Гуманітарна і політична безпека держави

УДК 338.45:622.324

Мордовцев Олександр Сергійович
кандидат економічних наук, старший науковий співробітник
Український державний науково-дослідний інститут «Ресурс»
Мордовцев Александр Сергеевич
кандидат экономических наук, старший научный сотрудник
Украинский государственный научно-исследовательский институт «Ресурс»
Mordovtsev Oleksandr
PhD in Economics, Senior Research Scientist
Ukrainian State Research Institute "Resource"

Аванесова Ніна Едуардівна
доктор економічних наук, професор,
завідувач кафедри менеджменту та публічного адміністрування
Харківський національний університет будівництва та архітектури
Аванесова Нина Эдуардовна
доктор экономических наук, профессор,
заведующий кафедрой менеджмента и публичного администрирования
Харьковский национальный университет строительства и архитектуры
Avanesova Nina
Doctor of Economics, Professor,
Head of Department of Management and Public Administration
Kharkiv National University of Civil Engineering and Architecture

Сергієнко Юлія Іванівна
аспірант кафедри економіки та бізнесу
Харківського національного університету будівництва та архітектури
Сергиенко Юлия Ивановна
аспирант кафедры экономики и бизнеса
Харьковского национального университета строительства и архитектуры

Serhiienko Yuliia

Postgraduate of the Department of Economy and Business

Kharkiv National University of Civil Engineering and Architecture

МЕТОДОЛОГІЧНІ АСПЕКТИ АНАЛІЗУ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ АНАЛИЗА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭНЕРГЕТИЧЕСКОЙ ИНФРАСТРУКТУРЫ УКРАИНЫ

METHODOLOGICAL ASPECTS OF THE ANALYSIS OF THREATS TO INFORMATION SECURITY OF THE ENERGY INFRASTRUCTURE OF UKRAINE

Анотація. *Статтю присвячено проблемам розробка методологічних аспектів щодо аналізу проблемних місць та шляхів зміцнення інформаційної безпеки в енергетичній інфраструктурі України у воєнний та поствоєнний час. З'ясовано, що головна проблема інформаційної безпеки в енергетичному секторі полягає як в обробці, так й в аналізі великої кількості даних у режимі реального часу від так званих корпоративних вузлів локальної мережі, включаючи дані інтелектуальних датчиків, які використовуються для з'ясування кіберзагроз і моніторингу їх ризиків, а також надання фахівцю-експерту великої кількості аналітичної інформації. Шляхом узагальнення наукових джерел було уточнено понятійно-категоріальний апарат щодо напрямку дослідження, а саме надані авторські визначення наступним поняттям: «критична інфраструктура», «енергетична безпека», «кіберінформаційної підсистеми», «кібернетична безпека». Систематизована ієрархія та взаємозв'язок критичних інфраструктур України. Побудовано загальну схему кібернетичної безпеки щодо об'єктів*

енергетичної інфраструктури та доведено, що процеси ідентифікації, кількісного визначення, аналізу та оцінки ризиків, а також їх обробки повинні бути невід'ємними компонентами загального процесу прийняття управлінських рішень щодо сталого функціонування енергетичної інфраструктури країни. – Запропоновані технологічні шляхи для подолання проблемних місць кібернетичної безпеки у енергетичної сфері України. Отримані результати дозволяють стверджувати, що при вирішенні проблеми зміцнення енергетичної безпеки до виділяють дві взаємопов'язані області – технологічна інфраструктура та інформаційно-комунікаційна інфраструктура. Зроблено узагальнюючий висновок, що успіх створення сталої захищеної системи багато в чому залежить від успішного застосування сучасних інформаційно-комунікаційних технологій.

Ключові слова: *інформаційна безпека, інформаційно-комунікаційні технології, енергетичний сектор, критична інфраструктура, воєнно-промисловий комплекс.*

Аннотация. *Статья посвящена проблемам разработка методологических аспектов анализа проблемных мест и путей укрепления информационной безопасности в энергетической инфраструктуре Украины в военное и поствоенное время. Выяснено, что главная проблема информационной безопасности в энергетическом секторе заключается как в отделке, так и в анализе большого количества данных в режиме реального времени от так называемых корпоративных узлов локальной сети, включая данные интеллектуальных датчиков, которые используются для выяснения киберугроз и мониторинга их рисков, а также предоставления специалисту-эксперту большого количества аналитической информации. Путем обобщения научных источников был уточнен понятийно-категориальный аппарат относительно направления исследования, а именно даны авторские определения следующим понятиям: «критическая инфраструктура»,*

«энергетическая безопасность», «кіберінформаційної подсистемы», «кибернетическая безопасность». Систематизированная иерархия и взаимосвязь критических инфраструктур Украины. Построено общую схему кибернетической безопасности в отношении объектов энергетической инфраструктуры и доказано, что процессы идентификации, количественного определения, анализа и оценки рисков, а также их обработки должны быть неотъемлемыми компонентами общего процесса принятия управленческих решений по устойчивому функционированию энергетической инфраструктуры страны. – Предложены технологические пути для преодоления проблемных мест кибернетической безопасности в энергетической сфере Украины. Полученные результаты позволяют утверждать, что при решении проблемы укрепления энергетической безопасности к выделяют две взаимосвязанные области – технологическая инфраструктура и информационно-коммуникационная инфраструктура. Сделан обобщающий вывод, что успех создания устойчивой защищенной системы во многом зависит от успешного применения современных информационно-коммуникационных технологий.

