НАЦІОНАЛЬНА БЕЗПЕКА

Жуйкова К.В.
магістр,
Навчально-науковий інститут інформаційної безпеки НА СБУ
Науковий керівник: **Гулак Г.М.**
кандидат технічних наук, доцент, професор кафедри,
Державний університет телекомунікацій

ФОРМАЛІЗАЦІЯ МОДЕЛІ ЗАГРОЗ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ

У сучасних умовах компанії паливно-енергетичного комплексу (ПЕК) працюють у середовищі, що швидко змінюється під впливом багатьох глобальних факторів. Розвиток енергетики має суттєвий вплив на стан економіки та рівень життя населення, від її стану залежить продуктивність всього господарського механізму, тому питання енергетичної безпеки (ЕБ) вкрай важливі для України. Проблеми ЕБ стають останнім часом все більш актуальними, про що свідчить перегляд енергетичної стратегії розвитку США, Євросоюзу, Японії та ряду інших країн. Протягом минулих років Україна, виходячи з досвіду передових країн світу, робить певні кроки в напрямку розбудови системи забезпечення ЕБ не тільки завдяки диверсифікації сфери енергетики, пошуку та впровадженню альтернативних джерел енергії, підвищенню енергоефективності тощо, ай шляхом впровадження в цю галузь сучасних комп'ютеризованих технологій, що в свою чергу потребує адекватних заходів із забезпечення кібербезпеки та боротьби з кіберзлочинністю та кібертероризмом.

Питання ЕБ, ефективного здійснення державної енергетичної політики, як основного інструменту забезпечення ЕБ, широко висвітлюються у наукових виданнях, вітчизняних та зарубіжних засобах масової інформації. Разом з тим, залишаються недостатньо дослідженими чимало проблем, пов'язаних із загрозами ЕБ, забезпеченням кібербезпеки підприємств ПЕК у русі національної безпеки української держави. Таким чином, на сьогодні існує об'єктивна потреба ґрунтовного і глибокого дослідження питань формалізації моделі загроз ЕБ та загроз кібербезпеки ПЕК України, аналізу кращих світових практик забезпечення кібербезпеки в енергетичній сфері, зокрема тих, що визначені міжнародними та національними стандартами з даної тематики.

В науковій літературі зустрічаються різні трактування визначення «енергетична безпека». Так як основу будь-якої безпеки складають інтереси, загрози і захист, відповідно ЕБ базується на енергетичних інтересах, загрозах для енергетики і захисті енергетичної галузі. Енергетичний інтерес ЕБ передбачає «досягнення стану технічно надійного, стабільного, економічно ефективного та екологічно безпечного забезпечення енергетичними ресурсами

економіки і соціальної сфери держави» [1]. Загрозами для енергетики загального характеру можуть бути: внутрішньо-економічні, соціально-політичні, техногенні, природні, зовнішньоекономічні та зовнішньополітичні загрози [2]. Загрози, характерні для України, визначені в Стратегії національної безпеки України [3].

Нормативно-правову базу в сфері забезпечення кібербезпеки та боротьби з кіберзлочинністю становлять Конвенція Ради Європи про кіберзлочинність [4], ратифікована Законом України від 07.09.2005 року № 2824-IV [5], а також відповідні закони України та Укази Президента України, присвячені цій проблемі, положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБО України. Незважаючи на те, що питання інформаційної безпеки, енергетичної безпеки, кібербезпеки прописані в певних нормативно-правових документах України, існує певний вакуум, деякі вимоги та норми взагалі нормативно не закріплені та не описані.

Національний галузевий стандарт «North American Electric Reliability Corporation critical infrastructure protection» (NERC CIP). NERC CIP являє собою набір вимог, спрямованих на забезпечення активів, необхідних для роботи основної електроенергетичної системи Північної Америки. Програма NERC CIP складається з 11 стандартів, що регламентують питання кібербезпеки в SCADA та інших критично важливих об’єктів інфраструктури електросистем [6].

В даний час найбільша увага зосереджена на міжнародному стандарті ISO/IEC 27032:2012 «Information technology – Security techniques – Guidelines for cybersecurity», який був підготовлений Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques* [7]. Слід зазначити, що в Україні діє певна серія національних стандартів 27000, основою яких є міжнародні стандарти, що були адаптовані/модифіковані до нашої країни.

Розглянемо загальну систему забезпечення ЕБ держави (рис. 1).

