Hristo A. Desev,

ENERGY CRITICAL INFRASTRUCTURE RISK ASSESSMENT TECHNOLOGY

Hristo A. Desev

National Military University "V. Levski", Artillery, "Air Defense and CIS" Faculty
Shumen, "K. Scorpil"str. № 1

***Abstract**: Increasing cyberattack capabilities against critical energy infrastructures qualitatively alters cyberspace and puts security systems at the heart of the challenge. The report proposes consistency technology to detect and assess the risk of cyber threats to infrastructure. The mechanisms for optimal protection of these sites and maintenance of their functioning are disclosed.*

***Keywords:** Energy security, criterion, mhe threat model, threat analysis.*

ТЕХНОЛОГИЯ ЗА ОЦЕНКА НА РИСКА НА КИБЕРБЕЗОПАСНОСТТА НА ЕНЕРГИЙНАТА КРИТИЧНА ИНФРАСТРУКТУРА

Христо А. Десев

Национален военен университет „В.Левски", Факултет „Артилерия , ПВО и КИС"

Енергийната сигурност е ключов аспект от Националната и глобалната сигурност, а енергийната информационна сигурност е от особено значение за нормалното функциониране на обществото и критичната инфраструктура. Енергийната инфраструктура е била винаги обект на специална защита поради няколко фактора свързани с промените в основните характеристики на енергийната инфраструктура, неопределеността в заплахите, средата за сигурност и преразпределението ролите и отговорностите между държавата и частния сектор. Самото понятие критична инфраструктура се тълкува в широк диапазон на различните обществени сфери, но най-често засяга съвкупността от обекти (физически и виртуални), които могат да доведат до значителни загуби на безопасността на нацията. Изследването на заплахите срещу критичната енергийна инфраструктура има съществено значение за икономика на страната и засяга основно сложните взаимовръзки в общата фактическа инфраструктура. [3]

Установяването на риска от срив на всяка критична инфраструктура е производна на анализа на заплахата и уязвимостта. Повишаването на възможностите за провеждане на кибератаки срещу критичната енергийна инфраструктура качествено променя киберпространството и поставя системите за сигурност пред сериозно предизвикателство.

Рисковете за енергийната критична инфраструктура които са свързани с извън проектни и хипотетични заплахи са най малко изследвани. Отсъствието на статистически данни за инциденти и сложността и обширността на енергийната инфраструктура предполагат прилагане на семантичен подход за моделиране на екстремни ситуации в енергетиката. Основната характеристика на подходите за откриване на аномалии е способността им да откриват нови и нови атаки. Моделът на заплаха определя сценариите за заплаха със свързаните с тях разпределения на риска.[6]

Извънредните ситуации в енергийния сектор са предмет на енергийната безопасност и заплахите се явяват и реализират, като дефицит на ресурсите осигуряващи безпроблемно енергоизточниците. Според ранговката киберзаплахите са от стратегически характер по отношение на безопасността, като тези ситуации се усложняват от липсата на методически ред и регламентация за моделиране на тези заплахи.

Определянето на влиянието на киберзаплахите за възникване на екстремални ситуации може да се реши при спазване на подход за анализ на заплахата, оценка на риска и оценка на поддържащите системи. Подхода следва да включва три методики за работа:

- методика на анализа на киберзаплахите в енергийната критична инфраструктура;
- методика за формулиране на сценарии за развитие на ситуациите след атаката;
- методика за оценка на рисковете на нарушенията на кибербезопасността.

Всяка от методиките решава комплекс от задачи необходим за извличане на изводи за осъществяване на кибербезопасността. В първата се решават следните задачи:

- определяне на ситуацията (същността на проблема, контекста и др.);
- одит на безопасността, който включва:
  - ✓ анкетиране;
  - ✓ определяне на киберуязвимостите в IT сектора;
  - ✓ оценка на активите;
  - ✓ описание на заплахите;
  - ✓ формулиране на типови атаки;
  - ✓ създаване на концептуални сценарии.

Методиката за определяне на сценариите за критични ситуации се основава на системен анализ и изследване на енергийната безопасност при което се включват следните последователности:[5]

- формиране на концептуални сценарии и техните взаимни връзки;
- определяне на вероятните характеристики, критериите и условията на всеки сценарий;
- провеждане на експеримент;
- изработване на частен модел за всеки тип заплаха;
- анализ на алтернативните сценарии.