***Ключевые слова**: информационная безопасность, информационно-коммуникационные технологии, энергетический сектор, критическая инфраструктура, военно-промышленный комплекс.*

***Summary.** The article is devoted to the problems of developing methodological aspects for analyzing problem areas and ways to strengthen information security in the energy infrastructure of Ukraine in war and post-war times. It was found out that the main problem of information security in the energy sector is both in processing and analyzing a large amount of data in real time from the so-called corporate nodes of the local network, including data from intelligent sensors that are used to find out cyber threats and monitor their risks, as well as providing an expert specialist with a large*

amount of analytical information. By summarizing scientific sources, the conceptual and categorical apparatus for the research direction was clarified, namely, the author's definitions of the following concepts were given: "critical infrastructure", "energy security", "cyber information subsystem", "cybernetic security". The hierarchy and interrelation of critical infrastructures of Ukraine is systematized. A general scheme of cyber security for energy infrastructure facilities is constructed and it is proved that the processes of identification, quantification, analysis and assessment of risks, as well as their processing, should be integral components of the overall management decision-making process for the sustainable functioning of the country's energy infrastructure. - Technological ways to overcome the problem areas of cyber security in the energy sector of Ukraine are proposed. The results obtained allow us to state that when solving the problem of strengthening energy security, there are two interrelated areas – technological infrastructure and information and communication infrastructure. A general conclusion is made that the success of creating a sustainable secure system largely depends on the successful application of modern information and communication technologies.

Key words: *information security, information and communication technologies, energy sector, critical infrastructure, military-industrial complex.*

Постановка проблеми. Розробка та впровадження сучасних інформаційно-комунікаційних технологій, а також просування концепції цифрової енергетичної трансформації разом із специфікою енергетичного сектору зумовили необхідність включення кіберзагроз до переліку стратегічних загроз енергетичній безпеці. Це зумовлено тим, що процес «цифровізації» енергетичних об'єктів може викликати кіберзагрози, пов'язані із впровадженням нових рішень, застосуванням нових бізнес-моделей, що може супроводжуватися відсутністю або недостатністю

інформації для прийняття оперативних рішень для забезпечення безпеки інформаційно-комунікаційної сфери об'єкта енергетичної інфраструктури.

Головна проблема інформаційної безпеки в енергетичному секторі полягає як в обробці, так й в аналізі великої кількості даних у режимі реального часу від так званих корпоративних вузлів локальної мережі, включаючи дані інтелектуальних датчиків, які використовуються для з'ясування кіберзагроз і моніторингу їх ризиків, а також надання фахівцю-експерту великої кількості аналітичної інформації.

Це визначає актуальність пошуку універсального методичного підходу щодо виявлення, аналізу та оцінки загроз інформаційної безпеки, а також застосування практичних заходів для її впровадження удосконалених методів її зміцнення для об'єктів енергетичної інфраструктури України у сучасних мінливих умовах воєнного та пост воєнного часу.

Аналіз останніх досліджень і публікацій. Енергетична безпека є стратегічно важливою сферою наукових інтересів вчених різних галузей науки. Серед цих наукових трудів вітчизняних та зарубіжних вчених, таких як Вітко А.Л., Музиченко М., Мітюшкіна Х.С., Черніченко Г.О., Мельниченко О.А., Белоцький О. О., Шолль Е., Вестфал К., Аванесова Н.Е., Мордовцев О.С., Сокол К., Совакул Б. К., Браун М. А. та ін. особливе місце займають ті, що присвячені проблемі інформаційної безпеки об'єктів енергетичної інфраструктури. Однак, незважаючи та теоретико-методологічні та практичні результати, які отриманні у дослідженнях цих вчених ще не вирішеним залишаються питання щодо побудови комплексної методологічної основи зміцнення інформаційної безпеки енергетичної інфраструктури України.

Мета та завдання дослідження. Метою статті є розробка методологічних аспектів щодо аналізу проблемних місць та шляхів зміцнення інформаційної безпеки в енергетичній інфраструктурі України

у воєнний та поствоєнний час.

Виклад основного матеріалу. У загальному сенсі, дослідження та аналіз критичної інфраструктури відносно сучасний і молодий науковий напрямок. Якщо проаналізувати та узагальнити вітчизняні та зарубіжні наукові джерела, можна зробити висновок, що критична інфраструктура = це така інфраструктура, вихід з ладу або руйнування якої має значний вплив на здоров'я, безпеку, соціально-економічне благополуччя населення країни або окремої адміністративно-територіальної її одиниці [1-3]. Тобто відмова або руйнування (природне, людський фактор тощо) такої інфраструктури може завдати шкоди суспільству та економіці, при цьому призвести до ланцюгу аварій, які спричинять збої у багатьох суміжних інфраструктурах з потенційно катастрофічними наслідками [1-3].

Треба відзначити, що забезпечення захисту та стійкості критичних інфраструктур є національними та міжнародними пріоритетами будь-якої країни світу та України зокрема. На рис. 1. показано ієрархію та взаємозв'язок секторів критичної інфраструктури країни відповідно за їхньої важливістю та складністю забезпечення їх ефективного функціонування і безпеки.

