доц. Ладислав Хофрейтер
Жилинский Университет

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА – СОДЕРЖАНИЕ, СТРУКТУРА И ПРОБЛЕМЫ ЕЕ ЗАЩИТЫ

Введение

Понятие инфраструктура известен прежде всего в хозяйственной сфере и значит совокупность сооружений, учреждений, в частности отраслии транспорта и коммуникационных сетей необходимых для обеспечения надлежащего хода организаций и производства данной страны, напр. железные дороги, маршруты, мосты, аэродромы, порты, энергетические и мелиорационные оборудования, телефон, телеграф, радио, телевидение итп.

В каждом обществе можем отождествлять секторы, системы или сети, от которых жизненно зависит общество и нарушение которых могло бы первенствовать в коллапс на общегосударственном, региональном или местном уровне. Комплекс этих секторов, систем или сетей начался называть **критическая инфраструктурап** (Hofreiter, L. a kol., 2013).

1. Понятие критическая инфраструктура

В связи с наращиванием угроз терроризма начались с 1998-ого года в развитых странах дискуссии об уязвимости национальных инфраструктур. Анализы были направленны не только на кибернетические инфраструктурные системы, но и на остальные области и секторы обеспечения жизни общества. В США v Presidential Decision Directive 63 (1998) определили критическую инфраструктуру как основные системы, которые могут имет материальную или виртуальную платформу и имеют воздействие на функциональность экономики государства. Эти основные системы вбирали в себя системы телекоммуникации, энерго-системы, банковый и финансовый сектор и службы, транспортную систему, снабжение водой и спасательные службы.

ISSN: 1898-4509

Вопросами критической инфраструктуры на национальном уровне начались с 1998-ого года заниматься и европейские государства. Общественным знаменателем этих деятельностей было прежде всего особое значение на охрану информационных и коммуникационных технологий.

В Европе проблематикой критической инфраструктуры начались раньше всех заниматься в Великобритании, где на конце 1999-ого года была определенна критическая национальная инфраструктура как системы, которых преемственность важна для функционирования государства, затрата или нарушение которых имело бы или могло бы подвергать угрозе жизнь граждан, могло бы нанести серьёзные негативные экономические или социальные следствия для общества или её крупной части. Между такие системы были включенные государственное управление, запасные службы, заготовка энергиямши и топливами, подача воды, телекоммуникации, заготовка продовольствием, санитария, финансы и экономика, коммуникационные сети и службы, юстиция и защита общественного порядка, социальные обслуживания, образование, наука и испытание, но и прогноз погоды.(Linhart, Richter, 2003).

В результате террористических нападений на обьекты в США, к которым произошло 11.9.2001, приняла проблематика критической инфраструктуры и ее защита новый объем и масштаб. Во февралье 2003-ого года была v США принята Национальная стратегия физической охраны критической инфраструктуры и ключевых сооружений (The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003), в которой критическая инфраструктура была определенна как системы и оборудования, так материальные, как и виртуальные, которые жизненно важные для США и повреждение или разрушение таких систем имело бы влияние на уменьшение безопасности, национальной экономической безопасности, национального общественного здравоохранения или безопасности, или на любую их комбинацию. Между секторы критической инфраструктуры были включенны: сельское хозяйство, продовольствие, вода, публичное здравоохранение, запасные (спасательные) службы, базы оборонной промышленности, телекоммуникации, энергетика, транспорт, банковое дело и финансы, химическая промышленность и опасные вещества, почтовое обслуживание. Между ключевые оборудования были зачисленны национальные культурные памятники, ядерные электростанции, пдотины (дамбы), правительственные оборудования, коммерческие ключевые оборудования и другие места, где концентрируется большое количество особ.

Соединение народных экономик членских государств ЕС, их взаимозависимость, но и необходимость противостоять совместным или подобным угрозам, отразились в принятии документа Critical Infrastructure Protection in the fight against terrorism. В этом документе критическая инфраструктура определенна как физические оборудования, информационные технологии, сети (транспортные, энергетические и т.п.), службы и другие актива, которых расстройство или разрушение имело бы серьёзные следствия на здоровье, охрану, надёжность или жизненный уровень граждан или штатное функционирование правительств v членских государствах.

В ЕС была также определённая критическая инфраструктура ЕС,которая будет состоять из тех физических ресурсов, услуг и информационно-технических средств, сетей и инфраструктурных активов, которые, если будут нарушенны или уничтожены, будут иметь серьезные последствия для здоровья, безопасности и социально-экономического благополучия двух или более государств-членов ЕС.