Як видно з рис. 1, загальна система зебезпечення ЕБ держави представлена чотирма блоками, які взаємопов’язані між собою. Лише комплексний підхід до забезпечення ЕБ держави дозволить досягти максимально енергетичного інтересу.

Компанії ПЕК займають лідируючі позиції рейтингів найбагатших організацій світу (Fortune Global 500, Fortune 1000). Саме це приваблює спецслужби зацікавлених країн та хакерів та спонукає їх проводити кібератаки для отримання необхідних для них даних.

Згідно звіту, опублікованого підрозділом міністерства національної безпеки США ICS-CERT (US Industrial Control Systems Cyber Emergency Response Team) [8], хакери атакували промисловість США щонайменше 245 раз за період з 1 жовтня 2013 року по 30 вересня 2014 року [8, с. 1]. Більшу частину зусиль атакуючі кинули на енергетичний сектор США – 79,32% від всіх інцидентів [8, с. 1]. Найчастіше атакуючі вдавалися до сканування мережі (53,22%) і фішингу (42,17%) [8, с. 2].

В Україні у грудні 2015 року зафіксована перша в історії держави успішна хакерська атака на автоматизовану систему управління енергосистемою (за

визначенням стандартів це категорія – АСУ ТВ). Зловмисники здійснили атаку на внутрішні мережі української енергокомпанії ПАТ «Прикарпаттяобленерго». Внаслідок злому протягом декількох годин велика частина області і саме місто залишилися без енергопостачання. В ході атаки хакери використовували шкідливе програмне забезпечення BlackEnergy.

