АКТУАЛНИ ПРОБЛЕМИ ЗА СИГУРНОСТТА НА ЕЛЕКТРОННАТА КРИТИЧНА ИНФРАСТРУКТУРА

Докторант Десислава Панчева Стоева
Университет по библиотекознание и информационни технологии

CURRENT PROBLEM OF SECURITY OF ELECTRONIC CRITICAL INFRASTRUCTURE

Desislava Stoeva

Abstract: *The article examines the scientific and theoretical problems relating Up to clarify the relevance of issues related to critical infrastructure.*

Key words: *Infrastructure, e- infrastructure, security*

Терминът „инфраструктура“ е въведен през XIX в. от швейцарския военен теоретик Антуан-ХенриЖоминин, който изтъква стратегическото и оперативното й значение за ръководство на бойните действия. Постепенно терминът „инфраструктура“ започва да се използва в икономическата теория и теорията на управлението. Понастоящем той се прилага широко в компютърните науки, икономическата география и в изследванията на сигурността. В края на XX в. защитата на критичната инфраструктура е съществен елемент от политиката за сигурност на много страни, най-вече в страните членки на НАТО и ЕС. Това е свързано, от една страна, с процеса на глобализация, а от друга с борбата срещу международния тероризъм. А от своя страна критичната инфраструктура е система от съоръжения, услуги и информационни системи, чието спиране, неизправно функциониране или разрушаване би имало сериозно негативно въздействие върху здравето и безопасността на населението, околната среда, националното стопанство или върху ефективното функциониране на държавното управление[1]. Критична инфраструктура има в някои сектори като: енергетика; ядрена промишленост; информационни и комуникационни технологии; водоснабдяване; осигуряване с хранителни продукти; здравеопазване; финансова сфера; транспорт; химическа промишленост; космически капацитет; научен капацитет, както и други сектори, които някои държави считат важни такива. Обекти на критичната инфраструктура в тези сектори са: атомните електрически централи, оръжейната промишленост, водоснабдителните и водноелектрическите централи, автоматизираните канализационни системи, болници и болнична апаратура както и други обекти, при които нарушаването на работата на автоматизираните им системи може да доведе до бедствие или авария, която би застрашила важните общочовешки интереси и ценности. Като жизненоважни интереси в Стратегията за национална сигурност на Република България са записани: гарантиране на правата, свободите, сигурността и благосъстоянието на гражданина, обществото и държавата; запазване на суверенитета, териториалната цялост на страната и единството на нацията; защита на конститу-

[1] Закон за управление при кризи, Допълнителна разпоредба, § 1, т.8.

ционно установения ред и демократичните ценности; защита на населението и критичната инфраструктура при кризи, бедствия, аварии, катастрофи и други рискове и заплахи; съхраняване и развитие на националната идентичност, изграждаща се на основата на единно гражданство; гарантиране интегритета на българското гражданско общество; преодоляване на негативните демографски процеси, на значителните диспропорции в развитието на регионите и изграждане на социално-икономическа среда, осигуряваща условия за развитието на поколения български граждани, способни да гарантират на Република България достойно място в ЕС и в световните политически, икономически, финансови и социални процеси[2]. Имайки предвид, че Република България се намира в Европа и принадлежи към ЕС[3] и политиката на ЕС за споделените ценности разбираме, че това са основните жизненоважни европейски интереси. Използването на автоматизирани системи в критичната инфраструктура е неделима част от нея в съвременния живот, но и я прави много уязвима за злонамерени лица, организации дори и правителства. През юли 2010 година немската компания Siemens установява, че нов (за времето си) вирус атакува индустриалните тайни в Siemens SCADA системите. Експерти по сигурността смятат, че вирусът е зловреден софтуер, проектиран да се промъкне в системите, използвани за пускане в действие на фабрични линии и части от критична инфраструктура. Този вирус се разпространява не само чрез интернет, но и като се самокопира на всяко USB флаш устройство, което бъде поставено в USB порта на заразена машина. След поставянето на флашката вирусът сканира системата SiemensWinCC или друго USB устройство и ако засече софтуер на Siemens, веднага се опитва да се свърже, ползвайки парола по подразбиране. В противен случай не прави нищо и така ние не разбираме, че устройството или машината са заразени.[4] В този случай според специалисти изследвали зловредния софтуер, вирусът е използван за кражба на тайни от заводи и други индустриални обекти, но вируи от този тип могат да бъдат използвани и за значително по – опасни за човечеството цели. Тъй като софтуер от този тип може да поеме контрола над SCADA системите в критичната инфраструктура, той може и да предизвика инцидент, който да извади системата от устойчивото и състояние и по този начин да доведе до разрушаването на производствения цикъл в определен обект. Много опасно би било такъв софтуер, попаднал в ръцете на „неподходящи“ хора, да порази обект на критичната инфраструктура като например АЕЦ. Политиката на ЕС по ЗКИ се развива много динамично след 2004 г. в контекста на борбата срещу международния тероризъм. От институционална гледна точка политиката на ЕС по защита на критичната инфраструктура (ЗКИ) се координира от Главна дирекция „Правосъдие, свобода и сигурност” на Европейската Комисия. През ноември 2005г. Европейската Комисия приема т.нар. Зелена книга за Европейска програма за ЗКИ. В Зелената книга за първи път на общностно ниво се дава дефиниция на понятието “критична инфраструктура” и се предлага препоръчителен списък на секторите от критичната инфраструктура. Освен термина „национална критична инфраструктура”, авторите на Зелената книга утвърждават и термина „Европейска критична инфраструктура. За постигането на удовлетворителни резултати е необходимо да бъдат ясно формулирани задачите, които трябва да се решават за оценяване и планиране на защитата на критичната инфраструктура. Освен това трябва да бъдат обмислени средствата за защита на критичната инфраструктура от кибер атаки, за да може практическата реализация на политиките да от-