Словацкая Республика приняла Национальную программу защиты и обороны критической инфраструктуры (Národný program..., 2007). Как критическая инфраструктура отмечается та доля национальной инфраструктуры (выбранные организации и учреждения, объекты, системы, оборудования, системы обслуживания), которой разрушение или ущемление в результате воздействия рисковых факторов поставить под угрозу или причинит нарушение политического и экономического хода государству или угрожать жизни и здоровья населения . Составной частью критической инфраструктуры являются тоже объекты оборонной инфраструктуры.

В 2011 г. был принят в Словакии Закон об критической инфраструктуре. В этом Законе определенно, что критическая инфраструктура состоит из элементов, подрыв или разрушение будут иметь серьезные неблагоприятные последствия для осуществления экономических и социальных функций государства, и, следовательно, качества жизни, защиты жизни, здоровья, безопасности, имущества и окружающей среды (Zákon 475/2011).

Значит, мы можем совершить обобщение, что критические инфраструктуры включают в себя физические объекты, ресурсы, услуги и информационно-технические средства, сети и других инфраструктурных активов, которые, если нарушены или уничтожены, будут иметь серьезные последствия для здоровья,

безопасности или экономического благосостояния граждан или эффективного функционирования правительства.

2. Структура критической инфраструктуры

Критическая инфраструктура представляет собой систему, которая состоит из секторов и элементов.

Сектором критической инфраструктуры (Šimák, 2012) называется таков сектор национальной инфраструктуры, у которого отказ некоторой его важных функцией или некоторого его элемента, прежде всего следствием террористического нападении, поставить под угрозу или причинит нарушение некоторой из областей безопасности государства, напр.:

- политического хода государства, в том числе функционирования общественного управления,
- обороны государства,
- работы хозяйства государства,
- жизни, здоровья или имущества населения,
- транспорта, информационных и коммуникационных систем,
- бытовой среды.

Это определение изъявляет содержание и значимость критической инфраструктуры не только для функционирования государства во время нормальных условий, но и в кризисных ситуациях, которые могут быть вызванны преднамеренно или непреднамеренно, внешними или внутренними, натуральными, технологическими или социальными деятелями.

Между секторы критической инфраструктуры входят (COM 702):

- энергетические оборудования и сети, напр. электрические распределительные сети, газопроводы, нефтепроводы, сборники горючего и т.п.,
- коммуникационные и информационные технологии, напр. телекоммуникации, радиовещательные и телевизионные передатчики и сети, интернет, другие информационные сети, и т.п.,
- финансовая система, напр. банковое дело, капиталовые рынки, инвестирование и т.п.,
- здравоохранение, особенно больницы, поликлиники, снабжение кровью, лаборатории, сантехнический а спасательные службы,

- продукты, напр . пищевая промышленность, сельское хозяйство, торговля а снабжение продовольствием,
- вода, особенно дамбы, гидроресурсы, обрядка и снабжение водой,
- транспорт, особенно авиационный, шоссейный, железнодорожный, комбированный коммуникационные узлы, но и системы управления транспортом,
- производство, хранение и транспорт опасных товаров, особенно химических, биологических , радиологических ядерных материалов,
- государственное управление, в частности критические службы и оборудования, информационные сети, важные экономические объекты, стратегические объекты , но и культурные памятники.

Критериями для разрешение о том, можем ли данный инфраструктурных элемент определить как критический, являются:

- территориальная досягаемость негативных результатов, напр. Транснациональный (через-граничный), народный, региональный, локальный (местный) и т.п.
- крупность последствий, напр. гуманитарных, материальных, экономических, политических или ущербы и потери по отношению к окружающей среде,
- временной эффект последствий, особенно когда появятся негативные следствия (напр. немедленно, за 24 ч. ит.п.) и как долго могут продолжаться (напр. до 24 часов, до 3 дней и т.п.) (COM 576, COM 702).

3. Защита критической инфраструктуры

Понятие защита может восприняты разных значение. Наиболее общее значение этого термина, означает забота о предотвращение опасность, разный вредный влияние среды, z окресности социального субъекта или материального объекта, которые могут поставить под угрозу его безопасность. Мы можем защиту изучать v двоих её основных значениях:

- защита как деятельность, целью которой является обеспечение безопасности объектов защиты,
- защита как средство, или же системное упорядочение средств на обеспечение безопасности объектов защиты.

Защиту критической инфраструктуры (Critical Infrastructure Protection) можем определить как совокупность мероприятий, которые планируются и выполняются с целью:

- опознать и защищать эти секторы инфраструктуры государства, которые являются критическими с точки зрения сохранения их безопасности, функциональности, экономической и общественной стабильности, причём необходимо равноценно оценивать как государственную, так и приватную сферу,
- обеспечить функциональность системы раннего предупреждения появления кризисных ситуаций и защиту той инфраструктуры, которая важна для решения кризисных ситуаций.