Методика за оценка на рисковете на нарушенията на кибербезопасността е ориентирана към:

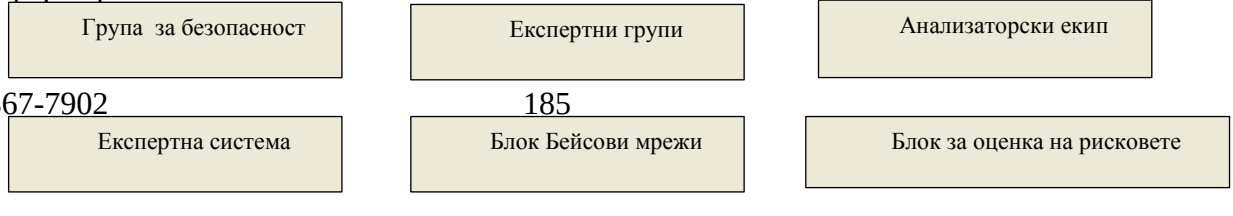
- описание на рисковете;
- качествена и количествена оценка на рисковете;
- ранжиране на обектите по определените критерии;
- оценка на каскадни аварии, безалтернативност на ресурсите и екологични заплахи.

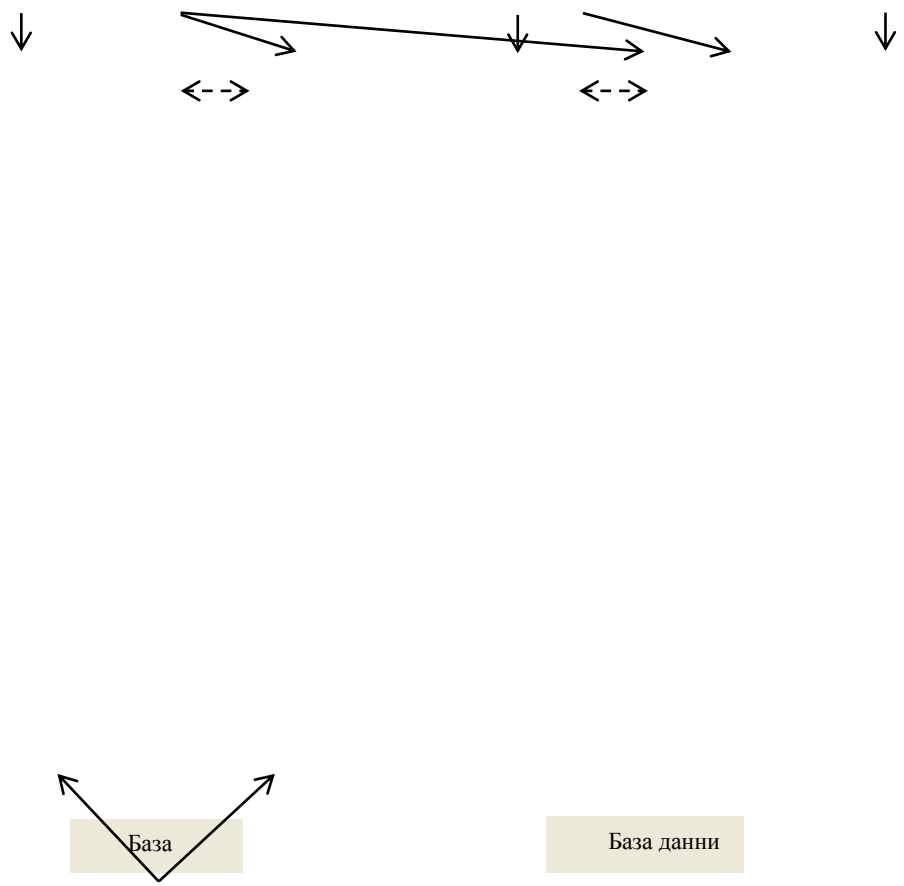
Изложената методология предполага създаване на интелектуална система и технология за разкриване на киберзаплахите фиксира три основни блока: (Архитектура на технологията е представена на фигура 1)

- първи блок – за провеждане на одит за определяне на уязвимостите, актуализиране на заплахите и систематизиране на активите;
- втори блок – за формиране на сценариите, анализ на заплахите и последствията от евентуална реализация на заплахата;
- трети блок – за оценка на риска от настъпване (сбъдване) на екстремалната ситуация.