[2] Стратегия за национална сигурност на Република България.

[3] Европейски съюз.

[4] http://computerworld.bg/31081_nov_virus_atakuva_industrialni_tajni_v_siemens_sca

говори на очакванията, заложени в хода на процесите по прогнозиране и планиране. Един национален подход за справяне със заплахите има за цел да бъде изготвена стратегия за реагиране на база на вече предварително направените анализи и оценки. Критичната инфраструктура съдържа системи, мрежи активи и обекти които осигуряват стоки и услуги, необходими за нормалното функциониране на обществото. Всяко прекъсване било то в обект или сектор от системата би имало сериозно негативно влияние върху националната и икономическата сигурност.

Суверенитетът, сигурността и независимостта на държавата се определя от стабилното и непрекъснато функциониране на критичната инфраструктура. Тя се характеризира със силна степен на уязвимост от страната на множество заплахи. Всеки сектор, включен в състава й, се намира в тясна зависимост и взаимозависимост с останалите сектори и обекти от инфраструктурата. В България критичната инфраструктура съдържа 19 сектора,които са част от националното стопанство на страната

(Енергетика, Транспорт, Телекомуникации, Здравеопазване,Земеделие и храни; Околна среда; Финанси и банково дело и др.). Всяка повреда или прекъсване в нормалното им функциониране би довело до сериозни негативни последици за обществената безопасност и националната сигурност на страната. През последните години защитата на критичната инфраструктура започва да се превръща в част от националната политика за сигурност на всяко модерно и бързо развиващо се общество. Същевременно някои аварии и инциденти, които се случват в нейни обекти оставят впечатление, че мерките предприети за нейната защита, не са достатъчно ефективни. Актуалността на проведеното научно изследване се определя от следните групи фактори: - отсъствие на адекватна нормативна база защитата на критичната инфраструктура в България се регламентира от Закон за защита при бедствия, Наредба на Министерски съвет за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и рисковете за тях. Съществуват и допълнителни нормативни документи, които имат пряко отношение към защитата на инфраструктурата. Нормативната база в България към момента не е достатъчна да гарантира сигурността на инфраструктурата; липса на секторен анализ процесът на защита на критичната инфраструктура изисква провеждането на секторен анализ определяне секторите и обектите на инфраструктурата, които да отговарят на определени критерии за критичност; отсъствие напартньорство между участниците в процеса на защита на критичната инфраструктура критичнатаинфраструктура съдържа множество мрежи и активи, обединени в сектори, които са собственост или се контролират от редица министерства, ведомства, агенции и др. Мерките за укрепване и поддържане на сигурна, функционираща и устойчива критична инфраструктура са от първостепенна важност за националната сигурност като цяло. След като уточнихме какво представлява киберсигурност, критична инфраструктура и неограничените възможности в областта на автоматизираните системи и влияние върху тях, трябва ясно да се дефинират задачите, които трябва да се решат за оценяване и планиране на защитата на критичната инфраструктура. Задачите могат да бъдат обединени в няколко групи: оценка и представяне на заплахите; оценка на уязвимостта; оценка на негативни въздействия; формиране на политики за защита на критичната инфраструктура; стратегическо управление и вземане на решения за инвестиране в защитата на критичната инфраструктура. Всяка нова заплаха за сигурността на глобалния свят, в който живеем, изисква време за адекватно противодействие. Кибер атаките са една от най-новите и най-усъвършенствани заплахи за сигурността на всеки един елемент на сигурността (индивида, групата от индивиди (общността), нацията (държавата), региона (групата от държави) и целия свят). Това е важно основание, към което би трябвало да се отне-