Пойдёт прежде всего об секторы критической инфраструктуры, которые являются важными с точки зрения:

- обеспечения правильного функционирования правительства, органов государственного управления и самоуправления, преимущественно в области безопасности и обеспения основных (жизненных) товаров и служб,
- функциональности государственной и приватной сферы рпи обеспечивании правильного хода экономики и осуществлении общественных служб,
- обеспечения внутренного порядка, общественной стабильности и безопасности граждан.

Защищение критической инфраструктуры будет выполняться всегда как результат аналитического процесса, которого содержание состоит из:

- идентификации областей и секторов критической инфраструктуры на национальном, региональном и локальном уровне,
- идентификации релевантных рисков для секторов критической инфраструктуры,
- анализа уязвимости отдельных секторов критической инфраструктуры,
- оценки рисков нарушения или уничтожения секторов критической инфраструктуры,
- принятия соответствующих предохранительных мероприятий, т.е. в создании системы защиты критической инфраструктуры.

4. Анализ рисков критической инфраструктуры

Ключевым фактором оказывается идентификация и оценка риска. Под понятием риск (Р) воспринимаем вероятность (В), что наступит негативное событие и из него явствующий ущерб (У) или затрата:

$$P = BxY \qquad (1)$$

Вероятность того, что наступит негативное событие, выражаем путём определения величины:

- уязвимости объекта,
- угрозы для объекта.

Под **уязвимостью** объекта понимается степень его незащищенности от внешних и/или внутренних угроз. Для оценки уязвимости мы должны образовать модель угроз и и системы защиты. Эти два фактора далее сопоставляем и качественно оцениваем. Уязвимость будет:

- малая (м), если угроза не способна преодолеть систему защиты и нанести объекту ущерб,
- средняя (с), если имеется какая-нибудь возможность, что угроза преодолеет систему защиты и изыщет возможность доступа к объекту,
- большая (б), если имеющая система защиты недостаточно способна предупредить подступ угроз к объекту.

Угрозы – это события социального свойства, находившиеся в внешней и/или внутренной окружающей среде объекта, которые способны вызвать негативные события, нанести ущерб и потери.

Значительность угрозы определяем путём высказывания отношений следующих факторов:

- существование источника угрозы,
- существование причины проявления угрозы или мотивов злоумышленных несанкционированных действий,
- существование случайев угрозы в прошлом.

Способ конечной оценки угрозы показано в таблице 1.

Табл. 1. Матрица оценки угрозы

Существование источника угрозы	Существование причин или мотивов	Существование случайев угрозы в прошлом	Оценка угрозы
Да	Да	Да	Большая (Б)
Да	Да	Нет	Большая (Б)
Да	Нельзя точно определить	Нет	Средная (С)
Да	Нет	Нет	Малая (М)
Нельзя точно определить	Нет	Нет	Малая (М)
Нет	Нет	Нет	угроза отсутствует (0)

Для определения величины риска мы должны определить величину **последствий (ущерба)** негативного события. Примерами категорий ущерба являются:

- **нематериальный ущерб**, когда последствиями будут нравственные, человеческие или информационные потери,
- **материальный ущерб**, когда последствиями будут материальные (финансовые) потери соответствующих масштабов.

Ущерб (**У**) негативного события мы определяем в зависимости от установленной системы оценки ущерба как **малый, средний** или **большой**.

Для оценки величины риска применяем таблицу или матрицу. Чаще всего используем отношение и контекст между определёнными факторами риска: *ущерб, уязвимость и угрозы*. Решающую роль при оценке величины риска имеет экспертная оценка отношения между этими факторами. Величие риска можем определить как **очень малый (ОМ), малый (М), средний (С), большой (Б), очень большой (ОБ)** риск**.**

Величина риска, которую получим из таблицы 2, будет пересечение величины ущерба, угрозы и уязвимости. Например, если будет величина ущерба средняя (С), угрозы малая (М) и уязвимости большая (Б), результирующая величина риска будет малая (М).

Табл. 2. Матрица для оценки риска

Ущерб	Угроза								
	М			С			Б		
	Уязвимость								
	М	С	Б	М	С	Б	М	С	Б
М	ОМ	ОМ	ОМ	ОМ	М	М	М	М	М
С	ОМ	М	М	М	С	С	С	Б	Б
Б	М	М	С	С	Б	Б	Б	ОБ	ОБ

5. Система защиты

Защита критической инфраструктуры представляет совокупность организационных и технических мер на обеспечение защиты секторов критической инфраструктуры от разных угроз (террористов, диверсантов, экстремистов), в случае появления чрезвычайных или кризисных ситуаций, да и от последствий непреднамеренных действий, которые могли бы нанести ущербы для критической инфраструктуры.

Современные СЗ строятся на базе применения различных средств и содержат следующие основные составные части (подсистемы):

- механические барьеры, ограждения, ворота, решетка и под.
- система контроля и управления доступом (СКУД),
- система охранной сигнализации (СОС),
- система телевизионного наблюдения (СТН),
- организационные мероприятия,
- служба охраны /силы реагирования.

Система физической защиты – это интегрированный комплекс реальных элементов, деятельностей и процессов, логично и функционально упорядоченных таким способом, что она создавает орудие для обеспечения безопасности объектов критической инфраструктуры в определёное время и в данным пространстве. С точки зрения системного подхода мы можем её считать синергической системой с целевым поведением.

Желаемые функции системы физической защиты являются:

- **отпугивать** потенциальных нападающих от нападении на охраняемый объект,
- **детектирование** нарушения охраняемых объектов, помещений, зон, или детектирование возникновения опасной обстановки в объекте, или же его близкой окрестности,
- **задержка** движения атакующих,
- **реакция** на нарушение охраняемых объектов, пространств или зон, с целю недопустить подступ атакующих к охраняемым объектом, простором или зонам, недопустить поставить под угрозу объект, его функций или личности в объекте.

Заключение

Критической инфраструктурой будем понимать все материяльые объекты, физические ресурсы, услуги, информационно-технические системы, сети и все остальные инфраструктурные компонеты, которых нарушение или уничтожение серьезно влияет на состаяние безопасности людей, предрпиятий, национальной экономики и систему управления государства.

Эффективная система защиты критической инфраструктуры должна успешно противостоят различным угрозам рпи адекватном уровне охранных мер, в зависимости от значения сектора критической инфраструктуры, потенциальных угроз и их возможных последствий.

Анализ риска является исходным этапом процесса проектирования системы защиты. Зависит от качества проведения анализа, будет ли система защиты эффективной, докажет ли успешно сопротивляться всем угрозам, которые могут нарушить безопасность объекта критической инфраструктуры.

Эффективная система защиты критической инфраструктуры должна успешно противостоят различным угрозам рпи адекватном уровне охранных мер, в зависимости от значения сектора критической инфраструктуры, потенциальных угроз и их возможных последствий. Защита секторов/ объектов критической инфраструктуры будет выполняться всегда, коли оценка риска будет боьшая, чем приемлемый (акцептованный) риск.

Целью принимаемых предохранительных мероприятий будет снизить риск нарушения или уничтожения объектов критической инфраструктуры на приемлемую (акцептованную) степень.

Литература

COM(2005) 576 final: Green paper: *On a European Programme for Critical Infrastructure Protection*, Brussels, 17.11.2005

COM (2004) 702 final: *Critical Infrastucture Protection in the fight against Terrorism*, Communication from the Commision to the Council and the European Parlaiment, Brusseles, 20.10.2004

Hofreiter, L. a kol. (2013): *Ochrana objektov kritickej dopravnej infraštruktúry*, Žilinská univerzita v Žiline/EDIS, Žilina

Linhart, P., Richter, R. (2003): *Ochrana kritické infrastruktury*, http.//www.mvcr.cz/casopisy/112/3_2003/linhart.html

Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike (2007): http://www.minv.sk/?ochrana-kritickej-infrastruktury.

Presidential Decision Directive 63 (1998), https://www.fas.org/irp/offdocs/pdd/pdd-63.htm

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, http://www.whitehouse.gov/pcipb/physical.html

Šimák, L. a kol. (2012): *Ochrana kritickej infraštruktúry v sektore dopravy*, Žilinská univerzita v Žiline/ EDIS, Žilina

Zákon 475/2011 Z.z. o kritickej infraštruktúre, http://www.zbierka.sk

Статья была написана в рамках решения проекта APVV-0471-10 Critical Infrastructure Protection In Sector Transportation

Ladislav Hofreiter

Critical infrastructure – content, structure and problems of its protection

Abstract

Security, economic and social stability of the country, its functionality but also protecting the lives and property of citizens are dependent on the proper functioning of many infrastructure systems of state. Disruptions, lack or destruction of such systems, institutions, facilities and other services could cause disruption of social stability and national security, provoke a crisis situation or seriously affect the operation of state and local governments in crisis situations. This is known as critical infrastructure. It is in the interest of the State to the critical infrastructure effectively protected.

Key words: *Critical Infrastructure, critical infrastructure protection, sectors, physical protection system*