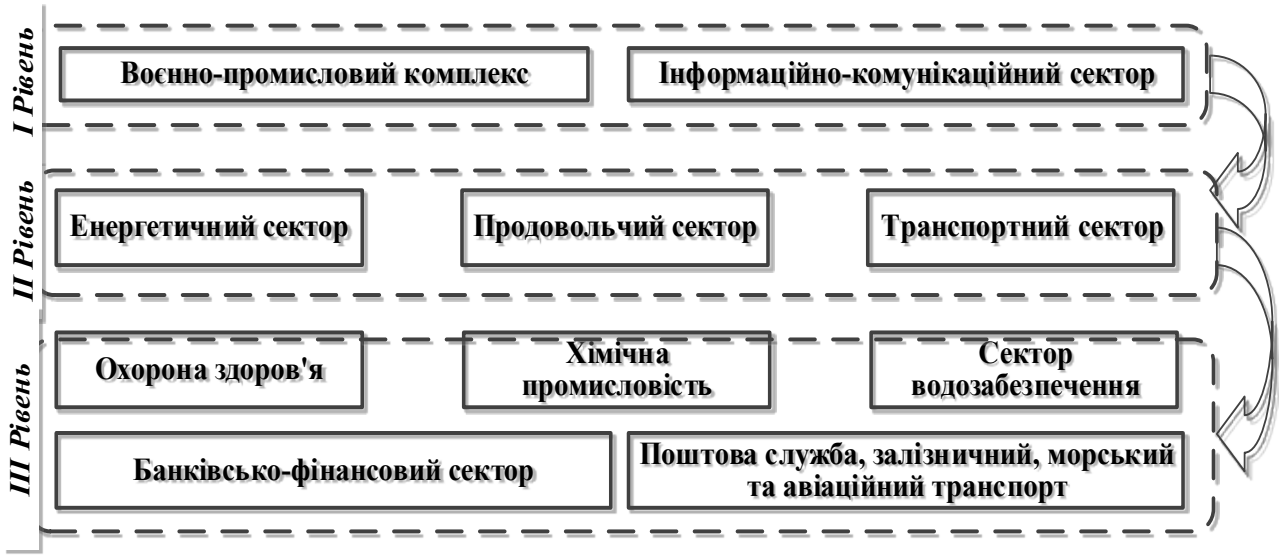

Рис. 1. Ієрархія та взаємозв'язок критичних інфраструктур України

Джерело: розроблено авторами на основі [4]

Рис. 1 показує, що найбільш небезпечними секторами критичної інфраструктури на сучасному етапі розвитку України є воєнно-промисловий комплекс та інформаційно-комунікаційні мережи, які безпосередньо та/або опосередковано впливають на усі інші досліджувані сектори. Все це дозволяє зробити висновок, що енергетична інфраструктура, як й інші потребують удосконалень не тільки в рамках своєї галузі, а й з урахування постійних внутрішніх і зовнішніх викликів, ризиків, загроз та небезпек, які породжують сучасним мінливим середовищем.

Якщо систематизувати вітчизняні та іноземні науково-практичні джерела у енергетичній сфері, то можна зробити висновок, що енергетична безпека на сьогоднішній день виступає станом захищеності країни, її громадян, інформаційного суспільства, держави, економіки від обумовлених внутрішніми та зовнішніми факторами загроз дефіциту у забезпеченні їх обґрунтованих потреб у енергії економічно доступними паливно-енергетичними ресурсами прийнятної якості в нормальних умовах та за надзвичайних (воєнних) обставинах, а також від порушень стабільності, безперебійності паливо- та енергозабезпечення [5-7]. Ці загрози визначаються як зовнішніми (геополітичними, макроекономічними, кон'юнктурними) факторами, так й фактичним станом і функціонуванням енергетичного комплексу країни. Останнім часом перелік загроз поповнився загрозами кібернетичної безпеки (особливо збоку ворожих держав), реалізація яких може спровокувати найсерйозніші екстремальні ситуації в енергетиці, що загрожує значним зниженням можливості забезпечення споживачів енергоресурсами. Отже, кіберзагрози вважаються одними з найважливіших сучасних видів загроз енергетичній безпеці.

Треба відзначити, що небезпечні ситуації в енергетичному секторі, такі як критичні чи надзвичайні, є предметом досліджень енергетичної

безпеки. Загрозами енергетичній безпеці можна вважати дефіцит вимог до ресурсів прийнятної якості в звичайних умовах та екстремальних ситуаціях, порушення стабільності та безперервності енергопостачання через вплив внутрішніх та/або зовнішніх чинників.

З одного боку, стрімке поширення комп'ютерного середовища, розвиток інформаційно-комунікаційних технологій і тенденція переходу до інтелектуальної енергії роблять кібернетичні загрози однією з найважливіших тактичних і стратегічних загроз електронній безпеці. З іншого боку, недооцінюється необхідність системних превентивних заходів щодо запобігання кібернетичним загрозам та постійного оновлення засобів захисту на об'єктах енергетичної та іншої критичної інфраструктури, що, у свою чергу, може вплинути на виникнення значного та тривалого дефіциту енергоресурсів залежно від масштабів та наслідків кібернетичних атак.

Однак для потреб нашого дослідження необхідно виокремити поняття «кіберінформаційної підсистеми» як основного компонента сталого функціонування загальної системи енергетичного сектору України. Отже, під «кіберінформаційною підсистемою» на основі систематизації наукових праць буде розумітися високорівнева інтеграція обчислювальних, мережевих і фізичних процесів, ключовою характеристикою якої є інтенсивна взаємодія апаратних і програмних ресурсів для вирішення інформаційно-комунікаційних завдань за дотриманням принципу постійного отримання даних із середовища, їх обробки та застосування для подальшої оптимізації процесів управління енергетичною інфраструктурою країни [8-10].