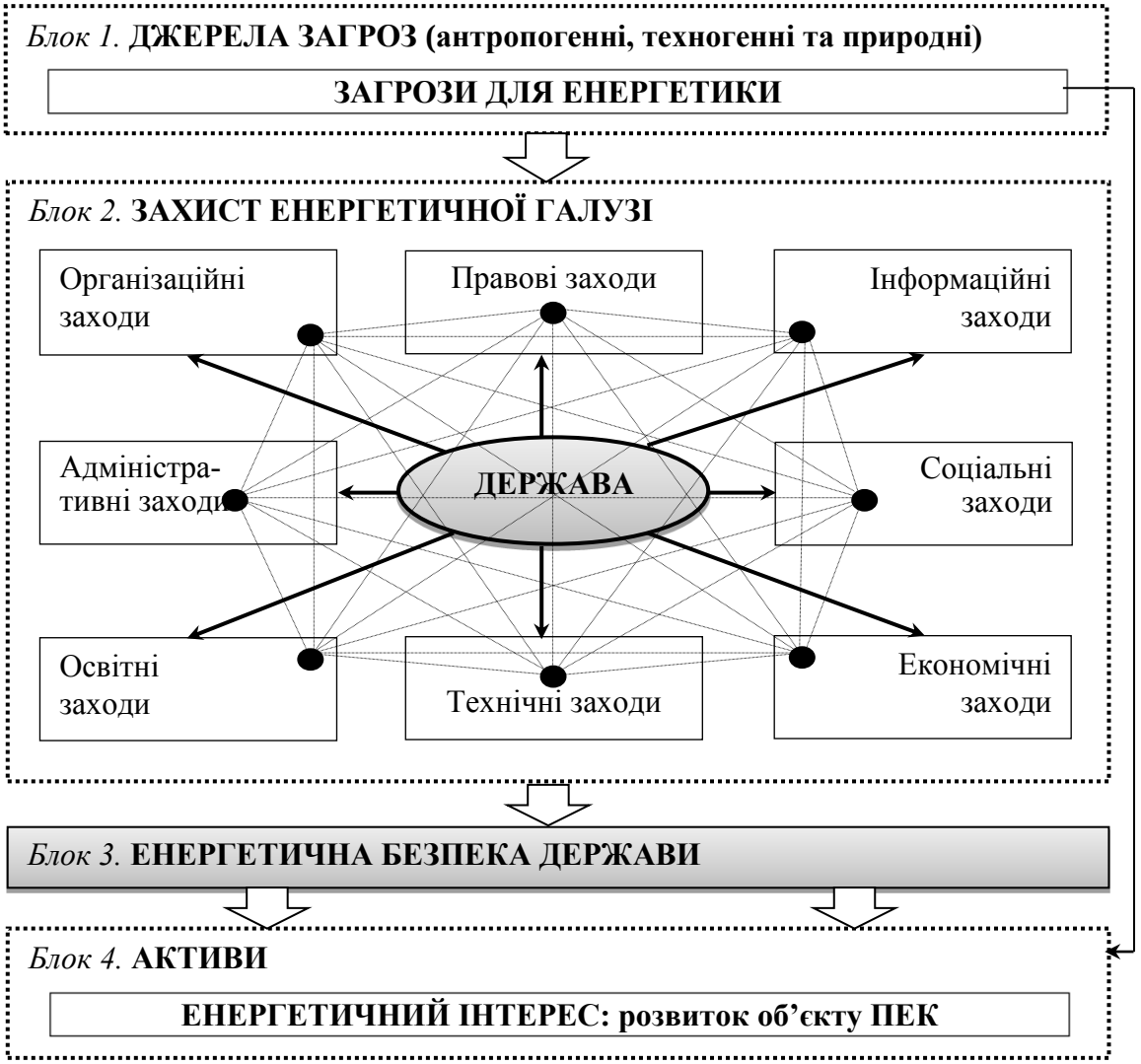

Рис. 1. Загальна система забезпечення ЕБ держави

Джерело: розроблено авторами

Згідно звіту [9] страхової компанії Lloyds і Центру вивчення ризиків при Кембриджському університеті, потенційна кібератака на електричну мережу може коштувати США сотень мільярдів доларів, досягаючи $ 1 трлн збитків.

Системи і об'єкти енергетики відносяться до об'єктів критичної інфраструктури. Кібератаки на ПЕК є серйозною загрозою для багатьох країн. Суть енергетичних інтересів держави, в кінцевому підсумку, зводиться до: 1) побудови надійної системи безпеки, в тому числі і від кібератак; 2) раціонального використання наявних енергоресурсів і одержуваних за їх рахунок усіх видів енергії; 3) виробництва, збереження та накопичення енергетичного потенціалу і енергоресурсів високої якості, в тому числі і за рахунок альтернативних джерел отримання енергії; 4) науково-технічного

прогресу (визначає рівень розвитку енергетики, промисловості і транспортної системи країни) тощо.

Енергетична безпека держави, в тому числі кібербезпека, вимагає скоординованих зусиль в усіх областях (інформаційної, правової, технічної, освітньої, наукової тощо).

Таким чином, для ефективного управління ЕБ держави, прийняття оперативних і стратегічних рішень необхідно:

– усунути нормативно-правовий вакуум в Україні;

– використовувати системи, що базуються на використанні формалізованих знань відповідної предметної області;

– застосовувати комплексний підхід до забезпечення ЕБ.

Список використаних джерел:

1. Енергетична стратегія України на період до 2030 р. Стратегія Кабінету Міністрів України від 24.07.2013 // Верховна Рада України 1994-2016. URL: http://zakon2.rada.gov.ua/laws/show/n0002120-13

2. Жуйкова К.В., Жуйков В.Я. Энергетическая безопасность: угрозы и приоритеты // 21 century: fundamental science and technology X: Proceedings of the Conference. North Charleston, 3-4.10.2016 – North Charleston, SC, USA: CreateSpace, 2016, p. 270, 140-144.

3. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». Указ Президента України; Стратегія від 26.05.2015 № 287/2015 // Верховна Рада України 1994-2016. URL: http://zakon5.rada.gov.ua/laws/show/287/2015

4. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 // Верховна Рада України 1994-2016. URL: http://zakon2.rada.gov.ua/laws/show/994_575

5. Про ратифікацію Конвенції про кіберзлочинність. Верховна Рада України; Закон від 07.09.2005 № 2824-IV // Верховна Рада України 1994-2016. URL: http://zakon2.rada.gov.ua/laws/show/2824-15

6. CIP Standards // North American Electric Reliability Corporation. – 2016. URL: http://www.nerc. com/pa/Stand/Pages/CIPStandards.aspx

7. ISO/IEC 27032:2012 (en) Information technology – Security techniques – Guidelines for cybersecurity // ISO. Online Browsing Platform. – 2012 ISO/IEC. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

8. ICS-CERT MONITOR. INCIDENT RESPONSE ACTIVITY // ICS-CERT. Industrial Control Systems Cyber Emergency Response Team. Department of Homeland Security. URL: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

9. Business Blackout. Lloyd's Emerging Risk Report – 2015 // Lloyd's 2016. URL: https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf