УДК 004.413.4

д.т.н., проф. **Даник Ю.Г**. (НУОУ)
Вдовенко С.Г. (НУОУ)

ЛАНЦЮГОВІ ЕФЕКТИ В КІБЕРДІЯХ

У статті представлені результати досліджень особливостей гібридної війни, яка відбувається в Україні та інших державах в кіберпросторі. Встановлені роль і місце ланцюгових ефектів та асиметричних деструктивних дій у сфері інформаційної та кібербезпеки. У зв'язку з тим, що на цей час енергетика є базовою галуззю національної економіки та національної безпеки будь-якої держави, особливості комплексних деструктивних кібер-, інформаційних та когнітивних дій та впливів в кіберпросторі та через кіберпростір розглянуті на прикладі енергетичної сфери з урахуванням загроз, ризиків та особливостей кібервпливів на системи і об'єкти критичної інфраструктури паливо-енергетичного комплексу. Актуальність забезпечення енергобезпеки держав світу зростає, про що свідчить перегляд енергетичних стратегій розвитку Євросоюзу, США, та інших країн. За поглядами ряду вітчизняних та іноземних фахівців, енергетика з галузі економіки перетворилася на інструмент геополітики. Від її ефективного, надійного й сталого функціонування значною мірою залежать рівень національної безпеки держави в цілому, темпи структурних перетворень в економіці, забезпечення потреб населення, суспільного виробництва та оборони. Застосування на об'єктах критичної інфраструктури держави сучасних комп'ютерних, інформаційно-телекомунікаційних та кібертехнологій вимагає впровадження та здійснення заходів із кібербезпеки, протидії кібертероризму та забезпечення кібероборони. Визначені найбільш важливі аспекти цих впливів, запропоновані підходи щодо розробки обґрунтованих організаційних та технічних заходів щодо забезпечення кібербезпеки суспільства і держави в сучасних умовах.

Ключові слова: кібербезпека, кібероборона, комплексний інформаційно-кібернетичний вплив, об'єкти енергетики, розподілено-зосереджений кібервплив, кібервплив з ланцюговим ефектом

Вступ та постановка проблеми. Розвиток інформаційних та кібертехнологій та глобальна інформатизація призвели до того, що інформаційна та кіберсфери стали об'єктом різноманітних деструктивних впливів на усі сфери діяльності суспільства через кіберпростір, який доповнив існуючи: сухопутний, морський, повітряний, космічний, та став сферою конфліктів і можливих бойових дій [1,2]. При цьому відбувається зміна традиційних форм і способів ведення протиборства. Більше того, майбутня війна може бути спровокована в кіберпросторі. Сучасне суспільство практично повністю залежить від стану безпеки інформаційної інфраструктури. Не лише урядові структури держав, але й злочинні та терористичні організації отримали можливість використання глобальної мережі для досягнення своїх цілей. Через це забезпечення безпеки кібер- та інформаційної інфраструктури об'єктів управління є надважливою умовою забезпечення обороноздатності держави, її економічного та соціального розвитку.

Виходячи з цього, необхідність побудови ефективної кібероборони слід розглядати через призму ризиків та загроз, що притаманні світові та насамперед для України у першій чверті XXI століття. Гібридна війна, яка йде на території України, фактично охоплює все більше учасників у всьому світі. Це конфлікт, в якому стираються відмінності між безпосередньо війною в її класичному розумінні, і політикою та економікою, між військовими й іншими її учасниками та мирним населенням. **Гібридна війна** є високотехнологічним конфліктом, продовженням політики держав (коаліцій, політичних угруповань, транснаціональних корпорацій тощо) з метою нав'язування опонентам своєї волі за допомогою комплексних адаптивних і асиметричних синхронізованих впливів на них у різних просторах та сферах з поєднанням конвенційної і неконвенційної складових, забезпеченням багатовимірності, мультиплікативності та синергетичності результатів і високого рівня невизначеності для опонентів щодо кінцевих цілей і шляхів їх досягнення. Гібридна війна не оголошується і тому не може бути завершена в класичному розумінні завершення воєн і воєнних конфліктів. Це перманентна війна змінної

інтенсивності. Деструктивні впливи в ній супроводжуються, як правило, ланцюговими ефектами і синергетичними наслідками. У гібридних війнах в тій чи іншій мірі свідомо чи несвідомо задіяне не тільки все населення країни, яка стала об'єктом агресії, а й міжнародне співтовариство. У гібридних конфліктах військові дії поєднуються з іншими, головним чином економічними, політичними, дипломатичними, інформаційними, психологічними, кібернетичними, когнітивними й іншими діями, які комплексно призводять до системної дестабілізації в усіх сферах життя і діяльності держави, яка є об'єктом агресії.

Кібервійна (війна у кіберпросторі) – складне суспільно-політичне явище, що відбивається в протиборстві непримиренних сторін в кіберпросторі з використанням кіберзброї, засобів кіберрозвідки, захисту або впливу для завдання матеріальних втрат (збитків) супротивнику і мінімізації особистих втрат (збитків) в економічній, військовій, політичній та ідеологічних сферах. На відміну від інших деструктивних впливів, або війни, воєнних чи бойових дій та конфліктів, кібервійна не оголошується, а якщо починається – то не закінчується. Вона може бути закінчена лише у випадку зникнення (знищення) кіберпростору.

Кіберзброя – сукупність технічних, програмних та інших засобів, призначених для здійснення деструктивних впливів на визначені елементи кіберпростору противника з метою виведення їх з ладу, або - на елементи управління через кіберпростір з метою порушення процесів управління [3]. З асоби кібервпливу це перші в історії людства засоби боротьби, які реально існують і застосовуються, але без повного розуміння і контролю [3]. В класичному розумінні кіберзброю під контроль та на облік за номерами та комплектністю взяти не можливо.

Кібервплив – сукупність реалізованих підрозділами кібероборони за єдиним замислом та під єдиним керівництвом одночасних або послідовних взаємопов’язаних за метою і завданнями кібератак та/або кіберударів, спрямованих на визначені елементи кіберпростору противника з метою порушення їх функціонування (стану), або - на елементи управління через кіберпростір з метою порушення процесів управління [4]. Його складові: програмно-комп’ютерний вплив; фізичний вплив на органи і системи управління; радіоелектронне подавлення (ураження); інформаційно-психологічний вплив тощо. Кібератаки та кіберудари – розосереджені в кіберпросторі та часі, та зосереджені на досягненні кінцевої мети

В січні 2018 року в Сенаті США здійснено доповідь [5], в якій відзначено, що з 2014 року Росія невпинне й різноманітно використовує кіберпростір України в якості театру кібердій та полігону для випробовування російської кіберзброї, а кібератаки, як головний інструмент гібридної війни в російській операції в Україні направлені на всі сектори суспільства та економіки, зокрема такі як медіа, фінанси, транспорт, політика, енергетика і військова справа. Принаймні у двох випадках, у грудні 2015 року та грудні 2016 року, російські кібератаки були спрямовані на українську систему розподілу електроенергії, знеструмлюючи на тривалий час об’єкти економіки, інфраструктури та оселі. Після нападу на українську енергетичну мережу, американські чиновники Департаменту енергетики, Департаменту внутрішньої безпеки, ФБР і Корпорації Північноамериканської електричної надійності активізували свою діяльність, визнавши необхідність використання такої ситуації для розуміння тактики й практики дій російського уряду, прогнозування типів майбутніх кіберударів та відпрацювання ефективних заходів захисту від них, з одночасним наданням допомоги Україні в побудові оборонних сил. Співпраця з Україною щодо протидії цим загрозам вважається також критично важливим елементом створення кібероборони Сполучених Штатів [5].