Однією з основних вимог до кіберінформаційної підсистеми інформаційно-комунікаційного сектору, окрім його функціональної ефективності, є також безпека взаємодії її компонентів з урахуванням комплексного впливу на керовані об'єкти. Забезпечення безпеки цього

сектору пов'язане з двома ключовими властивостями кіберінформаційної підсистеми, а саме:

– безпеку націлено на забезпечення захисту системи від випадкових відмов;
– захищеність спрямовано на безпеку системи від навмисних атак.

Практична реалізація пов'язана з комплексним дослідженням наступних технологій, зокрема:

– «Інтернету речей» – сукупність будь-яких фізичних об'єктів (не тільки звичайних комп'ютерів), яким можна присвоювати IP-адреси і які можуть передавати дані ,а саме: це побутова техніка, різні датчики, автомобілі, камери відеоспостереження та медичні (у тому числі імплантовані) пристрої. Підсумовуючи можна стверджувати, що цей термін використовується для опису об'єктів, підключених до Інтернету і здатних автоматично збирати та передавати дані без взаємодії з людьми [11].
– бездротові сенсорні мережі – розподілена, самоорганізуюча, стійка до збоїв мережа окремих елементів, що складається з безлічі необслуговуваних і не потребуючих спеціального встановлення датчиків (датчиків) і виконавчих механізмів, підключених по радіоканалу [12].

Таким чином, критичні інфраструктури взагалі, та енергетичні зокрема, розраховані на тривалий період часу (кілька десятиліть), їх функціонування забезпечується за рахунок обслуговування, оновлення та інтеграції нових матеріальних та інформаційно-комунікаційних технологій. З практичної сторони проблема полягає в тому, що в енергетичних інфраструктурах все більше системних порушень, які виникають через незначні збої, що переходять каскадом до великомасштабних наслідків. Провідним напрямком вирішення проблем безпеки є методичні підходи, що основані на концепції ризику, яка, як правило, включає визначення поточних станів елементів

системи, умов, за яких виникає і розвивається аварійна, надзвичайна або навіть катастрофічна, а також якісний і кількісний опис можливих сценаріїв і наслідків при досягненні граничних станів цієї складної системи.

Як було сказано вище, у нашому досліджені буде зосереджена увага саме на розробці теоретико-методичних та практичних основ зміцнення безпеки кіберінформаційної підсистеми, що дозволить досягти сталого рівня функціонування усього енергетичного сектору нашої держави.

Зазначимо, що авторське трактування щодо категорії «кібернетична безпека» наступне, а саме – набір інструментів, стратегій, принципів і гарантій безпеки, рекомендацій, підходів до управління ризиками, дій, професійної підготовки, практичного досвіду, страхування та технологій, які можна використовувати для захисту кібернетичного середовища, ресурсів організації та користувача у сучасних умовах постійних зовнішніх та внутрішніх викликів і небезпек. З цього можна зробити висновок, що загальна схема кібернетичної безпеки щодо об'єктів енергетичної інфраструктури виглядає наступним чином (рис. 2).

Рис. 2. Загальна схема кібернетичної безпеки щодо об'єктів енергетичної інфраструктури

Джерело: розроблено авторами на основі [13]

Таким чином, рис. 2 та загальні відомості щодо функціонування критичних інфраструктур [5-10] показують, що сучасні рішення для автоматизації технологічного процесу на об'єктах енергетики стають

дедалі складнішими та використовують інноваційні інформаційно-комунікаційні технології, що призводить до зростання ризиків порушення безпеки цих об'єктів, аж до виникнення екстремальних ситуацій, що особливо небезпечно при воєнному стані, коли від безперебійного функціонування цих об'єктів залежить як територіальна цілісність країни, так й життя окремих її суб'єктів (населення, підприємства, військові структури тощо).

Процеси ідентифікації, кількісного визначення, аналізу та оцінки ризиків, а також їх обробки повинні бути невід'ємними компонентами загального процесу прийняття управлінських рішень щодо сталого функціонування енергетичної інфраструктури країни.

Управління безпекою інформаційних систем включає в себе також й управління ризиками, тобто всі скоординовані дії для ідентифікації, контролю та усуненню ситуацій, які можуть загрожувати енергетичному сектору країни. Тому можна зробити висновок, що для цієї ситуації дві основні цілі управління ризиками полягають у забезпеченні вжиття адекватних заходів для захисту людей, навколишнього середовища та активів від небажаних наслідків вжитих дій, а також у збалансуванні різних питань, таких як безпека та витрати. Управління ризиками охоплює як заходи щодо запобігання виникненню небезпек і загроз, так й заходи щодо зменшення їх потенційних наслідків.

Методи аналізу системного ризику використовуються для аналізу систем, в яких недостатньо даних для точного прогнозування майбутніх характеристик цієї системи, що саме властиво ризикам у сфері інформаційно-комунікаційних технологій. При цьому система розкладається на підсистеми та компоненти, щодо яких доступна додаткова інформація. Загальні ймовірності та ризик залежать від побудови системи та ймовірностей на рівні підсистем та компонентів. Кількісна (імовірнісна) оцінка ризику систематизує поточний стан знань,

включаючи невизначеність явищ, процесів, діяльності та систем, що аналізуються. Вона призначений для виявлення можливих небезпек і загроз, а також для аналізу їх причин і наслідків. Деякі з традиційних інструментів, які використовуються для аналізу ймовірностей і ризиків, - це теорія статистичної оцінки, аналіз дерева відмов та аналіз дерева подій. Інші методи присвячені більш детальному представленню та аналізу ризику та пов'язаних з ним невизначеностей, включаючи завдання щодо прийняття управлінських рішень, які повинні підкріплюватися результатами аналізу.

