом это может быть достигнуто посредством установления контактных центров по защите европейских критических инфраструктур ("контактные центры ECIP") в каждом государстве-члене ЕС, которое должно разрешать проблемы по защите европейских критических инфраструктур самостоятельно, а также при содействии иных государств-членов ЕС и Европейской комиссии.
- 18) В целях развития деятельности по защите европейских критических инфраструктур в сферах, требующих определенной степени конфиденциальности, в рамках настоящей Директивы необходимо обеспечить последовательный и безопасный информационный обмен. Следует учитывать, что правила конфиденциальности в соответствии с подлежащим применению национальным законодательством или Регламентом 1049/2001 Европейского парламента и Совета ЕС от 30 мая 2001 г. о всеобщем доступе к документам Европейского парламента, Совета ЕС и Европейской комиссии <*> должны соблюдаться в отношении отдельных сведений об активах критических инфраструктур, которые могут быть использованы при планировании или осуществлении действий, направленных на создание неприемлемых последствий для объектов критических инфраструктур. Секретная информация подлежит защите в соответствии с подлежащим применению законодательством Сообщества или государства-члена ЕС. Каждое государство-член ЕС и Европейская комиссия обязаны соблюдать степень секретности, установленную автором документа.

<*> ОЖ N L 145, 31.5.2001, стр. 43.

- 19) Обмен информацией, касающейся ECIs, должен осуществляться в атмосфере доверия и безопасности. Обмен информацией требует доверительных отношений, в рамках которых компании и организации могут быть уверены, что их секретные и конфиденциальные данные защищены надлежащим образом.
- 20) Поскольку цели настоящей Директивы, а именно создание процедуры выявления и установления ECIs, а также утверждение общего подхода к проведению оценки необходимости усиления защиты таких инфраструктур, не могут быть в полной мере достигнуты государствами-членами ЕС, и могут поэтому, в силу масштабности действий, быть в наилучшей степени достигнуты на уровне Сообщества, Сообщество вправе принимать меры в соответствии с принципом субсидиарности, установленным статьей 5 Договора. В соответствии с принципом пропорциональности, установленным в указанной статье, настоящая Директива не выходит за пределы, необходимые для достижения указанных целей.
- 21) Настоящая Директива признает основные права и соблюдает принципы, признанные, в частности, Хартией Европейского Союза об основных правах,

принял настоящую Директиву:

Статья 1

Предмет

Настоящая Директива устанавливает процедуру выявления и установления европейских критических инфраструктур (ECIs), а также общий подход к проведению оценки необходимости усиления защиты таких инфраструктур в целях содействия обеспечению безопасности населения.

Статья 2

Определения

Для целей настоящей Директивы:

- а) "критическая инфраструктура" означает активы, систему или ее часть, расположенные в государствах-членах ЕС, функционирование которых необходимо для решения наиболее важных социальных задач, обеспечения здоровья, безопасности, защиты, экономического или социального благополучия населения; нарушение или уничтожение таких инфраструктур способно вызвать значительные последствия для государства-члена ЕС в виде неспособности исполнения указанных функций;
- б) "европейская критическая инфраструктура" или "ЕСИ" означает критическую инфраструктуру, расположенную на территории государств-членов ЕС, нарушение или уничтожение которой способно вызвать значительные последствия, по крайней мере, для двух государств-членов ЕС. Значительность последствий оценивается в соответствии с межотраслевыми критериями. Это включает в себя последствия, возникающие в результате межсекторальной зависимости от других типов инфраструктур;
- в) "оценка рисков" означает рассмотрение соответствующих ситуаций, связанных с возникновением угроз, в целях проведения оценки уязвимых мест и потенциальных последствий нарушения или уничтожения критической инфраструктуры;
- г) "секретная информация о защите критической инфраструктуры" означает сведения о критической инфраструктуре, которые в случае их рассекречивания могут быть использованы в целях планирования или осуществления действий, направленных на нарушение или уничтожение объектов критической инфраструктуры;
- д) "защита" означает все виды деятельности, направленной на обеспечение функциональности, непрерывности работы и целостности критических инфраструктур в целях сдерживания, смягчения или нейтрализации угроз, рисков или уязвимости;
- е) "владелец/операторы ECIs" означает организации, ответственные за финансирование и/или ежедневное функционирование конкретных активов, системы или части системы, которым присвоен статус ЕСИ в соответствии с настоящей Директивой.