Аналіз останніх досліджень. Концептуальні проблемні питання щодо загроз національній безпеці, зокрема у сфері інформаційної безпеки, соціальні аспекти кіберконфліктів, окремі організаційно-правові засади протидії кіберзлочинності та боротьби з кібертероризмом, дефініційні, правові та технічні аспекти проблем захисту військової інфраструктури від деструктивних, в тому числі кібервпливів досліджували О.А.Баранов, В.Л.Бурячок, Ю.І.Грицюк, Р.В.Грищук, Ю.Г.Даник, Д.В.Дубов, Р.В.Лук'янчук, В.В.Петров, В.П.Шеломенцев, М.Ю.Яцишин та інші [4, 6-23]. Проблеми кібероборони, з точки зору воєнно-політичного та воєнно-стратегічного аналізу розглядаються здебільш іноземними фахівцями, публікуються в офіційних виданнях самітів НАТО, але не мають юридичної сили альянсу та є лише поглядами фахівців [24, 25].

Питання виявлення та протидії комплексним інформаційно-кібернетичним впливам з ланцюговим ефектом на всі сфери діяльності держави та суспільства національними та іноземними фахівцями не розглядалися. Недостатньо також досліджені проблеми, пов'язані із кіберзагрозами енергетичній сфері, що безпосередньо впливає на стан національної безпеки України. Таким чином, на сьогодні існує об'єктивна необхідність дослідження та аналізу питань теорії та практики забезпечення кібербезпеки людини, громадянина, суспільства і держави в умовах кібервпливів з ланцюговим ефектом, зокрема розглядаючи кіберзагрози в енергетичній сфері. **Під ланцюговим ефектом кібервпливу** слід розуміти ефект виникнення, в результаті його здійснення на певний об'єкт впливу, великої кількості (ланцюга) негативних наслідків на інші об'єкти, взаємопов'язані з ним, в тому числі в інших взаємопов'язаних сферах, які у свою чергу породжують свої вторинні хвилі деструктивних ефектів, що призводять до ще більш системно руйнівних наслідків такого впливу.

Викладення основних результатів. Законами та нормативно-правовими актами [26-28] визначено, що найбільш актуальними для України у середньостроковій перспективі загрозами визнані: агресивні дії Росії, розвідувально-підривна і диверсійна діяльність Російської Федерації та інших держав та наголошено на уразливості об'єктів критичної інфраструктури та їх систем управління, а саме: урядових структур; установ сектору безпеки і оборони; науково-дослідного сектору; кредитно-фінансової і банківської системи, сфер соціального захисту, цивільної оборони, енергетики, хімічної та харчової промисловості, транспорту, комунального господарства, водопостачання, телекомунікацій, сільського господарства, закладів охорони здоров'я, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв.

Глибоке проникнення енергетики в усі галузі економіки та в соціальну сферу визначає її особливу роль у забезпеченні безпеки розвитку сучасного суспільства. Енергетична безпека характеризує міру виконання енергетикою її функцій перед суспільством, державою як у звичайних, так і в критичних умовах, зокрема в умовах надзвичайного чи воєнного стану, особливий період тощо.

Підприємства та установи енергетичної сфери відіграють провідну роль в розвитку держави. Основним споживачем електроенергії залишається промисловість, хоча її питома вага у загальному споживанні електроенергії в усьому світі дещо зменшується. Електрична енергія у промисловості застосовується для приведення в дію різних механізмів і безпосередньо в технологічних процесах. Зараз коефіцієнт електрифікації силового приводу у промисловості становить 80%. При цьому близько 1/3 електроенергії витрачається безпосередньо на технологічні потреби. Об'єкти енергетичної сфери є стратегічно важливими об'єктами і повинні функціонувати безперервно та якісно. На території України в кожній області присутні об'єкти енергетики, які відносяться до критичної інфраструктури, і на кожному з них є так звані «критичні точки», елементи порушення нормального функціонування яких призводить до порушення їх функціональної придатності, а у ряді випадків викликає ланцюгові деструктивні ефекти. Всі вони пов'язані певною ієрархією, системою управління та системою захисту. Основу електроенергетики становить об'єднана енергетична система України, яка централізовано забезпечує електроенергією внутрішніх споживачів, а також здійснює її експорт та імпорт. Дана система об'єднує 8 регіональних електроенергетичних систем, пов'язаних між собою системоутворюючими та міждержавними високовольтними лініями електропередач. За даними Держкомстату України, найбільша частка електроенергії виробляється на теплових електростанціях - приблизно 50%, на АЕС - 45%, на гідроелектростанціях – до 5%, відновлювальні джерела електроенергії – до 1%.

Загрози в енергетичній сфері. Вся сукупність загроз, які можуть впливати на функціонування систем енергетики умовно можливо поділити на ординарні загрози (ймовірні відмови та аварії) та неординарні (унікальні за причиною виникнення, характером розвитку та наслідками). Для протидії неординарним загрозам в системах енергетики передбачені різноманітні форми резервування потужностей, по виробленню та транспортуванню паливно-енергетичних

ресурсів, систем забезпечення гарантованого енергопостачання та створення запасів паливно-енергетичних ресурсів. За умов розвитку та функціонування національної економіки подібні ординарні явища майже не становлять загроз енергетичній безпеці, на відміну від неординарних впливів, які здатні негативно впливати на енергетичний комплекс в цілому. Серед неординарних загроз провідне місце займають кіберзагрози, які здатні спровокувати такі проблеми, як порушення забезпечення енергоресурсами, так і надзвичайні ситуації в енергетичному комплексі (ЕК) держави.

Такі кіберзагрози можуть бути реалізовані шляхом впливу на весь ЕК в цілому, або на його окремі елементи, як без так і з досягненням синергетичності результатів. Вплив може бути проведений комплексно, одночасно, послідовно або змішано на автоматизовану систему управління (АСУ), апаратно-програмний комплекс, персонал, фінансову систему енергетики. Найбільш уразливим місцем об'єднаної енергетичної системи (ОЕС) є АСУ.

Система управління ОЕС відіграє провідну роль у функціонуванні всього ЕК України. Саме на АСУ ОЕС може бути здійснений потужний кібервплив, який може призвести до порушення управління певним об'єктом енергетики або ЕК в цілому. За допомогою шкідливого програмного забезпечення кіберзловмисник може контролювати, а в окремих випадках, керувати частиною або всією АСУ. АСУ ОЕС має бути стійкою до кібервпливів та мати відповідну комплексну систему реагування на кібератаки.

У грудні 2015 року здійснені розосереджені синхронні кібератаки типу «розвинена стійка загроза» (*Advanced Persistent Threat* – APT) на АСУ енергосистемами компаній ПАТ «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго». Внаслідок кібератак виникли збої в роботі систем віддаленого доступу, протягом однієї-шести годин повністю або частково відключено понад 100 населених пунктів, вимкнено близько 60 підстанцій, в тому числі такі, від яких живляться стратегічні об'єкти, велика кількість користувачів залишилися без енергопостачання. Наслідки такої атаки можливо були здійсненні з метою перевірки функціонування системи захисту енергокомпаній та системи реагування на критичні ситуації. Кібератаки були комплексними та системно організованими, в ході яких було здійснено:

попереднє зараження мереж за допомогою підроблених листів електронної пошти;

захоплення управління АСУ з виконанням операцій вимикань на підстанціях;

виведення з ладу елементів АСУ;

видалення за допомогою утиліти KillDisk інформації на серверах та робочих станціях;

атака на телефону мережу кол-центрів, з метою забезпечення відмов в обслуговуванні знеструмлених абонентів.

Система управління виявилася вразливою до кібератак такого роду. Реагування на таку кібератаку не було своєчасним, система захисту не виконала свої функції.

У грудні 2016 року була проведена менш масштабна за наслідками кібератака енергокомпанії «Укренерго», яка призвела до виведення з ладу підстанції «Північна» та знеструмлення північної частини м. Києва та прилеглих районів. Атака мала за мету «демонстрацію сили» та була частиною операції проти державних установ України.