Аналіз ризиків в сфері інформаційно-комунікаційних технологій є ключовим елементом процесу управління безпекою кіберінформаційної підсистеми та загальної системи інформаційної безпеки та складається з трьох взаємопов'язаних етапів:

I. Ідентифікація викликів, загроз, небезпек та можливостей (джерел).

II. Аналіз причин і наслідків, з обов'язковим включенням аналізу уразливості.

III. Опис ризику з використанням ймовірностей та очікуваних значень.

Дослідження останніх років показують, що більшість ризиків уразливості зазнають автоматизовані системи, які контролюють енергетичний сектор та воєнно-промисловий комплекс (приблизно 23 % та 31 % відповідно серед усіх секторів критичної інфраструктури (рис. 1.1))

У переважній більшості випадків найбільш успішні кібератаки направлені на сервери і комп'ютери кінцевих користувачів, які підключені до Інтернету. Для атаки на «Інтернет речей» часто використовуються такі інструменти, як:

– аналіз трафіку – це аналіз сукупності шифрованих повідомлень, переданих по системі зв'язку, що не приводить до дешифрування, але дозволяє противнику і/або порушнику отримати непряму інформацію про

переданих відкритих повідомленнях, а також про функціонування спостережуваної системи зв'язку. При цьому використовуються особливості шифрування повідомлень, їх довжина, час передачі, дані про відправника і одержувача тощо;

– DDoS-атака (distributed denial of service) – розподілена атака типу «відмова в обслуговуванні», відрізняється від звичайної тим, що проводиться з декількох комп'ютерів. Для атаки зазвичай використовується ботнет, що складається із заражених комп'ютерів або пристроїв IoT;

– бекдор (backdoor) – це кіберзагроза, при реалізації якої надається можливість віддаленого управління комп'ютером об'єкта енергетичної інфраструктури. На відміну від звичайних утиліт віддаленого адміністрування, трояни цього типу встановлюються, запускаються і працюють непомітно. Після установки бекдори можуть отримувати команду на відправку, прийом, виконання і видалення файлів, збір конфіденційних даних, інформації про дії користувача і багато іншого;

– атака на ланцюг поставок (supply chain attack) – це кібератака, при якій зловмисник впроваджує шкідливий код або використовує інші уразливості перед установкою скомпрометованого програмного забезпечення на об'єкті з метою фільтрації даних, маніпулювання апаратними засобами та програмним забезпеченням, операційними системами, периферійними пристроями (продуктами інформаційних технологій) або службами в будь-якій точці життєвого циклу цього об'єкту;

– перехоплення TCP/IP (TCP/IP hijacking) – це кібератака, при якій авторизований користувач отримує доступ до легітимного з'єднання іншого клієнта мережі;

– підміна DNS (DNS spoofing) – це атака, яка полягає в спотворенні даних кешу DNS-сервера, в результаті чого трафік об'єкту буде

перенаправлено на адресу, вказану хакером (замість легітимного IP-адреси);

– шпигунські програми;

– шкідливе програмне забезпечення;

– клавіатурні шпигуни – троянські програми, які чекають підключення користувача до справжньої банківської веб-сторінці і потім перехоплюють введені з клавіатури символи (тобто, логін і пароль);

– міжсайтовий скриптинг (XSS) – атака, при якій в сторінку сайту впроваджується шкідливий код. При відкритті сторінки, код виконується на його комп'ютері і встановлює з'єднання з веб-сервером хакера, який таким чином отримує контроль над усією або елементами системи;

– спам;

– спуфінг електронної пошти, тобто підміна адреси відправника в листах електронної пошти з метою обману користувача;

– словникова атака – метод підбору пароля (або ключа шифрування), що полягає в переборі слів зі словника до тих пір, поки пароль не буде знайдений;

– атака за сторонніми каналами – спосіб злому криптографічного алгоритму, оснований на аналізі роботи допоміжних систем, що беруть участь в шифруванні;

– троян-PSW (password Stealing ware) – шкідливе програмне забезпечення, призначене для крадіжки паролів та іншої облікової інформації. Вони можуть витягувати збережені секретні ключі з браузерів та інших утиліт, аналізувати кеш і файли cookie і отримувати доступ до різних кондиційних даних (відомості троянець зазвичай відправляє на командний сервер).

Тому для систематизації цих ризиків та рекомендацій щодо їх зменшення або усунення, розробимо в табл. 1 рекомендаційну модель, де

висвітлімо проблеми кібербезпеки та технологічні рішення щодо їх подолання.

Таблиця 1

Проблемні місця кібернетичної безпеки енергетичної сфери та технологічні рішення щодо їх подолання

