НАЦІОНАЛЬНА БЕЗПЕКА

УДК 004.056.5+351.865

ФОРМАЛІЗАЦІЯ МОДЕЛІ ЗАГРОЗ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ

Жуйкова К.В.
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України
Гулак Г.М.
Державний університет телекомунікацій

У статті досліджено питання формалізації моделі загроз енергетичної безпеки (ЕБ) та загроз кібербезпеки паливно-енергетичного комплексу (ПЕК) України. Розглянуто міжнародні стандарти ISO/IEC 27032-2012 та NERC CIP в енергетичній сфері. Проаналізовано фактори, що впливають на ЕБ та кібербезпеку ПЕК. Розроблено загальну систему забезпечення ЕБ держави. Наведено приклади кібератак на енергетичний сектор.
Ключові слова: енергетична безпека, енергетична безпека держави, паливно-енергетичний комплекс, кібербезпека, загрози для енергетики, захист енергетичної галузі, система безпеки, стандарти кібербезпеки в енергетичній галузі, стандарти NERC CIP, стандарт ISO/IEC 27032.

Постановка проблеми. У сучасних умовах компанії паливно-енергетичного комплексу (ПЕК) працюють у середовищі, що швидко змінюється під впливом багатьох глобальних факторів [1-4]. 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. Енергетика є особливою сферою економіки завдяки її технологічній специфіці. 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.

Аналіз останніх досліджень і публікацій. На сьогоднішній день дослідження ПЕК України, в тому числі в області ЕБ, ведуться такими знаними українськими вченими, як Денисюк С.П., Жуйков В.Я., Кириленко О.В., Півняк Г.Г., Стогній Б.С., Шидловський А.К. [5-10].

Серед відомих вчених, які системно досліджують питання кібербезпеки варто виділити праці таких, як Бурячок В. Л., Толубко В. Б., Толюпа С. В., Хорошко В. О. [11-16].

В Україні вивченням проблем ЕБ і, зокрема, кібербезпеки, займаються фахівці Ради національної безпеки і оборони України, Національної академії Служби безпеки України, Національної Академії наук, Національного технічного університету України «Київський політехнічний інститут», Інституту електродинаміки Національної академії наук України, Державного університету телекомунікацій, Національного інституту стратегічних досліджень, Національного інституту проблем міжнародної безпеки при РНБОУ, Інституту економічного прогнозування НАНУ тощо.

Виділення невирішених раніше частин загальної проблеми. 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.

Формулювання цілей статті (постановка завдання): провести формалізацію моделі загроз ЕБ та загроз кібербезпеки ПЕК України, аналізу кращих світових практик забезпечення кібербезпеки в енергетичній сфері.

Відповідно до зазначеної цілі поставлено такі задачі:

– дослідити фактори, що впливають на ЕБ та кібербезпеку ПЕК;

– розробити загальну система забезпечення ЕБ держави;

– розглянути міжнародні стандарти з ЕБ та кібербезпеки в енергетичній сфері.

Виклад основного матеріалу дослідження. В науковій літературі зустрічаються різні трактування визначення «енергетична безпека» [17]. ЕБ розглядається як: «енергетична незалежність держави»; «комплексна оцінка теплоенергетичного комплексу країни»; «можливість і здатність паливно-енергетичного комплексу країни забезпечувати пропозицію»; «економічна доступність енергетичних ресурсів»; «стан захищеності громадян, суспільства і держави від загрози дефіциту енергії та паливно-енергетичних ресурсів»;

«стан суспільства і економіки, яке дозволяє підтримувати необхідний рівень в енергоспоживанні»; «сукупність умов, при яких відсутня дефіцит енергії»; «засіб економічного і політичного впливу» тощо.

Згідно Енергетичної стратегії України на період до 2030 р. ЕБ України – «це спроможність держави забезпечити ефективне використання власної паливно-енергетичної бази, здійснити оптимальну диверсифікацію джерел і шляхів постачання в Україну енергоносіїв для забезпечення життєдіяльності населення та функціонування національної економіки у режимі звичайного, надзвичайного та стану війни, попередити різкі цінові коливання на паливно-енергетичні ресурси, або ж створити умови для безболісної адаптації національної економіки до нових цін на ці ресурси на світових ринках» [18].