Статья 3

Выявление ECIs

1. В соответствии с процедурой, предусмотренной в Приложении III, каждое государство-член ЕС обязано выявлять потенциальные ECIs, которые отвечают межотраслевым и отраслевым критериям и соответствуют определениям, указанным в статье 2 "а" и "б".

По запросу государств-членов ЕС Европейская комиссия вправе оказывать помощь при выявлении ECIs.

Европейская комиссия вправе обратить внимание соответствующих государств-членов ЕС на наличие потенциальных критических инфраструктур, которые могут считаться отвечающими требованиям для присвоения статуса ЕСИ.

Все государства-члены ЕС, а также Европейская комиссия должны на постоянной основе продолжать деятельность по выявлению ECIs.

2. Межотраслевые критерии, указанные в параграфе 1, должны включать:
 - а) критерий по числу жертв (оценка производится с учетом количества потенциальных погибших или раненых);
 - б) критерий, связанный с экономическими последствиями (оценка производится с точки зрения значительности экономических потерь и/или степени ухудшения качества продуктов или услуг; включает возможные последствия для окружающей среды);
 - в) критерий воздействия на население (оценка производится с точки зрения воздействия на общественное доверие, физических мучений и нарушения повседневной жизни, включая утрату возможности

предоставления важных услуг).

Пороги межотраслевых критериев должны устанавливаться с учетом тяжести последствий в виде нарушения или уничтожения конкретной инфраструктуры. Четкие пороги, применимые к межотраслевым критериям, должны определяться в каждом конкретном случае на индивидуальной основе теми государствами-членами ЕС, интересы которых связаны с конкретной критической инфраструктурой. Каждое государство-член ЕС обязано ежегодно информировать Европейскую комиссию о количестве инфраструктур в каждой отрасли, в отношении которых проводились обсуждения о порогах межотраслевых критериев.

Отраслевые критерии должны учитывать особенности отдельных отраслей ЕС.

Европейская комиссия совместно с государствами-членами ЕС должна разработать руководство по применению межотраслевых и отраслевых критериев и примерных пороговых значений, предназначенных для использования в целях выявления ЕСИ. Критерии должны быть классифицированы. Использование такого руководства не является обязательным для государств-членов ЕС.

3. Действие настоящей Директивы распространяется на энергетическую и транспортную отрасли. Подотрасли определены в Приложении I.

При необходимости в случае пересмотра настоящей Директивы в соответствии со статьей 11 может быть установлено, что действие настоящей Директивы распространяется и на иные отрасли. В первую очередь это должно касаться отрасли ИСТ.

Статья 4

Установление ЕСИ

1. Каждое государство-член ЕС обязано информировать другие государства-члены ЕС, на которые ЕСИ может оказать существенное влияние, о выявлении такой ЕСИ и причинах возможного присвоения ей статуса ЕСИ.
2. Каждое государство-член ЕС, на территории которого располагается потенциальная ЕСИ, должно вступить в двусторонние и/или многосторонние переговоры с другими государствами-членами ЕС, на которые ЕСИ может оказать существенное влияние. Европейская комиссия вправе участвовать в таких переговорах, однако ей не предоставляется доступ к подробной информации, которая позволяет однозначно идентифицировать конкретную инфраструктуру.

Государство-член ЕС, имеющее основания полагать, что на его деятельность может оказать существенное влияние потенциальная ЕСИ, не идентифицированная в качестве таковой государством-членом ЕС, на территории которого она находится, вправе информировать Европейскую комиссию о своем желании участвовать в двусторонних и/или многосторонних переговорах по данному вопросу. Европейская комиссия обязана незамедлительно уведомить об этом государство-член ЕС, на территории которого располагается потенциальная ЕСИ, а также приложить все усилия для достижения соглашения между сторонами.

3. Государство-член ЕС, на территории которого располагается потенциальная ЕСИ, при присвоении ей статуса ЕСИ должно руководствоваться соглашением между государством-членом ЕС и государствами-членами ЕС, на которые ЕСИ может оказать существенное влияние.

Требуется согласие государства-члена ЕС, на чьей территории располагается инфраструктура, которой надлежит присвоить статус ЕСИ.