№ з/п	Інструменти для атаки на кібернетичний простір елементів енергетичної інфраструктури	Технологічні шляхи подолання проблемних місць кібернетичної безпеки енергетичної сфери
I.	Аналіз трафіку	– SSL (secure sockets layer) технологія забезпечення захищеної передачі даних між веб-сервером і браузером; – TLS (transport layer security) технологія безпечної передачі даних в Інтернеті. Є розвитком стандарту SSL і виступає в якості надбудови протоколу HTTP. Для створення захищеного з'єднання TLS використовує симетричне і асиметричне шифрування даних, кілька криптографічних алгоритмів і сертифікати відкритого ключа; – IPSec (IP security): комплект протоколів, запропонований IETF для передачі інформації у віртуальних приватних мережах. Забезпечує аутентифікацію, перевірку цілісності та шифрування IP-пакетів та шифрування IP-пакетів; – SSH (secure shell) мережевий протокол для передачі даних в зашифрованому вигляді. SSH застосовують як тунель для інших протоколів (наприклад, TCP), що дозволяє відправляти через нього практично будь-який вміст. SSH створює захищені канали для передачі паролів, відеопотоку, віддаленого управління комп'ютером. Важливою особливістю протоколу є можливість стиснення даних. Недоліком SSH є слабкий захист від дій зловмисників, що володіють привілеями суперкористувача (root); – MACsec (media access control (MAC) security) стандарт безпеки IEEE, що визначає набір протоколів відповідно до вимог безпеки для захисту даних в локальних мережах. Забезпечує виявлення несанкціонованих дій в локальній мережі і запобігання взаємодії з ними, дозволяє виявити несанкціоновані з'єднання і виключити їх
II.	DDoS атака Бэкдор Атака на ланцюжок поставок	– захист кінцевої точки (EPP, endpoint protection platform) захисні заходи, реалізовані за допомогою програмного забезпечення для захисту комп'ютерів об'єктів енергетичної інфраструкутри від атак. Такими заходами, як правило, є антивірус, антишпигунське та антірекламне програмне забезпеення, персональні брандмауери, системи виявлення і запобігання вторгнень тощо
III.	Перехоплення TCP/IP	– DNSSEC (domain name system security extensions) розширення протоколу DNS, що використовує цифровий підпис даних

		DNS для забезпечення безпеки процесу перетворення доменних імен; – BGP (border gateway protocol) – прикладний протокол, який застосовується для маршрутизації пакетів між автономними сегментами мережі Інтернет. Використовується для передачі інформації про вузли мережі, доступні для групи хостів, між якими встановлено з'єднання. На підставі цієї інформації визначається найкоротший шлях проходження кожного конкретного пакета. Завдання BGP полягає виключно в маршрутизації
IV.	Шпигунські програми Шкідливе програмне забезпечення Клавіатурні шпигуни	– корпоративні брандмауери призначений для захисту периметра локальної мережі від несанкціонованого доступу для забезпечення доступу локальних користувачів в інтернет; – системи виявлення вторгнень – служба безпеки, яка відстежує і аналізує мережеві або системні події з метою виявлення і надання попереджень в реальному часі спроб отримати доступ до системних ресурсів несанкціонованим чином; – засоби довіреної завантаження –здійснюють блокування спроб несанкціонованого завантаження нештатної операційної системи, контроль цілісності програмного забезпечення та середовища функціонування (програмної середовища і апаратних компонентів засобів обчислювальної техніки), а також не перешкоджає доступу до інформаційних ресурсів у разі успішного контролю цілісності програмного забезпечення та середовища функціонування, автентифікації користувача і операційної системи; – тестування на проникнення – методологія тестування, призначена для обходу функції безпеки системи
V.	Міжсайтовий скриптинг (XSS) Спам Спуфінг електронної пошти	– спам-фільтр – програма для визначення та фільтрації небажаних електронних повідомлень, які можуть надходити через корпоративні поштові сервери та публічні сервіси електронної пошти; – брандмауер веб-додатків – засоби фільтрації трафіку прикладного рівня, спеціально орієнтовані на веб-додатки; – політика захисту контенту (CSP) – додатковий рівень безпеки, що дозволяє розпізнавати і усувати певні типи атак, спектр застосування яких включає, крадіжкою даних, підміною сторінок і поширенням шкідливого програмного забезпечення тощо; – інфраструктура політики відправника – технологія, при якій сервер-одержувач повинен мати можливість перевірити, чи збігається Адреса сервера, з якого фактично було відправлено повідомлення, зf адресою справжнього поштового сервера, асоційованого з доменом відправника
VI.	Словарна атака Атака за сторонніми каналами Троян-PSW	– управління ідентифікацією і доступом – технологія забезпечення доступу легітимних користувачів до запитуваних ресурсів в потрібний час в точній відповідності з їх правами. Найбільш критичне значення проблема забезпечення гарантій відповідного доступу набуває у зв'язку з широким застосуванням технологічно неоднорідного обладнання і необхідністю точної відповідності вимогам

		посилених політик безпеки. Ця проблема має ключове значення для будь-якої об'єктів енергетичної інфраструктури. Ефективна організація цього процесу надає можливість оптимізації витрат та створити умови для підключення нових додатків – двофакторна аутентифікація – метод використання інформації з двох джерел для ідентифікації особистості. При цьому звичайний пароль «об'єднується» із зовнішнім пристроєм перевірки автентичності, наприклад з апаратним токеном. Особливої актуальності набуває у стратегічних секторах критичної інфраструктури; – шифрування –процес перемішування даних таким чином, що неавторизованим особам, які не володіють ключем для дешифрування, неможливо їх зрозуміти. Шифрування використовується для того, щоб захистити передані дані.

Джерело: розроблено авторами на основі [14-16]

Таким чином, для побудови сталої і міцної інтелектуальної та цифрової безпеки енергетичної інфраструктури необхідно враховувати наступні потенційні ризики використання сучасних інформаційно-комунікаційних технологій, а саме:

– підвищена складність інформаційно-комунікаційної мережі призводить до збільшення кількості вразливостей для потенційних атак і ненавмисних помилок;

– мережі, взаємопов'язані з іншими мережами, які також можуть займати кілька доменів мережі, збільшують ймовірність «каскадних» аварій;

– велика кількість взаємозв'язків програмних компонентів збільшує вразливість програмного коду, що спрощує хакерам впровадження в програмний код шкідливого коду і вразливостей;

– у наслідок збільшення вузлів інформаційно-комунікаційної мережі збільшується і число точок входу в систему для зловмисників.