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» [18]. Загрозами для енергетики загального характеру можуть бути: внутрішньо-економічні, соціально-політичні, техногенні, природні, зовнішньоекономічні та зовнішньополітичні загрози [19]. Загрози, характерні для України, визначені в Стратегії національної безпеки України [20]. Сферами забезпечення безпеки на об'єктах ПЕК є: фізичний захист, антитерористична захищеність, кадрова безпека, інформаційна безпека, економічна безпека, правова безпека, екологічна безпека, промислова безпека, охоронна діяльність, пожежна безпека тощо. Терористична небезпека в сучасних умовах України характеризується масштабністю та розвинутою організаційною структурою [2]. При цьому, на відміну від терористичних загроз, з якими світ стикався раніше, в Україні основна небезпека тероризму походить не від окремих терористичних угруповань, а від держави-агресора – Російської Федерації [2].

Нормативно-правову базу в сфері забезпечення кібербезпеки та боротьби з кіберзлочинністю становлять Конвенція Ради Європи про кіберзлочинність [21], ратифікована Законом України від 07.09.2005 року № 2824-IV [22], а також відповідні закони України та Укази Президента України, присвячені цій проблемі, положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБО України [11].

В наукових статтях та літературі [11; 23, с. 28; 24] зустрічається змішення формулювань та різне трактування понять «кібербезпека», «кібезлочинність» тощо. 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. Отже, актуальним є проведення аналізу зарубіжних нормативних документів, тому що у світі з'являються нові системи, наприклад, Smart Grid, впровадження яких забезпечує максимально надійне, технічно та екологічно безпечне, обґрунтовано достатнє енергозабезпечення економіки та населення [9; 10; 25].

Розглянемо 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. На сьогоднішній день підлягають виконанню [26]:

– CIP-002-5.1 – Cyber Security – BES Cyber System Categorization;
– CIP-003-6 – Cyber Security – Security Management Controls;
– CIP-004-6 – Cyber Security – Personnel & Training;
– CIP-005-5 – Cyber Security – Electronic Security Perimeter (s);
– CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems;
– CIP-007-6 – Cyber Security – System Security Management;;
– CIP-008-5 – Cyber Security – Incident Reporting and Response Planning;
– CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems;
– CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments;
– CIP-011-2 – Cyber Security – Information Protection;
– CIP-014-2 – Physical Security.

Мета стандартів NERC CIP гарантувати, що автоматизовані системи та комунікаційні мережі, необхідні для надійного постачання електроенергії в країні, розумно захищені від атак з різних джерел, що заслуговують на довіру, а також підтримувати життєздатність та ефективність такого захисту [27, с. 10]. Стандарти описують практично всі рівні забезпечення безпеки від фізичної охорони до захисту систем управління.

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* [28]. Слід зазначити, що в Україні діє певна серія національних стандартів 27000, основою яких є міжнародні стандарти, що були адаптовані/модифіковані до нашої країни.

Перша область фокусу стандарту ISO/IEC 27032:2012 полягає у вирішенні проблем безпеки кіберпростору або кібербезпеки, які концентруються на усуненні розривів між різними доменами безпеки в кіберпросторі. Зокрема, цей міжнародний стандарт містить технічні рекомендації для вирішення загальних ризиків кібербезпеки. Друга область фокусу – співпраця, оскільки є потреба в ефективному і продуктивному спільному обміні інформацією, координації та обробці інциденту серед зацікавлених сторін в кіберпросторі. Ця співпраця повинна бути безпечним і надійним способом, який також захищає конфіденційність зацікавлених людей. Багато з цих зацікавлених сторін можуть перебувати в різних географічних

точках і часових поясах, і, ймовірно, будуть регулюватися різними нормативними вимогами [28].

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

Як видно з рис. 1, загальна система зебезпечення ЕБ держави представлена чотирма блоками.

Блок 1: під джерелами загроз слід розуміти окремих індивідуумів, деякі злочинні угруповання, спеціальні служби ворожих держав що діють з певною метою (антропогенні джерела), штучні системи та технологічні комплекси вихід з ладу яких може призвести до негативних явищ (техногенні джерела) та природні катаклізми (природний фактор). За стандартом ISO/IEC 27032:2012 загрози розглядаються в їх прив'язці до активів: загрози персональним активам, загрози активам організації (Блок 4). Загрози в даному стандарті означають потенційно небажані впливи, в результаті яких може бути завдано шкоди системі, особистості або організації. Порушники або агенти загроз створюють загрози та мають на меті неправомірно використати або пошкодити активи.