Кібератаки проведені на енергетичні підприємства у 2015 році були не в повній мірі самостійно організованими. В 2016 році дії стали більш оперативними, а шкідливе програмне забезпечення (ПЗ) «Crash Override» забезпечувало проведення спланованих атак на декілька «критичних точок» ЕК, передбачало самоорганізацію дій в процесі атак, було спроможним надсилати команди обладнанню енергетичної мережі щодо включення або відключення живлення. Що могло призвести до віяльного відключення електроенергії по всій державі. Аналіз кібервпливів на енергосистеми України представлено в таблиці 1.

Таблиця 1

Аналіз кібервпливів на енергосистеми України.

	Засіб впливу	Шлях проникнення	Ефект впливу	Наслідки
2015 рік				
«Прикарпаттяобленерго»	1. DoS-атака «відмова від обслуговування» на кол-центр обленерго.	Мережа Інтернет	Перенасичення мережевого устаткування великою кількістю зовнішніх запитів	Неможливість споживачів повідомити про відключення електроенергії.
	2. APT- атака.	Мережа SCADA, встановлення шкідливого ПЗ «Black Energy».	Перехоплення системи управління в мережі SCADA через викрадені облікові записи, команда на вимкнення систем безперебійного живлення та запобіжних систем	Відключення протягом 1-6 годин близько 30 підстанцій, залишення без світла близько 230 тисяч мешканців.
«Чернівціобленерго»	1. DoS-атака «відмова від обслуговування» на кол-центр обленерго.	Мережа Інтернет	Перенасичення мережевого устаткування великою кількістю зовнішніх запитів	Неможливість споживачів повідомити про відключення електроенергії.
	2.Утиліта KillDisk.	Мережа Інтернет	Знищення інформації на серверах та робочих станція	Виведення з ладу елементів IT інфраструктури
	3. APT-атака.	Мережа SCADA, встановлення шкідливого ПЗ «Black Energy»	Захоплення управління SCADA з виконанням операцій вимикань на підстанціях	Перерва електропостачання на 1-3,5 год. Зменшення обсягу споживання на 73 МВт/год (0.015% добового обсягу України).
«Київобле-	1. APT-атака.	Система віддаленого доступу.	Несанкціоноване втручання в АСУ	Відключення від електропостачання протягом 1-3 годин 30 вузлових підстанцій стратегічних об'єктів, близько 80 тис. споживачів
2016 рік				
«Укренерго»	Шкідливе ПЗ «Crash Override». (повністю автоматизована атака)	Мережа Інтернет	Перехоплення управління енергетичною системою, автоматизоване знеструмлення підстанцій	Повне знеструмлення підстанції із втратою живлення власних потреб. Зниження постачання від Київської ГАЭС до: ПАО «Київенерго» 144,9 МВт/год, ОАО «Київобленерго» - 58 МВт/год.

У червні 2017 року зловмисниками проведена масштабна деструктивна хакерська атака, яка була націлена на порушення роботи web-сайтів компаній та на систему клієнтської підт-

римки, яка отримала назву «Petya». Під деструктивним впливом опинились й «критичні точки» енергетичної галузі України. У травні 2018 року фахівці компанії Cisco повідомили про зараження більш ніж 500000 маршрутизаторів та роутерів в 54 державах. Для проведення такої атаки було використане деструктивне шкідливе ПЗ «VPNFilter», що дозволило зловмисникам здійснювати моніторинг протоколів Modbus, які використовуються в АСУ системи диспетчерського управління (СДУ) і збору даних (*Supervisory Control And Data Acquisition,* SCADA), перехоплювати весь трафік, що проходить через уражений пристрій, збирати інформацію (включно дані авторизації та персональні дані платіжних систем), віддалено керувати інфікованим пристроєм та виводити його з ладу.

На фоні довготривалої політичної кризи у Венесуелі 7 березня 2019 року, внаслідок кібератак на АСУ СДУ гідроелектростанції «Ель-Гурі», відбулася аварія, що спричинила широкомасштабне відключення електрики. Без енергопостачання залишилися 23 з 25 штатів, або 80% території країни. а також її столиця - Каракас. Системи управління енергопостачанням розбалансовані. У столиці обмежена подача води, виникли проблеми з каналізацією, магазини зачинені або працюють в умовах обмежень, гостро не вистачає продовольства та медикаментів. Платіжні банківські системи не працюють, телекомунікації, зокрема мобільний зв'язок, порушені. Припинив роботу міжнародний аеропорт Майкетія, знеструмлені лінії метро. За три місяці у лікарнях Венесуели з причин пов’язаних із відсутністю електрики померло 79 осіб. Уряд закликав до жорсткої економії пального. Жителі декількох районів Каракаса вийшли на вулиці, вимагаючи від влади відновити електропостачання. У країні проходять масові протести опозиції і зіткнення з поліцією. 10 березня 2019 року тимчасовий президент Венесуели Х. Гуайдо, який є головою парламенту країни - Національної асамблеї, запропонував оголосити надзвичайний стан у зв'язку з масштабними відключеннями електроенергії, що дозволяє запросити міжнародної допомоги, та закликав військових країни перейти на бік опозиції. Уряд США ввів санкції проти посадовців урядових силових структур, під керівництвом яких здійснювалися акції насильства та спалення гуманітарних вантажів продовольства та медикаментів, а також проти 35 нафтових танкерів декількох кампаній, в тому числі найбільшого державного нафтового концерну PDVSA [29-31].

Основні особливості APT-атак:

спрямованість на елементи критичної інфраструктури;

проведення групою висококваліфікованих зловмисників «хакерів»;

залишення невідомими (невиявленими) протягом тривалого часу;

ретельне маскування з використанням спеціально розроблених програмних засобів (спеціалізовані Shell-коди, RootKit та ін.);

належність до розвідувально-підривних операцій і підкріплення розвідувальними або руйнівними акціями.

АСУ ЕК є вразливими перед кібератаками. В результаті проведеного аналізу виокремлюються категорії можливих кібератак, які можуть бути націлені на:

елементи систем управління, наприклад віддалені термінали зв’язку з об’єктом (*Remote Terminal Unit*), або людино-машинного інтерфейсу (*Human Machine Interface* - ЛМІ), які зазвичай мають можливість віддаленого налаштування або управління;

протоколи передачі даних, які добре задокументовані та їх опис знаходиться у відкритому доступі.

Через віддалений доступ зловмисник може перехопити управління системою та спричинити повне або часткове виведення елементів системи з ладу; пошкодити обладнання, внести зміни в інформацію та передані оператору дані. Що може призвести до значних матеріальних та фінансових витрат через пошкодження обладнання, вимкнення ліній електропередач, аварії під час роботи працівників, перевиробництво електричної енергії, перенавантаження систем тощо.

На підставі проведеного аналізу кібератак на підприємства енергетичної галузі України, можемо спрогнозувати один з варіантів проведення типової кібератаки на АСУ. Розділимо її на фази: доступ, розвідка, перехоплення управління.

Для здійснення атаки на АСУ СДУ ЕК зловмисник спочатку має отримати до них доступ. Для нормальної роботи АСУ СДУ необхідний обмін інформацією. Зазвичай, інформація з АСУ СДУ потрапляє до тих чи інших баз даних, включно термінали операторів, долаючи мережеві шлюзи між комерційною та промисловою підмережами. Системи захисту операторського терміналу та комунікації обміну інформацією можуть бути вразливим до атак та використані зловмисником для проникнення до мережі АСУ СДУ ЕК.

Вразливим до атак може бути і віддалений доступ операторів або інших інженерів до систем АСУ СДУ ЕК через віртуальну мережу (*Virtual Private Network*), особливо у випадку невірного налаштування. Вразливість можуть становити сторонні сервери (архівування даних, розробників, аналітиків, тощо) та їхнє підключення до системи промислового управління.

Після здобуття доступу до мережі промислового управління, зловмисник має здійснити розвідку з метою вивчення схеми роботи АСУ СДУ. Складність систем АСУ СДУ примушує зловмисника витрачати час та сили на її вивчення. Одразу після вторгнення зловмисник, швидше за все, матиме дуже обмежений доступ до решти мережі. Серед доступних йому джерел інформації можуть бути внутрішні web-сервери, робочі станції операторів, мережеві диски, інші інтерфейси до керованих систем. Ці джерела інформації можуть бути доступними всім терміналам у мережі, інколи навіть без автентифікації користувача.

Іншим джерелом інформації може стати пасивна розвідка комп'ютерної мережі. Успіх цього методи істотно залежить від знаходження скомпрометованої системи в мережі та вимагає від операторів виконувати якісь дії (аби генерувати потоки даних). На відміну від попереднього підходу, може надати інформацію про облікові дані користувачів, використані ними протоколи, налаштування, тощо. Також пасивна розвідка мережі не потребує відправки пакетів даних і тому непомітна системам виявлення вторгнень. Якщо скомпрометована система знаходиться в одній мережі з основними складовими АСУ СДУ, зловмисник матиме можливість розвідки використаних протоколів та команд.

Зловмисник може вдатись і до активної розвідки мережі. Для цього йому знадобиться доступ до скомпрометованої системи з правами адміністратора, оскільки й цей метод передбачає можливість відправляти мережею спеціально сформовані пакети даних. Однак, ці пакети можуть бути помічені системою виявлення вторгнень, внаслідок чого системні адміністратори дізнаються про існування в мережі скомпрометованої системи. На противагу попереднім методам, цей метод дозволяє зловмисникові дізнатись про доступні зі скомпрометованої системи пристрої та інші термінали в мережі.

Нарешті, для розуміння та відтворення промислового процесу зловмисникові доведеться ретельно вивчити отриману ним інформацію.

Після вивчення промислового процесу, зловмисник може перейти до перехоплення управління ним. Різні методи можуть надавати різний рівень контролю, а відповідно, і результати атаки.

Серед найважливіших об'єктів для атаки є головний диспетчерський блок (*Front-End Processor*), який відповідає за взаємодію між програмованими логічними контролерами та іншими компонентами системи АСУ СДУ, зокрема, ЛМІ з оператором.

Однією з важливих цілей для зловмисника може бути ЛМІ, оскільки він доступно представляє стан всієї системи та надає можливість оператору керувати нею. Однак, можливості для атаки будуть обмежені можливостями ЛМІ і тому зловмисникові може не вдатись вивести систему з ладу або завдати більш істотної шкоди. Атака на ЛМІ є атакою націленою на часткове або повне перехоплення управління. З її переваг можна назвати те, що вона може бути здійснена із використанням звичайних підходів та інструментів, не пов'язаних з промисловими системами управління. Також атака на ЛМІ дозволить зловмисникові приховати свою діяльність під виглядом звичайної роботи оператора.

Схожою на атаку на ЛМІ може бути атака на робочі станції персоналу (РСП - *Engineering workstation*), залучених в розробці програмного забезпечення для ЛМІ та іншого системного ПЗ. Перевага атаки на РСП полягає в тому, що вони можуть не мати обмежень, які накладає

ЛМІ. Зловмисник, після вивчення протоколу між ЛМІ і контролерами, може здійснити спуфінгову атаку – відправляти підроблені команди контролерам або спотворювати дані, передані оператору.

Кіберзловмисники продовжують розвивати та нарощувати спроможності щодо здійснення кібервпливу на різні об'єкти та системи, продовжують створювати й застосовувати нові способи та форми існуючих і модернізованих кібератак. Виходячи з проведеного аналізу проведення кібератак на об'єкти критичної інфраструктури енергетичної сфери, встановлено, що кожна кібератака має свою форму застосування, свій ефект та наслідки після її проведення.

Стійкість системи – це здатність витримати різноманітні деструктивні впливи та відновлюватись у разі пошкоджень. Головне забезпечити функціонування, хоча б і в обмеженому обсязі [22]. Функціональна стійкість може бути оцінена кількістю і потужністю впливів, які може витримати система зі збереженням своєї функціональної спроможності.

Рівень стійкості та стан ОЕС буде впливати на інші галузі з можливістю проявів ланцюгових ефектів. То б то, від ЕК держави залежить функціонування інших об'єктів критичної інфраструктури, які впливають на економіку та обороноздатність держави.

Зниження стійкості та нестабільна робота ЕК держави нанесе колосальні збитки державі та населенню. Довгострокове відключення електроенергії призведе до хаосу у великих містах. Всі галузі та об'єкти пов'язані між собою, тобто створений так званий «ланцюг» і енергетична галузь знаходиться на ключовому місці. Руйнування системи енергетики або порушення її функціонування призведе до створення надзвичайних ситуацій, аварій, катастроф. Збої функціонування систем: транспортної, телекомунікаційної, фінансової, життєзабезпечення, безпеки населення можуть призвести до глобальних екологічних та техногенних наслідків.

Управління паливно-енергетичним комплексом (ПЕК) є автоматизованим, кожний цикл функціонування супроводжується роботою АСУ, тому на кожному етапі управління будь якою складовою ПЕК, може бути здійснений кібервплив на АСУ. Кібератаки можуть бути направлені як на об'єкти генерації енергоресурсів, так і на об'єкти їх транспортування та споживання. Кібервплив на складові ПЕК може бути проведено як асинхронно, так і синхронно. Найбільш уразливою ланкою є СДУ ЕК. Крім того, одночасно може бути проведений психологічний вплив, який буде спрямований на цільову аудиторію таку як управлінській та/або обслуговуючий персонал, споживачів тощо. Існує велика ймовірність проведення кібератак на всі об'єкти та системи одночасно. Метою проведення такого кібервпливу є створення ланцюгового ефекту, який розповсюджується на взаємодіючі об'єкти та системи. Характер та метод їх здійснення може мати гібридний розподільно-зосереджений вплив з ланцюговим ефектом, що передбачає здійснення зосереджених ефективних кібератак на найбільш вразливі елементи об'єкту (системи) і одночасно – інших розподілених кібератак на всі елементи системи, які здатні впливати синхронно, комплексно, одночасно або послідовно і наносити ураження елементам системи та/або виводити її з ладу. Методика здійснення гібридного розподільно-зосередженого кібервпливу з ланцюговим ефектом на прикладі АСУ об'єкту енергетичної сфери представлена в таблиці 2.

Таблиця 2

Методика можливого здійснення гібридних розподільно-зосереджених кібервпливів з ланцюговим ефектом

Об'єкти впливу	**Уразливість**	**Засоби впливу**	**Результат**	**Наслідки**	**Втрати**
Система управління видобуванням сировини	Людино-машинний комплекс	Зосереджена кібератака	Зупинка комплексу добутку сировини	Пошкодження програмного комплексу АСУ	Порушення безперервності функціонування
Система управління транспортом	АСУ транспортної галузі	Зосереджена кібератака на АСУ транспортування сировини	Затримка або припинення доставки сировини та готової продукції	Пошкодження програмного комплексу АСУ, фінансові втрати	Порушення функціонування інших складових транспортної системи
Переробні підприємства	АСУ переробної (нафто, газопереробної) галузі	Зосереджена кібератака на АСУ переробної промисловості	Зупинка переробних підприємств	Фінансові втрати	Зупинка постачання переробленої продукції
Енергетичні підприємства	АСУ, кол-центри	Організована комплексна асинхронна або синхронна кібератака на АСУ електростанціями	Відключення електроенергії, відмова роботи АСУ	Перехоплення управління	Припинення забезпечення електроенергією
Системи життєзабезпечення	Кол-центри, системи диспетчеризації		Збої у функціонуванні систем водопостачання та очищення	Фінансові втрати	Створення хаосу серед населення
Транспортна система регіону	АСУ, система диспетчеризації, системи оповіщення	Розподілено-зосереджені кібервпливи на транспортну та енергетичну галузі	Одночасна відмова функціонування АСУ транспортної системи та АСУ ЕК	Відмова в управлінні повітряним, водним та залізничним рухом, фінансові втрати	Створення хаосу серед населення в аеропортах, залізничних вокзалах
Системи довгострокового зберігання продовольства	АСУ енергетичного комплексу та транспортної галузі	Синхронні кібервпливи на АСУ транспортної установи та електростанції	Виведення з ладу систем, забезпечення довгострокового зберігання продовольства	Фінансові втрати підприємств, установ торговельної сфери	Порушення систем забезпечення потреб населення. Створення хаосу
Сектор безпеки та оборони (СБіО)	АСУ електростанцій, АСУ установ і організацій СБіО	Гібридні розподілено - зосереджені кібервпливи на АСУ установ та організацій	Відключення від електроенергії військових частин, установ і організацій	Втрата функцій контролю, управління, втрата інформації	Зниження бойової готовності, матеріальні та бойові втрати

Об'єкти впливу	Уразливість	Засоби впливу	Результат	Наслідки	Втрати
		СБіО та АСУ електростанцій, які забезпечують їх життєдіяльність та бойову готовність	ЗСУ, МВС, СБУ, ДПСУ, ДСНС, ДССЗЗІ. Знищення або вилучення інформації в ІТС військових частин, установ і організацій СБіО		
Підприємства важкої промисловості	АСУ електростанцій та транспортних установ	Синхронні кібервпливи на АСУ транспортних установ та електростанції, які забезпечують функціонування підприємств важкої промисловості	Повне відключення від електропостачання одного або декількох підприємств важкої промисловості	Фінансові втрати	Зупинка промисловості. Порушення систем забезпечення потреб держави, населення, СБіО.
Фінансова система (банки, фінансово-розрахункові установи)	АСУ електростанцій та АСУ фінансових установ та організацій	Гібридні розподілено- зосереджені кібервпливи на АСУ електростанцій, що забезпечують функціонування фінансивих установ і організацій та на АСУ фінустанов	Відключення від електроенергії фінустанов і організацій та одночасне проникнення в АСУ фінустанов	Фінансові втрати, втрата інформації	Фінансові втрати фізичних та юридичних осіб, державних підприємств, установ та організацій

Виходячи з проведеного нами аналізу проведення кібератак на об'єкти критичної інфраструктури та соціальні компоненти кіберпростіру, встановлено, що кожна кібератака має свої мету, зміст, організацію, тактику реалізації, основні та супутні ефекти і результати, наслідки після її здійснення тощо.

Кібердії можуть здійснюватися послідовно, паралельно та послідовно-паралельно, з використанням методів розподільно-зосереджених дій та/або сукупності одночасних та/або послідовних впливів, які полягають в зосередженні кібервпливів на найбільш вразливі елементи об'єкта (системи), які забезпечують отримання синергетичного ефекту в апріорі непередбачуваних місцях (елементах, системах, сферах), на які не обов'язково спрямовується безпосередній вплив.

Результат виникає за рахунок системи розосереджених впливів на не завжди безпосередньо взаємопов'язані елементи. Цей метод передбачає створення так званих гібридних кібератаки, які діють комплексно і взаємоузгоджено та охоплюють технічну, соціотехнічну та соціальну сфери. Вони здатні впливати синхронно, комплексно, одночасно або послідовно, наносити ураження елементам системи та/або виводити її з ладу. Метою проведення кібервпливу

на АСУ СДУ ЕК може бути створення ланцюгових ефектів, які розповсюджують деструктивну хвилю на взаємодіючі об’єкти та системи.

До складу АСУ можуть входити різноманітні технічні системи та засоби: системи і засоби координатно-часового, метеорологічного і інших видів забезпечення; системи, засоби, лінії та мережі зв'язку і передачі даних; системи і засоби дистанційного моніторингу; системи і засоби збору, накопичення та обробки інформації; автоматизовані системи і засоби управління; системи і засоби відображення і доведення інформації; інші технічні та програмно-технічні засоби. Значна частина систем і засобів використовується для формування каналу зворотного зв'язку як з людиною-оператором, так і з керованими технічними компонентами ОЕС.

Для протидії таким кібервпливам, що несуть в собі тяжкі наслідки для населення та держави в цілому, необхідно розробити методику виявлення таких особливих кібервпливів. Розглянемо розроблену методику щодо можливого здійснення гібридних розподілено-зосереджених кібервпливів з ланцюговим ефектом.

Критичність виходу з ладу об’єкта енергетики вимагає опрацювання питань захисту АСУ з акцентом на доступність та стійкість системи, а також цілісність інформації. Наприклад, можливі два підходи до побудови зон забезпечення кібербезпеки єдиного центру кіберзахисту (ЄЦК) енергетичної галузі – на основі рівнів або вимог безпеки і на основі загроз кібербезпеки. У першому випадку зони кібербезпеки визначаються як умовні кордони, що розділяються необхідними рівнями безпеки. На практиці зони утворюються шляхом виділення деяких функціональних областей АСУ.

В іншому випадку зони утворюються на основі можливих загроз кібербезпеки [22]. Для ЄЦК пропонуються наступні зони: зона ЄЦК (I), зона управління (II), зона доступу користувачів (III), зона мережевого обладнання (IV), зовнішня зона (V).

Для побудови ефективної системи захисту автоматизованої системи управління від кібервпливів, вибору і впровадженню адекватних організаційно-технічних заходів та засобів повинен передувати аналіз, опис і моделювання загроз й вразливості систем, розроблення методики виявлення кібервпливів. Отже, очевидним є те, що спочатку кожна загроза повинна бути розпізнана та ідентифікована. Зазначимо, що використовувані в сучасних системах виявлення й протидії кібератакам, методи є досить ефективними в тому разі, якщо відомі точні характеристики кібератак. Незалежно від використовуваних методів виявлення кібератак на автоматизовану систему управління енергетичної галузі зустрічаються з однаковою проблемою – постійно змінювані характеристики кібератак вимагають гнучкої системи захисту, яка здатна залишатися ефективною, навіть якщо не відомі точні характеристики кібератаки [21]. Методику виявлення та запобігання кібератакам представлено схематично на рисунку 1.

Реальність високого ризику практичної реалізації розглянутих кіберзагроз вимагає формування такої системи кібербезпеки та кібероборони, яка забезпечить скоординоване управління всіма її складовими. Така система потребує наявності відповідного єдиного органу управління, подібного за структурою, завданнями і функціями до аналогічних органів управління в цій сфері країн-членів НАТО, призначеного для реалізації єдиної політики та стратегії дій Міністерства оборони України та Збройних Сил України в інформаційному та кіберпросторі; організації та координації заходів щодо кібербезпеки та захисту критичної інформаційної інфраструктури держави; управління силами кібербезпеки та кібероборони під час кризових ситуацій, в умовах особливого періоду та правового режиму воєнного стану.