При вирішенні проблеми зміцнення енергетичної безпеки до виділяють дві взаємопов'язані області – технологічна інфраструктура та інформаційно-комунікаційна інфраструктура. Успіх створення сталої захищеної системи багато в чому залежить від успішного застосування сучасних інформаційно-комунікаційних технологій. У свою чергу, її ефективне застосування

неможливо без наявності розвиненої сучасної технологічної інфраструктури. Рішення з розвитку технологічної інфраструктури енергетичного сектору, безумовно, відносяться до класу стратегічних рішень нашої країни. Для обґрунтування та підтримки прийняття таких рішень також доцільно залучення інноваційних інформаційних технологій та висококваліфікованих фахівців.

Висновки та перспективи подальших досліджень. У статті були проведені методологічні дослідження щодо проблемних місць та шляхів зміцнення інформаційної безпеки енергетичної інфраструктури України у воєнний та поствоєнний час. Отримані наступні результати, а саме:

– шляхом узагальнення наукових джерел було уточнено понятійно-категоріальний апарат щодо напрямку дослідження, а саме надані авторські визначення наступним поняттям: «критична інфраструктура», «енергетична безпека», «кіберінформаційної підсистеми», «кібернетична безпека»;

– визначено ієрархію та взаємозв'язок критичних інфраструктур України та з'ясовано, що найбільш небезпечними секторами критичної інфраструктури на сучасному етапі розвитку України є воєнно-промисловий комплекс та інформаційно-комунікаційні мережі, які безпосередньо та/або опосередковано впливають на усі інші досліджувані сектори;

– побудовано загальну модель кібернетичної безпеки щодо об'єктів енергетичної інфраструктури та зроблено висновок, що сучасні рішення для автоматизації технологічного процесу на об'єктах енергетики стають дедалі складнішими та використовують інноваційні інформаційно-комунікаційні технології, що призводить до зростання ризиків порушення безпеки цих об'єктів, аж до виникнення екстремальних ситуацій, що особливо небезпечно при воєнному стані, коли від безперебійного функціонування цих об'єктів залежить як територіальна цілісність країни,

так й життя окремих її суб'єктів (населення, підприємства, військові структури тощо);

– запропоновані технологічні шляхи для подолання проблемних місць кібернетичної безпеки у енергетичної сфері України.

Проведене дослідження повинно стати методологічною основою для формування міцною та сталої енергетичної безпеки у сфері інформаційно-комунікаційних технологій, а отже, запорукою зміцнення національної безпеки України у довгостроковому періоді.

Література

1. Вітко А.Л. Сфера забезпечення енергетичної безпеки держави як об'єкт публічного адміністрування. Вісник Харківського національного університету внутрішніх справ. 2016. № 3 (66). С. 144–152.
2. Muzychenko M. Security model of natural gas supply to EU member states. Journal L'Association 1901 "SEPIKE". Poitiers, Frankfurt, Los Angeles. 2016. Edition 15. Part II. P. 107-117.
3. Мітюшкіна Х.С., Черніченко Г.О. Концептуальні засади формування енергетичної безпеки країн в умовах глобалізації. Теоретичні і практичні аспекти економіки та інтелектуальної власності: Збірник наукових праць. Маріуполь: ДВНЗ «ПДТУ», 2018. Вип. 18. С. 106-113.
4. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. URL: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (дата звернення 25.05.2022).
5. Мельниченко О. А., Белоцький О. О. Енергетична безпека: сутність і засоби державного регулювання. Вісник Національного університету цивільного захисту України. Сер. «Державне управління». 2017. № 1. С. 33–42.

6. Scholl E., Westphal K. European Energy Security Reimagined. Stiftung Wissenschaft und Politic. 2017.
7. Аванесова Н.Е., Мордовцев О. С., Сергієнко Ю. І. Теоретико-методичні засади ідентифікації та взаємозв'язку впливу дестабілізуючих факторів на економічну безпеку промислового підприємства. Бізнес Інформ. 2020. №9. С. 20–28. URL: https://doi.org/10.32983/2222-4459-2020-9-20-28 (дата звернення 05.01.2021).
8. Sokol K. Assessing the scale and readiness of companies to enter the world market of informational technologies. L'Association 1901 "SEPIKE". Poitiers, Osthofen, Los Angeles, 2015. Edition № 9. P. 182-186.
9. Дергачова В.В., Колешня Я.О. Енергетична безпека сталого розвитку для підвищення якості та безпеки життя людей. Менеджер. 2017. Вип. 2. С. 12-17.
10. Маркевич К., Омельченко В. Глобальні енергетичні тренди крізь призму національних інтересів України: Аналітична доповідь. Київ: Заповіт, 2016. 118 с.
11. The Internet of Things (IoT) - What it is and why it matters URL: https://www.sas.com/en_us/insights/big-data/internet-of-things.html (дата звернення 25.05.2022).
12. Zill-E-Huma Kamal's, Mohammad Salahuddin. Introduction to Wireless Sensor Networks. 2015. № 1. P. 3-32. URL: https://www.researchgate.net/publication/283824268_Introduction_to_Wireless_Sensor_Networks (дата звернення 25.05.2022).
13. Sovacool B. K., Brown M. A. Competing Dimensions of Energy Security: An International Perspective. Environment and Resources. 2010. Vol. 35. P. 77-108.
14. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017.