Блок 2: захист енергетичної галузі залежить від взаємодії держави з навколишнім середовищем та комплексного виконання усіх заходів, які взаємопов'язані між собою та визначаються безпосередньо самою державою. Основною задачею усіх заходів є визначення активів захисту, наприклад, проведення адміністративних заходів виявляє рівні управління, на які може бути направлено вплив. Ефективне виконання зазначених заходів визначає рівень захищеності.

На рис. 1 під державою слід розуміти об'єкт енергетики та суб'єкт управління, який усуває небезпеку та загрози, використовує певні засоби захисту, зменшує ризики, усуває вразливості, зберігає ресурси, забезпечує кібербезпеку та управляє об'єктом енергетики. Об'єкт енергетики є дуже складною системою і його кібербезпека може бути забезпечена за умови що забезпечена безпека всіх його елементів, які мають контакти з кіберпростором [24, с. 73].

Блок 3: в сфері енергетичної безпеки доцільно виділити два аспекти:

1) аспект управління сферою енергетики (впливає на кібербезпеку);

2) аспект забезпечення надійності та ефективності (впливає на використання альтернативних джерел енергії, підвищення енергоефективності, економіко-організаційні показники тощо).

Безпека сфери управління залежить від:

– ефективності та надійності управління;

– комплексного забезпечення безпеки.

Блок 4: відповідно до стандарту ISO/IEC 27032:2012, об'єктами захисту є активи: матеріальні і нематеріальні. Енергетичним інтересом об'єкту ПЕК є його подальший сталий безпечний розвиток, наприклад, модернізація, оновлення морально зношеного та застарілого обладнання та устаткування, залучення інвестицій, впровадження сучасних автоматизованих систем управління технологіями виробництва (АСУ ТВ) тощо.

Таким чином, лише комплексний підхід до забезпечення ЕБ 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) [29], хакери атакували промисловість США щонайменше 245 раз за період з 1 жовтня 2013 року по 30 вересня 2014 року [29, с. 1]. Більшу частину зусиль атакуючі кинули на енергетичний сектор США – 79,32% від всіх інцидентів [29, с. 1]. Найчастіше атакуючі вдавалися до сканування мережі (53,22%) і фішингу (42,17%) [29, 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.

Згідно звіту [30] 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. Аналітики змоделювали атаку на інфраструктуру електропостачання східного узбережжя США і проаналізували найгірший варіант розвитку.

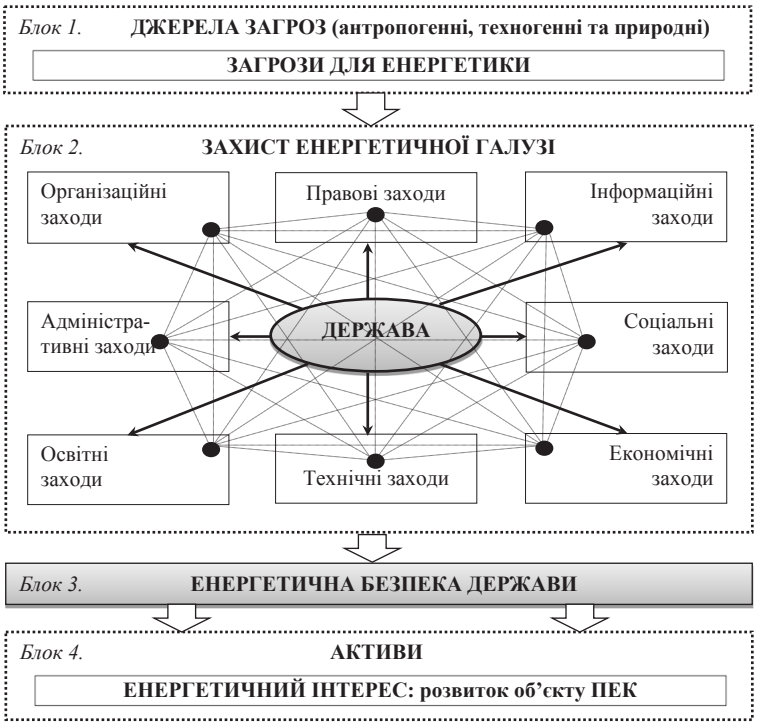

Рис. 1. Загальна система забезпечення ЕБ держави

Джерело: розроблено авторами

Автори звіту стверджують, що в результаті масованої атаки, яка може привести до збою електромережі, відразу різко виросте смертність через відключення систем життєзабезпечення і безпеки. Торгівля буде паралізована через закриття портів, порушиться водопостачання через відключення водяних насосів. На дорогах буде панувати повний хаос через непрацюючі інфраструктури.