Цей орган управління інформаційної та кібербезпеки повинен вирішувати такі основні задачі:

участь у формуванні та реалізації державної політики з питань інформаційної, кібер- безпеки та кібероборони;

формування та реалізація політики Міністерства оборони України та Збройних Сил України щодо дій у кіберпросторі;

ЗОНА ЄЦК (I)	ЗОНА УПРАВЛІННЯ (II)	ЗОНА ДОСТУПУ КОРИСТУВАЧІВ (III)	ЗОНА МЕРЕЖЕВОГО ОБЛАДНАННЯ (IV)	ЗОВНІШНЯ ЗОНА (V)

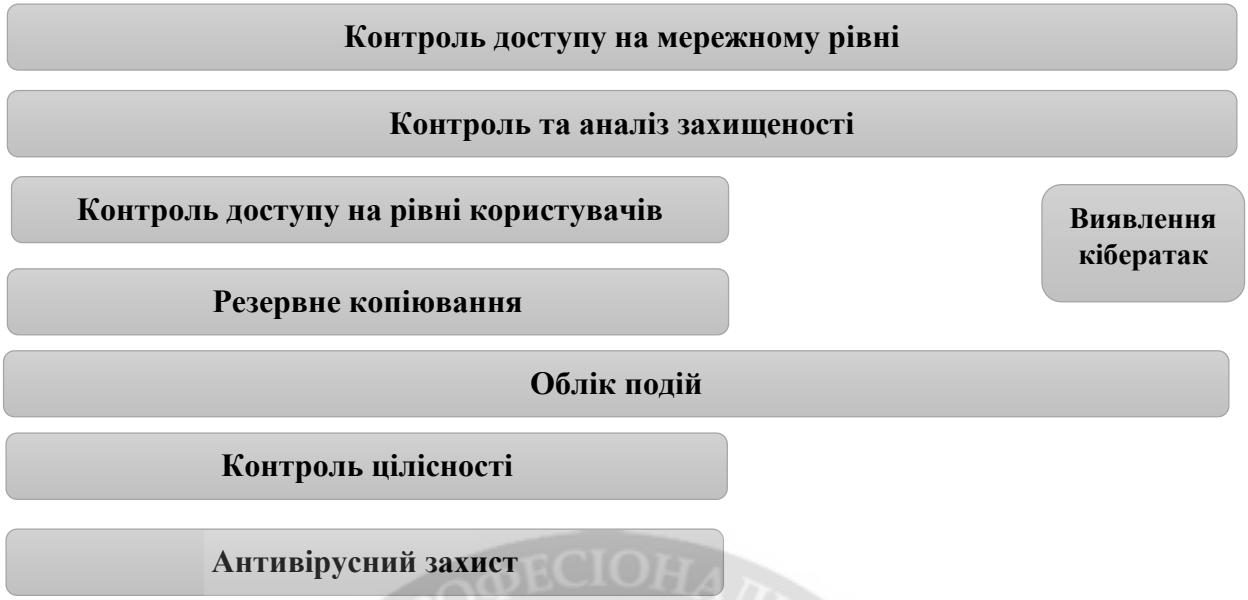

Рисунок 1 – Методика виявлення кібератак

участь у виконанні заходів зі створення та розвитку інформаційних систем та ресурсів у Збройних Силах України;

координації дій суб'єктів інформаційної, кібер- безпеки та кібероборони Міністерства оборони та Збройних Сил України;

участь у формуванні стандартів підготовки та держзамовлення на підготовку фахівців з інформаційної, кібер- безпеки та кібероборони;

організації взаємодії та проведення заходів (в т.ч. щодо підготовки держави до кібероборони) зі структурними підрозділами інших центральних органів виконавчої влади та міжнародними партнерами з питань кібербезпеки;

підтримання взаємодії з системою відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT);

планування та узгоджене управління діяльністю суб'єктів у кіберпросторі за єдиним замислом і планом. Контроль та координація їх дій;

моніторинг та аналіз кіберінцидентів, деструктивних інформаційних та когнітивних дій у кіберпросторі та ефективності дій системи кібербезпеки, виявлення уразливостей в інформаційних та кібер системах своїх і противника;

планування, організація та координація розвідувальних (Cyber Warfare Intelligence), оборонних (Defensive Cyber Warfare) і наступальних (Offensive Cyber Warfare) операцій в кіберпросторі (Cyberspace Operation) та кібероперацій (Cyber Operation);

організація та координація інформаційних дій у кіберпросторі (включаючи соціальні мережі).

З цією метою у складі органу управління інформаційної та кібербезпеки повинні бути підрозділи: моніторингу кіберпростору, захисту кіберпростору, активних дій у кіберпросторі,

Наявність ефективної системи управління силами і засобами які діють в кіберпросторі забезпечить інформаційну, кібернетичну та когнітивну перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції "смарт-оборони", ключовими елементами якої є високотехнологічна підготовка персоналу та збалансоване поєднання найбільш ефективних аспектів стратегій "жорсткої сили" та "м'якої сили", шляхом зваженого і узгодженого використання інструментарію стратегічних комунікацій, санкцій, переконання і застосування сили та інших впливів способом, який є найбільш рентабельним та має політичну і соціальну легітимність. Особливістю стратегії "м'якої сили" є об'єднання

трьох когнітивних компонентів: культури держави (у тому, чим вона цікавить інші держави), її політичних цінностей (чи дотримується вона їх у внутрішній і зовнішній політиці) та зовнішніх відносин (чи сприймаються вони як легітимні і морально обґрунтовані).

За досвідом провідних країн світу до найбільш ефективних та результативних дій сил спеціальних операцій у сучасних гібридних війнах відносяться впливи спрямовані на порушення систем управління державою та її сектором безпеки та оборони шляхом комплексного ведення різноманітних, але в першу чергу, інформаційних і кібернетичних дій спрямованих на дискредитацію військово-політичного керівництва держави у сприйнятті особового складу збройних сил, населення та світової спільноти.

Аналіз деструктивних дій, які ведуться з використанням спеціальних технологій в інформаційному та кібернетичному просторах України, дозволив виявити комплексні узгоджені за метою, замислом, місцем і часом інформаційно-кібернетичні впливи на всі верстви населення, соціальні і демографічні групи, керівництво держави, Міністерство оборони України та командування Збройних Сил України.

Для їх реалізації використовуються засоби телерадіомовлення, Інтернет ресурси (інформаційні сайти, соціальні мережі, спеціалізовані форуми тощо). Серед усіх деструктивних інформаційно-психологічних, інформаційно-кібернетичних дій, що проводяться, найбільш ефективними є ті, що спрямовані проти керівного складу держави та командування збройних сил.

Дослідження показали, що, як правило, такі дії є комплексними і включають елементи «непрямих впливів», маніпуляцію репутацією, сугестивний вплив. В рамках такої загальносистемної дії визначаються керівники, ті особи, вплив на яких забезпечує досягнення мети найкращим чином. Надалі обираються способи та форми впливу і проводиться інформаційна операція.

Вирішальним є те, що достатньо запустити інформацію, а далі, зважаючи на особливості соціуму, він сам буде продукувати плітки, будувати домисли та поширювати інформацію далі.

Таким чином, у кіберсфері уже є сформований спеціальний контент, активізація якого у визначений момент може блокувати дії будь-якого керівника і тим самим заблокувати дії структури, яку він очолює, або зробити її функціонування не ефективним, або примусити її працювати так як потрібно стороні, що проводить інформаційну операцію. Крім того такі дії створюють передумови до паніки, непокори, дезорієнтації, дезертирства тощо.

Завдяки використанню інноваційних технологій у конвенційній складовій сучасних війн став можливим перехід від дій загальноруйнівного характеру до дій із перевагою функціонально-структурного впливу на супротивника, а найголовніше – досягнення над ним когнітивної переваги.

Проведені дослідження показали, що когнітивне протиборство стало невід'ємною складовою сучасних і майбутніх війн і воєнних конфліктів як міждержавних і внутрішньодержавних, так і між будь-якими геополітичними та регіональними акторами. Когнітивній складовій належить виняткова роль в сукупності факторів, що формують і викликають воєнний конфлікт, впливають на його хід та результат, інтенсивність і наслідки. Тому, сучасні війни, а особливо війни майбутнього ведуться за когнітивну сферу соціуму (суспільства, соціальних груп, людини, населення) і керування ним (нею).

Когнітивні впливи можуть бути навмисними і випадковими, багатовекторними і комплексними, загальної спрямованості або цільовими (цілеспрямованими), спрямованими на суспільство в цілому чи на конкретні спільноти або індивідів, на досягнення короткотривалого або довготривалого ефекту, негайно або після латентної фази, з варіацією значень або без.