4. Государство-член ЕС, на территории которого располагается установленная ЕСИ, обязано ежегодно информировать Европейскую комиссию о количестве установленных инфраструктур в каждой отрасли, а также о количестве государств-членов ЕС, находящихся в зависимости от каждой установленной ЕСИ. Подробной информацией о ЕСИ вправе обладать только те государства-члены ЕС, на которые ЕСИ может оказать существенное влияние.
5. Государства-члены ЕС, на территории которых располагается ЕСИ, обязаны информировать владельца/оператора соответствующей инфраструктуры о присвоении ей статуса ЕСИ. Информация, связанная с присвоением статуса ЕСИ инфраструктуре, должна быть засекречена на соответствующем уровне.
6. Процесс идентификации и установления ЕСИ в соответствии со статьей 3 и настоящей статьей должен быть завершен к 12 января 2011 г. Его результаты должны регулярно пересматриваться.

Статья 5

Операторские планы обеспечения безопасности

1. Процедура, предусмотренная операторским планом обеспечения безопасности ("OSP"), должна быть направлена на выявление важных активов ЕСИ и мер безопасности, существующих или применяемых для их защиты. Минимальное содержание процедуры, предусмотренной OSP ЕСИ, установлено в Приложении II.

2. Каждое государство-член ЕС должно выяснить, предусмотрены ли при каждой установленной ЕСІ, расположенной на его территории, OSP или иные эквивалентные меры, направленные на решение задач, указанных в Приложении II. В случае если государством-членом ЕС установлено, что такой OSP или эквивалентные меры существуют и регулярно обновляются, необходимость в осуществлении дальнейших действий отсутствует.
3. В случае если государством-членом ЕС установлено, что такой OSP или эквивалентные меры не подготовлены, оно обязано любыми надлежащими способами обеспечить подготовку OSP или эквивалентных мер, направленных на решение задач, указанных в Приложении II.

Каждое государство-член ЕС обязано обеспечить наличие OSP или эквивалентных мер, а также их регулярный пересмотр по истечении года с момента присвоения критической инфраструктуре статуса ЕСІ. В исключительных случаях указанный срок может быть увеличен при согласии уполномоченного органа государства-члена ЕС и с уведомлением Европейской комиссии.

4. Действие данной статьи не распространяется на существующие соглашения об осуществлении контроля или надзора в отношении ЕСІ, и соответствующий уполномоченный орган государства-члена ЕС, указанный в данной статье, осуществляет контроль в рамках существующих соглашений.
5. Соблюдение всех мер, включая меры Сообщества, которые связаны с требованием или указанием на необходимость присутствия в конкретной отрасли плана, эквивалентного или схожего с OSP, и осуществления соответствующим уполномоченным органом надзора за соблюдением такого плана, должно быть расценено как исполнение требований государств-членов ЕС, принятых в соответствии с настоящей статьей или установленных ею. Руководство по применению, указанное в статье 3 (2), должно содержать примерный перечень таких мер.

Статья 6

Специалисты по обеспечению безопасности связи

1. Специалист по обеспечению безопасности связи должен выступать в качестве связующего звена между владельцем/оператором ЕСІ и уполномоченным органом соответствующего государства-члена ЕС для разрешения вопросов безопасности.
2. Каждое государство-член ЕС должно выяснить, предусмотрен ли при каждой ЕСІ, расположенной на его территории, специалист по обеспечению безопасности связи или иной эквивалентный специалист. В случае если государством-членом ЕС установлено, что такой специалист по обеспечению безопасности связи или иной эквивалентный специалист существуют, необходимость в осуществлении дальнейших действий отсутствует.
3. В случае если государством-членом ЕС установлено, что такой специалист по обеспечению безопасности связи или иной эквивалентный специалист отсутствуют, оно обязано любыми надлежащими способами обеспечить назначение такого специалиста по обеспечению безопасности связи или иного эквивалентного специалиста.
4. Каждое государство-член ЕС обязано имплементировать надлежащий механизм коммуникации между уполномоченным органом соответствующего государства-члена ЕС и специалистом по обеспечению безопасности связи или иным эквивалентным специалистом в целях обмена соответствующей информацией, касающейся выявленных рисков и угроз в отношении ЕСІ. Такой механизм коммуникации должен применяться без ущерба действию национальных требований о доступе к секретной и конфиденциальной информации.
5. Соблюдение всех мер, включая меры Сообщества, которые связаны с требованием или указанием на необходимость присутствия в конкретной отрасли специалиста по обеспечению безопасности связи или эквивалентного специалиста, должно быть расценено как исполнение требований государств-членов ЕС, принятых в соответствии с настоящей статьей или установленных ею. Руководство по применению, указанное в статье 3 (2), должно содержать примерный перечень таких мер.

Статья 7

Отчетность

1. Каждое государство-член ЕС обязано провести оценку угрозы в отношении подотраслей ЕСІ в течение одного года с момента присвоения критической инфраструктуре на его территории статуса ЕСІ в рамках указанных подотраслей.
2. Каждое государство-член ЕС обязано раз в два года в краткой форме предоставлять Европейской комиссии общие данные о типах рисков, угроз и уязвимых местах, выявленных в каждой отрасли ЕСІ, которой присвоен статус ЕСІ в соответствии со статьей 4 и которая находится на его территории.

Единый шаблон для предоставления такой отчетности может быть разработан Европейской комиссией при

содействию государств-членов ЕС.

Каждый отчет должен быть засекречен на соответствующем уровне в порядке, который сочтет необходимым подготовившее его государство-член ЕС.

3. На основании отчетов, указанных в параграфе 2, Европейская комиссия и государства-члены ЕС на отраслевой основе должны установить, существует ли необходимость в рассмотрении возможности принятия на уровне Сообщества дополнительных мер защиты в отношении ECIs. Этот процесс должен осуществляться в порядке пересмотра настоящей Директивы в соответствии со статьей 11.
4. Европейская комиссия при содействии государств-членов ЕС может разработать общее методологическое руководство по проведению оценки рисков в отношении ECIs. Использование такого руководства не является обязательным для государств-членов ЕС.

Статья 8

Поддержка ECIs Европейской комиссией

Европейская комиссия должна, действуя через уполномоченные органы соответствующего государства-члена ЕС, оказывать поддержку владельцам/операторам установленных ECIs посредством предоставления им доступа к наилучшим методикам и практикам работы по защите критических инфраструктур, а также должна содействовать обучению и обмену информацией о новых технических разработках, касающихся защиты критических инфраструктур.

Статья 9

Секретная информация о защите критической инфраструктуры

1. Любое лицо, осуществляющее обработку конфиденциальной информации от имени государства-члена ЕС или Европейской комиссии, должно пройти проверку безопасности соответствующего уровня.

Государства-члены ЕС, Европейская комиссия и соответствующие органы контроля должны гарантировать, что секретная информация о защите европейской критической инфраструктуры, переданная государствам-членам ЕС или Европейской комиссии, не используется ни для каких иных целей, помимо осуществления защиты критической инфраструктуры.

2. Положения настоящей статьи применяются также к неписьменной информации, обмен которой был осуществлен в ходе переговоров, где обсуждались секретные вопросы.

Статья 10

Контактные центры по защите

европейской критической инфраструктуры

1. Каждое государство-член ЕС должно учредить контактный центр по защите европейской критической инфраструктуры (контактный центр ECIP).
2. Контактные центры ECIP должны отвечать за координацию вопросов по защите европейской критической инфраструктуры внутри государства-члена ЕС с иными государствами-членами ЕС и с Европейской комиссией. Учреждение контактных центров ECIP не препятствует участию иных уполномоченных органов государства-члена ЕС в решении задач по защите европейской критической инфраструктуры.

Статья 11

Пересмотр

Пересмотр настоящей Директивы должен быть начат 12 января 2012 г.

Статья 12

Имплементация

Государства-члены ЕС должны до 12 января 2011 г. принять необходимые меры во исполнение настоящей Директивы. Они должны незамедлительно проинформировать Европейскую комиссию о принятых мерах и сообщить текст принятых актов и их корреляцию с положениями настоящей Директивы.

Принятые нормативные правовые акты должны содержать ссылку на настоящую Директиву или должны сопровождаться такой ссылкой в случае их официального опубликования. Способы размещения такой ссылки устанавливаются государствами-членами ЕС.

Статья 13

Вступление в силу

Настоящая Директива вступает в силу на двадцатый день с момента ее опубликования в Официальном журнале Европейского Союза.

Статья 14

Адресаты

Настоящая Директива адресована государствам-членам ЕС.

Совершено в Брюсселе 8 декабря 2008 г.

От имени Совета ЕС

Председатель

в. KOUCHNER