Технологията на анализа на киберзаплахите и оценката на рисковете от нарушения на кибербезопасността се реализира от алгоритъма за използване на системата. Той преминава през четири основни етапа:

1. Анализ на киберзаплахите:
   - одит на безопасността;
   - определяне на ситуацията;
   - формиране на концепция.





Фигура 1 Архитектура на технологията за разкриване на киберзаплахите

2. Моделиране на сценариите:
   - декомпозиране на заплахите;
   - определяне възможните сценарии на заплахата;
   - определяне на критериите;
   - оценка на вероятността з а проява на заплахата;
   - анализ на оценката;
   - определяне на частни модели на заплахите
3. Оценка на рисковете.
4. Ранжиране на обектите.

Основата на тази технология се опира на добре познатия цикъл на Деминг (PDCA). В детайли отделните етапи преминават през определени последователни стъпки , които позволяват да се разкрие заплахата и вероятните следствия от пробива в киберзащитата.

При анализа на киберзащитата се описват основните характеристики на обекта, описание на активите и обща идентификация на системата. Одитирането на безопасността завършва с определяне на количеството на критични компоненти, които са подложени на уязвимости. Формират се групи от критични активи съответни на заплахата и типовете атаки според зависимостта (1).

$$P = Vi.Tj.Ak.Ra \quad (1)$$

където: P - модел на атаката;
Vi – уязвимост на обекта;
Tj – заплаха за обекта;
Ak – целеви активи;
Ra – възможна големина на атаката.

На етапа на създаване на модел на сценариите те се оценяват по интегрални показатели за възникване на нежелана ситуация. Песимистичните сценарии се свързват с maxколичество загуби. Използва се типов сценарий за реализация на произволна киберзаплаха във вида: (2)

$$S = X^F.X^V.X^T.X^C \quad (2)$$

където:S – структура на сценариите за екстремни ситуации;

X^F - променливи влияещи върху екстремните ситуации;

X^V – променливи обозначаващи активите и техните уязвимости;

X^T – променливи за заплахите;

X^C – променливи отчитащи последствията.

Резултатите от анализа на сценариите са основание за формиране и вземане на решение за достигане на предпочитаното крайно състояние.

При оценката на риска той се интерпретира като съчетание на последствия от нежелани събития и възможности за тяхното възникване. При оценката се комбинират рисковете за информационните технологии и рисковете за аварии и катастрофи на сложни технологични системи. Откриването на уязвимостите позволява да се съчетава списъка с критични активи, които трябва да се осигурят с ресурси за постигане на ниво на безопасност.

Ранжирането на обектите се състои в подреждане на оценените обекти по определени критерии и ниво на риска. Разгледаната технология то се провежда първо по величината на риска за възникване на екстремни ситуации и след това по взаимозависимости с други обекти от инфраструктурата представени като последствия.

В заключение следва да обобщим, че предложената технология е насочена към определени обекти в енергетиката, които потенциално изложени на риска от нарушения в сектора за сигурност. В условията на законова неопределеност и неяснота по защитата на енергийната критична инфраструктура тя позволява да се определят високо рисковите нарушения на киберсигурността, последствията и техните вероятни стойности на загубите и ранжиране на изследваните обекти. Прилагането на предложената технология може да формира подходи за постигане на безопасност от киберпровокации, с които да се поддържа правилно функциониране на обектите.

References

1. Закон за киберсигурност, ДВ 94 от 13.11.2018 г.

2. Наредба за минималните изисквания за мрежова и информационна сигурност, постановление на МС № 186 от 19 юли 2019 г.

3. Dantu R. and Kolan P., 2005, Risk management using behavior based bayesian networks // intelligence and security informatics, стр. 165-184.

4. Gordon A., Hernandez C., Official (ISC)² Guide to the CISSP CBK.

5. Massel L.V. Konvergentsiia issledovanii kriticheskikh infrastruktur kachestva zhizni i bezopasnosti // Trudy VI Mezhdunarodnoi nauchnoi konferentsii ″Informatsionnye tekhnologii i sistemy″. 2017. S. 170-175.

6. Стоянова, В., Интернет на нещата-анализ на сигурността при интелигентни структури, , II International scientific conference confsec, Borovec, 2018, year 2, issue 2(4), ISSN print 2603-2945, ISSN online 2603-2953, http://confsec.eu/sbornik

7. Управление на енергийния сектор и енергийна (не)сигурност в България, С., 2014.,ISBN 978-954-477-216-1