Експерти з'ясували масштаби шкоди за сценарієм, коли частина шкідливого ПО (троян «Erebos») заражає центри управління по виробництву електроенергії в деяких районах північно-східній частині Сполучених Штатів. Після активації вірус викликав стрибок напруги на 50 ключових генераторах, через що вони вийшли з ладу. Збій такого масштабу торкнувся близько 93 млн людей. Змодельована атака призвела до дестабілізації регіональної електромережі, викликавши тривалі відключення електроживлення, що призведе до різкого падіння виручки енергетичних корпорацій та збою бізнес-процесів для інших компаній. При річному обсязі ВВП країни на рівні $ 16,77 трлн легко уявити, якими руйнівними будуть наслідки для економіки [30, с. 4].

Висновки з даного дослідження і перспективи подальшого розвитку в цьому напрямку. 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:

– побудови надійної системи безпеки, в тому числі і від кібератак;

– раціонального використання наявних енергоресурсів і одержуваних за їх рахунок усіх видів енергії;

– виробництва, збереження та накопичення енергетичного потенціалу і енергоресурсів високої якості, в тому числі і за рахунок альтернативних джерел отримання енергії;

– 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).

Міжнародний стандарт ISO/IEC 27032-2012 дає цінні вказівки і перелік заходів щодо підвищення кібербезпеки. Документ NERC CIP регламентує питання забезпечення кібербезпеки в SCADA та інших критично важливих об'єктах інфраструктури електросистем.

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 літератури:

1. «Ризики для енергетичної безпеки: глобальний і національний аспекти». Аналітична записка // 2012 Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/1039/
2. «Проблеми оцінки терористичної вразливості та формування паспортів безпеки об'єктів енергетики». Аналітична записка // 2012 Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/content/articles/ files/pasport_bezpeki–3d468.pdf
3. «Екологічна складова енергетичної безпеки: нові глобальні виклики та завдання України». Аналітична записка // 2012 Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/content/articles/files/ekologichna_ skladova–413cf.pdf
4. International Index of Energy Security Risk. Assessing Risk in a Global Energy Market. 2012 Edition. Institute for 21st Century Energy. U.S. Chamber of Commerce // 2012 by the U.S. Chamber of Commerce. URL: http://www.energyxxi.org/sites/default/files/InternationalIndex2012.pdf
5. Інноваційні пріоритети паливно–енергетичного комплексу України / Під заг. ред. А. К. Шидловського. – Київ: Українські енциклопедичні знання, 2005. – 512 с.
6. Енергетична безпека України. Світові та національні виклики [Текст] / Б. С. Стогній [та ін.]; НАН України, Від-ня фізико-техн. проблем енергетики. – К.: Українські енциклопедичні знання; К.: ТЕКСТ, 2006. – 408 с.
7. Енергетична безпека України: оцінка та напрямки забезпечення [Текст] / Ю. В. Продан [та ін.]; ред. Ю. В. Продан, Б. С. Стогній; НАН України, Нац. техн. ун-т України «Київ. політехн. ін.-т». – К.: [б.в.], 2008. – 400 с.
8. Енергоефективність та відновлювані джерела енергії [Текст] / Бевз С. М. [та ін.]; під заг. ред. А. К. Шидловського; НАН України, П-во «Укренергозбереження». – К.: Українські енциклопедичні знання, 2007. – 560 с.
9. Интеллектуальные электроэнергетические системы: элементы и режимы: Под общ. ред. акад. НАН Украины А. В. Кириленко / Институт электродинамики НАН Украины. – К.: Ин–т электродинамики НАН Украины, 2014. – 408 с.
10. Інтелектуальні електричні мережі: елементи та режими: За заг. ред. акад. НАН України О. В. Кириленка / Інститут електродинаміки НАН України. – К.: Ін–т електродинаміки НАН України, 2016. – 400 с.
11. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д–ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
12. Бурячок В. Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / [В. Л. Бурячок, О. Г. Корченко, В. О. Хорошко, В. А. Кудінов] // Захист інформації. – 2013. – Т. 15, № 1. – С. 5–14.
13. Бурячок В. Л. Політика інформаційної безпеки: підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко; за заг. ред. д–ра техн. наук, проф. В. О. Хорошка – К.: ПВП «Задруга», 2014. – 222 с. , с. 180.
14. Бурячок В. Л. Завдання, форми та способи ведення воєн у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона. – 2011. – № 3. – С. 35–42, 57.
15. Бурячок В. Л. До питання організації та проведення розвідки у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона. – 2011. – № 2. – С. 19–23.
16. Бурячок В. Л. Поняття кібервійни та розвідки інформаційно–телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу / В. Л. Бурячок, О. А. Ільяшов, Г. М. Гулак // Збірник