В сучасних умовах всі сторони конфлікту прагнуть взяти під контроль саме когнітивний простір, який охоплює сприйняття, усвідомлення, переконання, розуміння і цінності, інтелектуальне середовище, як індивідів, так і соціальних груп і суспільства в цілому, в якому власне і відбувається ухвалення ними рішень. Тому головний результат успішних когнітивних впливів – це зміна моделі світу та його сприйняття в людині, соціальних групах суспільства, та суспільстві в цілому, що забезпечує можливість взяття їх під контроль і здійснювати зовнішнє управління ними на емоційному, моральному, культурному, світоглядному і ментальному рівнях, з формуванням стійких стереотипів для сприйняття дійсності через їх призму. Особливе

значення мають при цьому нав'язування та просування хибних наукових, суспільних, економічних, державних, військових теорій, парадигм, концепцій, стратегій, наративів, які найбільш ефективно просуваються та впроваджуються через заклади освіти та наукові установи, електронні, соціальні мережі та блогосферу. З цією метою використовуються всі можливості стратегічних комунікацій, ведуться інформаційні, психологічні, кібернетичні та інші дії (акції, операції тощо), які спрямовані як на безпосередніх учасників конфлікту, так і на населення країн, що беруть в ньому участь, міжнародне співтовариство. Особливістю є те, що навіть при проведенні державними акторами дій планово та узгоджено, вони проходять на тлі хаотичних цільових і випадкових подібних впливів всіх інших акторів. Це трансформується в інформаційно-кібернетичний і когнітивний варіант війни "всіх проти всіх" (в кібернетичному, інформаційному та когнітивному просторах). У результаті, як показують проведені дослідження, об'єкти, на які спрямовані когнітивні дії можуть бути не просто введені в стан когнітивного резонансу, дисонансу або дисбалансу, але і отримати інформаційні та когнітивні травми, дійти до когнітивної межі сприйняття (неможливості подальшого безпечного сприйняття когнітивних впливів), часткової або повної когнітивної дезорієнтації і навіть до когнітивного колапсу, з подальшим переходом у стан когнітивної агресії або розчарування у всьому апатії і депресії.

Взагалі в сучасних конфліктах досягнення мети агресії здебільшого починається з несилових методів, головним чином економічних, політичних, дипломатичних, інформаційних, психологічних, кібернетичних, когнітивних тощо. Але, при цьому значну роль відіграють демонстраційні заходи військового попередження і стримування. Вони, найчастіше, виступають не просто демонстрацією сили, а мають за мету спровокувати дії, які сприятимуть економічному і морально-психологічному виснаженню противника, тощо. В цілому, у гібридних конфліктах будь-якої інтенсивності бойові дії (операції) є складовою взаємоузгоджених за єдиним замислом і планом інших (несилових) дій, які превалюють на всіх їх стадіях (зародження, ескалація, інтенсифікація, затухання, залагодження). Цим створюються дестабілізуючі внутрішні і зовнішні процеси в державі, яка є об'єктом агресії (стурбованість і невдоволеність населення, міграції, акції громадської непокори тощо). Надалі для досягнення стратегічних цілей застосовуються силові методи ведення дій з широкомасштабним залученням сил і засобів розвідки, оперативного управління військами (силами) і засобами, а також традиційних засобів ураження, державних збройних формувань, некомбатантів та інших учасників (терористів, радикальних озброєних груп, рухів опору, найманців, партизан), сил спеціальних операцій і т.і.

Перспективи подальших досліджень полягають у тому, щоб визначити найбільш критичні об'єкти інфраструктури держави, що підлягають захисту, а також дослідити запропонований метод інтелектуального розпізнавання загроз на більш широкому класі задач кількісного і якісного розпізнавання кібернападів.

Для ефективного кіберзахисту критичної інфраструктури держави, установ та підприємств оборонного комплексу необхідно впроваджувати комплексні організаційні та технічні заходи, щодо запобігання (зниження ризику реалізації) та протидії кіберзагрозам. Підсистеми захисту, зокрема, реалізовані в АСУ, мають вирішувати наступні організаційно-технічні завдання:

забезпечення безпеки санкціонованого доступу персоналу до системи та її складових;

запобігання цілеспрямованих злочинів та ненавмисних помилкових дій персоналу та сторонніх осіб, направлених на НСД до системи та її складових;

захист АСУ та її складових від деструктивного кібервпливу та інші [22].

Завдання ідентифікації загроз полягає у визначенні типів загроз, їх властивостей та можливостей в умовах апріорної невизначеності про об'єкт, надмірності іншої зовнішньої інформації, в т.ч. й хибної, зовнішнього деструктивного впливу на АСУ, тощо. Вирішення задачі можливе лише за рахунок оптимізації підходів до реалізації АСУ, в тому числі – до побудови систем комплексного захисту від кіберзагроз. [22].

Такий підхід дозволить побудувати систему захисту АСУ, що виконує завдання в умовах апріорної невизначеності, на принципах доцільності, раціональності та розумної достатності. В результаті декомпозиції складних систем управління, які виконують завдання в кризових

умовах, з'ясовано, що для забезпечення функціональної стійкості складні системи мають створюватися з урахуванням наступних основних вимог [22]:

безперервність функціонування;

гнучкість та адаптивність до загроз (атак);

забезпечення захисту від загроз;

багаторівневість захисту відповідно до рівнів загроз;

комплексність (реалізація організаційних, організаційно-технічних й інженерно-технічних засобів та заходів);

уніфікація програмно-апаратних та алгоритмічних рішень систем захисту;

варіативність функціональної логіки (адаптивність підсистеми захисту ІКС до інших подібних складних систем);

автономність функціонування технічної компоненти системи захисту;

реалізація багаторівневої системи контролю безпеки та захисту від помилок персоналу;

гарантоване кореговане забезпечення обмежень кола службових осіб щодо виконання ними повноважних функцій;

дотримання розумного балансу між завданням швидкої обробки великих заданих обсягів інформації в АСУ за мінімальний наявний проміжок часу та необхідністю витрачання значного часового ресурсу на досягнення мети функціонування систем захисту. [22].

Висновки. У статті розглянуті шляхи й напрями до вибору та реалізації раціональних підходів при вирішенні питання комплексного захисту від деструктивних кібервпливів з ланцюговими ефектами критичної інфраструктури держави та отримані такі основні результати:

1. Проаналізовано всі основні кібератаки, які впливали на функціонування об'єктів критичної інфраструктури на прикладі енергетичної сфери. В ході дослідження кібератак, було встановлено, що атаки не були одиночні, а проводилась синхронно, всі вони мали деструктивний вплив на АСУ об'єктами енергетики. Встановлено, що основний синхронний деструктивний кібервплив здійснювався зосереджено на вразливі елементи АСУ. Перед проведенням основної кібератаки, проводилась кібератака на систему обслуговування і диспетчеризації, з метою відмови в обслуговуванні споживачів. Застосування декількох деструктивних зосереджених кібератак на ЕК проводились в рамках масштабної кібероперації, яка була направлена на порушення одночасно декількох об'єктів енергетичної галузі.

2. Встановлено, що в залежності від рівня стійкості залежить результат функціонування системи вироблення та постачання електроенергії. Аналіз проведення кібератак показав, що мінімальне значення рівня стійкості може призвести до руйнування енергетичної системи (об'єкта, мережі).

3. Описано (змодельовано) методику здійснення гібридних розподільно-зосереджених кібервпливів з ланцюговим ефектом на об'єкти критичної інфраструктури. Визначені уразливості об'єктів. Визначені уразливості АСУ. Встановлено, що кібератаки здатні проникати через електронну пошту, отримувати доступ до головних серверів, отримувати інформацію про стан функціонування системи, здійснювати перехоплення управління АСУ та об'єктом в цілому, здійснювати зміну параметрів функціонування об'єктів (особливо критичним є зміна частоти реактора на атомній електростанції).

4. Розроблено методику виявлення гібридних розподілено-зосереджених кібервпливів з ланцюговим ефектом за допомогою моделі інтелектуального розпізнавання кіберзагроз .