168 с.

15. Довгань О. Д. Інформаційна безпека: стан, проблеми, тенденції. Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах: філософсько-правові та прикладні аспекти. Матеріали круглого столу, 12 травня 2017 р., м. Вінниця. Київ: Видавничий дім «АртЕк», 2017. С. 31-39.
16. Марутян Р.Р. Механізми інтелектуального забезпечення політики національної безпеки України: зміст та структура. Web of Scholar : international academy journal. 2020. 1(43), January. P. 26–31.

References

1. Vitko A. (2016), Sfera zabezpechennja energhetychnoji bezpeky derzhavy jak ob'jekt publichnogho administruvannja [Sphere of ensuring energy security of the state as an object of Public Administration]. *Visnyk Kharkivsjkogho nacionaljnogho universytetu vnutrishnikh sprav*, vol. 3 (66), pp. 144-152.
2. Muzychenko M. (2016), Security model of natural gas supply to EU member states. *Journal L'Association 1901 "SEPIKE"*. Poitiers, Frankfurt, Los Angeles, edition 15, part II, pp. 107-117.
3. Mitjushkina Kh., Chernichenko G. (2018). Konceptualjni zasady formuvannja energhetychnoji bezpeky krajin v umovakh ghlobalizaciji. [Conceptual foundations of the formation of energy security of countries in the context of globalization] *Teoretychni i praktychni aspekty ekonomiky ta intelektualjnoji vlasnosti: Zbirnyk naukovykh pracj*, vol. 18, pp. 106-113.
4. *The National Strategy for the Physical Protection of Critical Infrastructure and Key* Assets. URL: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (available: 25.05.2022).

5. Meljnychenko O., Belocjkyj O. [2017]. Energhetychna bezpeka: sutnistj i zasoby derzhavnogho reghuljuvannja [Energy security: the essence and means of state regulation.]. *Visnyk Nacionaljnogho universytetu cyviljnogho zakhystu Ukrajiny. Ser. «Derzhavne upravlinnja»*, vol. 1, pp. 33–42.
6. Scholl E., Westphal K. (2017), European Energy Security Reimagined. Stiftung Wissenschaft und Politic.
7. Avanesova N., Mordovcev O., Serghijenko Ju. (2020). Teoretyko-metodychni zasady identyfikaciji ta vzajemozv'jazku vplyvu destabilizujuchykh faktoriv na ekonomichnu bezpeku promyslovogho pidpryjemstva [Theoretical and methodological foundations of identification and interrelation of the influence of destabilizing factors on the economic security of an industrial enterprise]. *Biznes Inform*, vol 9, pp. 20–28. URL: https://doi.org/10.32983/2222-4459-2020-9-20-28 (available: 05.01.2021).
8. Sokol K. (2015) Assessing the scale and readiness of companies to enter the world market of informational technologies. *L'Association 1901 "SEPIKE"*. Poitiers, Osthofen, Los Angeles, vol. 9, pp. 182-186.
9. Derghachova V., Koleshnja Ja. (2017). Energhetychna bezpeka stalogho rozvytku dlja pidvyshhennja jakosti ta bezpeky zhyttja ljudej [Energy security of sustainable development for improving the quality and safety of people's lives]. *Menedzher*, vol. 2, pp. 12-17.
10. Markevych K., Omeljchenko V. (2016), *Ghlobaljni energhetychni trendy krizj pryzmu nacionaljnykh interesiv Ukrajiny: Analitychna dopovidj* [Global energy trends through the prism of national interests of Ukraine: analytical report]. Kyjiv: Zapovit, 118 p.
11. The Internet of Things (IoT) - What it is and why it matters. URL: https://www.sas.com/en_us/insights/big-data/internet-of-things.html (available: 25.05.2022).

12. Zill-E-Huma Kamal's, Mohammad Salahuddin (2015), Introduction to Wireless Sensor Networks, vol. 1, pp. 3-32. URL: https://www.researchgate.net/publication/283824268_Introduction_to_Wireless_Sensor_Networks (available: 25.05.2022).
13. Sovacool B., Brown M. (2010), Competing Dimensions of Energy Security: An International Perspective. Environment and Resources, vol. 35, pp. 77-108.
14. Nashynecj-Naumova A. (2017), *Informacijna bezpeka: pytannja pravovogho reghuljuvannja* [Information security: issues of Legal Regulation]. Kyjiv: Vydavnychyj dim «Gheljvetyka», 168 p.
15. Dovghanj O. (2017), *Informacijna bezpeka: stan, problemy, tendenciji. Informacijni resursy, intelektualjna vlasnistj, komunikaciji v osvitnjo-naukovij ta innovacijnij sferakh: filosofsjko-pravovi ta prykladni aspekty* [Information Security: State, problems, trends. Information resources, intellectual property, communications in Educational, Scientific and innovative spheres: philosophical, legal and applied aspects]. *Materialy krughlogho stolu, 12 travnja 2017 r., m. Vinnycja*. Kyjiv: Vydavnychyj dim «ArtEk», pp. 31-39.
16. Marutjan R. (2020), Mekhanizmy intelektualjnogho zabezpechennja polityky nacionaljnoji bezpeky Ukrajiny: zmist ta struktura [Mechanisms of intellectual support of the national security policy of Ukraine: content and structure]. *Web of Scholar : international academy journal,* vol. 1(43), pp. 26–31.