матеріалів круглого столу «Актуальні питання підготовки фахівців із розслідування кіберзлочинів», 25.11.2011. – К.: Наук.–вид. відділ НА СБ України, 2011. – С. 27–32.
17. Прокіп А. В. Еволюція змісту поняття «енергетична безпека» // Стратегічні пріоритети, № 2 (35), 2015 р. – С. 115–119. URL: http://sp.niss.gov.ua/content/articles/files/14–448ed.pdf
18. 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
19. 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 p.
20. 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
21. 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
22. 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
23. Марков А. С., Цирлов В. Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 28–35.
24. Ворожцова Т. Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности / Т. Н. Ворожцова // Онтология проектирования. – № 4 (14), 2014. – С. 69–77.
25. Юдин А. Анализ и оценка нормативных документов, применяемых для обеспечения информационной безопасности Smart Grid систем / Алексей Юдин, Глеб Пирогов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково–технічний збірник. – 2013. – Вип. 1 (25). – С. 88–95.
26. CIP Standards // North American Electric Reliability Corporation. – 2016. URL: http://www.nerc. com/pa/Stand/Pages/CIPStandards.aspx
27. Презентация «CISCO. Обзор стандартов NERC CIP для отрасли энергетики. Безопасность инфраструктуры энергостабжения. Алексей Лукацкий» (28 слайдов) // LinkedIn Corporation 2016. URL: http://www.slideshare.net/CiscoRu/nerc–cip
28. 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
29. 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
30. 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

Жуйкова К.В.
Учебно-научный институт информационной безопасности
Национальная академия Службы безопасности Украины
Гулак Г.Н.
Государственный университет телекоммуникаций

ФОРМАЛИЗАЦИЯ МОДЕЛИ УГРОЗ ЭНЕРГЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Аннотация
В статье исследованы вопросы формализации модели угроз энергетической безопасности (ЭБ) и угроз кибербезопасности топливно-энергетического комплекса (ТЭК) Украины. Рассмотрены международные стандарты ISO/IEC 27032-2012 и NERC CIP в энергетической сфере. Проанализированы факторы, влияющие на ЭБ и кибербезопасность ТЭК. Разработана общая система обеспечения ЭБ государства. Приведены примеры кибератак на энергетический сектор.
Ключевые слова: энергетическая безопасность, энергетическая безопасность государства, топливно-энергетический комплекс, кибербезопасность, угрозы для энергетики, защита энергетической отрасли, система безопасности, стандарты кибербезопасности в энергетической отрасли, стандарты NERC CIP, стандарт ISO/IEC 27032.

Zhuikova K.V.
Educational and Scientific Institute of Information Security
of the National Academy of the Security Service of Ukraine
Gulak G.N.
State University of Telecommunications

FORMALIZATION OF THE THREATS MODEL OF ENERGY SECURITY

Summary
In article questions of formalization of the threats model of energy security (ES) and threats of cyber security of the fuel and energy complex (FEC) of Ukraine are investigated. The international ISO/IEC 27032-2012 and NERC CIP standards in the power sphere are considered. Factors which influence on ES and cyber security of FEC are analysed. General system of providing ES of the state is developed. Examples of cyber-attacks to the power sector are given.
Keywords: energy security, energy security of the state, fuel and energy complex, cyber security, threats for power sector, protection of power sector, security system, standards of cyber security in power sector, NERC CIP standards, ISO/IEC 27032 standard.