сем отговорно, за да изградим политики за защита от кибер атаки. Факта, че кибер атаките са едно глобално явление ни показва, че за една държава би било трудно сама да изгради политика за защита, както и да осъществи тази политика. Тук идва ролята на съюзите. Организациите на европейския съюз са тези, които имат за задача да изградят политики и нормативни бази за запазването на нормалното развитие на държавите членки, както и за запазването на сигурността в едно устойчиво състояние на целия съюз. Това трябва да се случи във възможно най – кратки срокове, защото подготовката на защитата ще отнеме време. Ако ЕС няма изградена адекватна защита за всяка една област от критичната инфраструктура, ще се наложи да влага средства не в изграждането на политика за борба с кибер атаките, а за справяне с последствията от техните поражение, където тези средства могат да бъдат значително повече и доста закъснели. Това автоматично ще повлияе на финансовата стабилност, което е заплаха за нормалното развитие и просперитет на държавите членки и Съюза като тяхно обединение.

Кибер атаките са една много сериозна заплаха за критичната инфраструктура, и за хората като нейни ползватели, защото последствията от една реализирана атака срещу обект в сферата на критичната инфраструктура, може да нанесе не само финансови загуби, но и може да доведе до загуба на най-ценното за човечеството – живота. В стремежа си да усъвършенстваме света в който живеем, ние вкарваме технологии във всичко заобикалящо ни. Автоматизирани системи се използват в обекти, от чието устойчиво състояние зависи живота ни. Такива обекти са различните видове транспорт (въздушен, железопътен, воден и др.), обекти в областта на енергетиката (водно – електрически централи (ВЕЦ), топло – електрически централи (ТЕЦ) и др.), атомната енергетика (АЕЦ), лечебни заведения, военната техника и още много други, от които ние сме зависими. В обхвата на Рамково споразумение между България и Европейската банка за възстановяване и развитие относно дейностите на Международния фонд за подпомагане извеждането от експлоатация.

Не можем да отминем с мълчание и акцентите на политиката срещу тероризма, както на национално, така и на Европейско ниво. Най-малкото трябва да сме в състояние да знаем какви са политиките на органите за сигурност в страната и тези в рамките на Общонстта. Последното ще позволи да се планира по най-добрия начин действията в случай на необходимост от получаване на помощ за защита. От друга страна, изпълнението на горното не е възможно без идентификация и обозначаване на критичната инфраструктура, както и определянето на нейните характеристики, т.е. това което водещите държави отдавна са осъществили и от които ние трябва да черпим знания и опит. На фона на динамично развиващата се среда и опита на законодателството да регламентира параметрите на нейното функциониране, Република България се превръща в ключов фактор за изграждане и поддържане, в национален, регионален и международен план, на стратегически енергийни и транспортни обекти. Повишаването на тяхното количество, разнообразяването на типът им и разширяването на териториалните области, в които те се намират, в съчетание с увеличаващите се рискове от терористични действия, налага предприемането на синхронизирани мерки за тяхната защита, не само по отношение на използването на системи за наблюдение, ранно предупреждение и оповестяване, но и средства за адекватна реакция.Установяването на критичните инфраструктури и обектите им и оценката на риска за тях се извършват с цел намаляване на риска от бедствия и защита на населението.

В заключение е необходимо да се отбележи, че идентификацията на критичната инфраструктура не е самоцел. Показателен е примера с Българския проект – всеки

здравомислещ човек знае (или поне предполага), че инфраструктурните обекти от сектор „Енергетика" са критични, а газопреносната система се вписва в определението на Европейската комисия за Европейска критична инфраструктура. Но процеса на нейната идентификация дава възможност на съответните ръководители да определят своите приоритети, както и средствата и механизмите за тяхното постигане. Това е първият етап от прилагането на системен подход за създаване на интегрирана система за сигурност и защита на съответния обект от критичната инфраструктура.

Литература:

1. Стратегия на ЕС за киберсигурност.
2. National CyberSecurityStrategiesPracticalGuideonDevelopmentandExecutionDecember 2012
3. Стратегия за развитие на електронното управление в Република България 2014–2020 г.
4. Стратегия за национална сигурност на Република България
5. Закон за управление при кризи
6. https://www.me.government.bg
7. http://nslatinski.org/?q=bg/node/354