5. Запропоновані організаційні та технічні заходи щодо забезпечення кібербезпеки на об'єктах критичної інфраструктури. Визначено, що технічні заходи мають бути реалізовані за допомогою комплексу засобів захисту, який буде забезпечувати своєчасне виявлення кібератак та протидію ним.

Запропоновані методика оцінки функціональної стійкості складних систем до деструктивних впливів та виявлення критичних елементів, вузлів та зв'язків системи, а також диференційний підхід до класифікації, розпізнання та визначення рівня загроз для складних АСУ, дозволяють обґрунтувати та створити комплексну організаційно-технічну підсистему захисту

критичної інфраструктури держави, яка гарантовано забезпечить адекватне реагування на реальні та потенційні загрози, раціонально використовуючи наявні у держави можливості і ресурси

ЛІТЕРАТУРА:

1. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 - Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

2. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

3. Alexander Kosenkov. Cyber Conflicts as a New Global Threat file: Режим доступу: //C:/Users/Downloads/futureinternet-08-00045.pdf

4. С.Вдовенко, Ю.Даник, С.Фараон, "Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення". Електронний журнал політики відкритого доступу "Комп'ютерні науки та кібербезпека" Харківського національного університету імені В.Н.Каразіна. SSN 2519-2310 (Online) №1 (12) 2019

5. Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018 Available: Режим доступу: http://www.gpoaccess.gov/congress/index.html

6. О.А.Баранов, Про тлумачення та визначення поняття "кібербезпека" "Правова інформатика", № 2(42)/2014 – С. 54-62.

7. В. Л. Бурячок. Основи формуваннядержавної системи кібернетичної безпеки: монографія / В. Л. Бурячок. – К.: НАУ, 2013. – 432 с.

8. В.Л. Бурячок. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / А.Л. Бурячок // Сучасна спеціальна техніка : зб. наук. праць. – 2011. – № 3 (26). – С. 104-114.

9. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа (2015). В. Б. Толубко (загальна редакція). Інформаційна на кіберберзпека: соціотехнічний аспект / В. Л. Бурячок, . – К.: ДУТ, 2015. – 288 с.

10. В. Л.Бурячок, Г. М. Гулак, В. О. Дорошко. Завдання, форми та способи ведення воєн у кібернетичному просторі. Наука і оборона, № 3 2011. – С .35-42.

11.Ю.І. Грицюк. Кіберінтервенція та кібербезпека україни: проблеми та перспективи їх подолання, Науковий вісник НЛТУ України. – 2016. – Вип. 26.8 Національний лісотехнічний університет України http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf

12.Р.В. Грищук , Ю.Г.Даник. Основи кібернетичної безпеки. Монографія. вид. трете перероблене Житомир. ЖНАЕУ, 2016. – 636 с.

13.Д.В.Дубов. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К.: Вид-во НІСД, 2011. – 30 с.

14. Д.В. Дубов. Стратегічні аспекти кібербезпеки України / Д.В. Дубов // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К.: Вид-во НІСД. – 2013. – № 4 (29). – С. 119-126.

15. Д. В. Дубов. Кіберпростір як новий вимір геополітичного суперництва : монографія /– К. : НІСД, 2014. – 328 с. Режим доступу: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

16. Р.В. Лук'янчук. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук'янчук // Вісник НАДУ: зб. наук. праць. – 2015. – Вип. 3. – С. 110-116.

17. Р. В. Лук'янчук. Деякі питання реформування системи державного управління у сфері забезпечення кібернетичної безпеки: сучасний погляд / Р.В. Лук'янчук // Вісник НАДУ : зб. наук. праць. – 2013. – Вип. 2. – С. 81 -92.

18. В.В. Петров. Щодо формування національної системи кібербезпеки України / В.В. Петров // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К. : Вид-во НІСД. – 2013. – № 4 (29). – С. 127-130.

19. В.П. Шеломенцев. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : зб. наук. праць. – 2012. – № 1(27). – С. 312-320.

20. М. Ю. Яцишин. Міжнародно-правова протидія кібервійнам / Яцишин М. Ю. //Збірник праць Національного авіаційного університету – 2015 – № 1 – С. 67-71

21. С.Г. Вдовенко, Ю.Г.Даник. Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління Збройних сил / Сучасні інформаційні технології у сфері безпеки та оборони № 2(29), 2017. С. 98-106.

22. С.Г.Вдовенко, Ю.Г.Даник. Концептуальні напрямки комплексного вирішення проблеми захисту від несанкціонованого доступу в складних системах спеціального призначення. Тези доповідей Шостої Міжнародної науково-технічної конференції, Вінниця 24-25.10.2017. С. 61-64

23. О.М.Гук, О.Ю.Чередниченко, Р.М.Штонда, І.О.Диба. Дії в кіберпросторі під час підготовки та ведення мережецентричної війни / Сучасні інформаційні технології у сфері безпеки та оборони № 2(29), 2017. С. 107-110.

24. J. Andress Cyber warfare: Techniques, tactics and tools for security practitioners / Andress J., Winterfeld S., Rogers R. – Amsterdam: Syngress/Elsevier, 2011. – 289 p

25. The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0. Tallinn 2016. Режим доступу – http://csef.ru/media/articles/3990/3990.pdf

26. Закон України Про основні засади забезпечення кібербезпеки України № 2163-VIII від 5 жовтня 2017 року.[Електронний ресурс] – Режим доступу:http://zakon.rada.gov.ua/laws/show/2163-19

27. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96 // Офіц. вісн. України. – 2016. – № 23.

28. Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14.03.2016 №92/2016

29. [Електронний ресурс] – Режим доступу: https://glavcom.ua/world/observe/venesuela-zalishilasya-bez-elektriki-575648.html

30. [Електронний ресурс] – Режим доступу: https://vesti-ukr.com/mir/328311-blekaut-v-venesuele-khuan-huajdo-reshil-vvesti-rezhim-chp

31. [Електронний ресурс] – Режим доступу: https://www.facenews.ua/news/2019/443568/

REFERENCES:

1. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 -Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

2. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

3. Kosenkov,A Cyber Conflicts as a New Global Threat file, Available:///C:/Users/Downloads/futureinternet-08-00045.pdf.

4. Vdovenko, S Danik,Y and Faraon, S (2019), "Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення." [Definitive problems of the Terms of the Sphere of Cyber security and Cyber Defense and the Ways of their solution], International electronic scientific journal Computer Science and Cybersecurity Issue 1(12) 2019 ISSN 2519-2310 (Online). – Available:https://periodicals.karazin.ua/cscs/issue/view/80

5. Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018 Available: Режим доступу: http://www.gpoaccess.gov/congress/index.html

6.Baranov,A (2014) "Pro tlumachennya ta vyznachennya ponyattya kiberbezpeka", [*On the interpretation and definition of cyber security*], "Pravova informatyka", [*Legal Informatics*], No. 2 (42) / 2014 - p. 54-62.

7. Buryachok,V (2013) "Osnovy formuvannya derzhavnoyi systemy kibernetychnoyi bezpeky",[*Fundamentals of the formation of the state system of cybernetic security*], a monograph , Kyiv: NAU, 432 pp.

8. Buryachok,V (2011) "Kibernetychna bezpeka – holovnyy faktor staloho rozvytku suchasnoho informatsiynoho suspilstva", [*Cybernetic security - the main factor for the sustainable development of a modern information society*],"Suchasna spetsialna tekhnika ",[*Modern special technique*] sciences works, No. 3 (26), p. 104-114.

9. Buryachok,V, Tolubko,V, Khoroshko,V and Tolyupa,S. (2015) "Informatsiyna na kiberberzpeka: sotsiotekhnichnyy aspekt",[*Information on cyber-security: the sociotechnical aspect*], Kyiv, DUT, 288 p.p.

10.Buryachok,V, Gulak,G and Doroshko,V. (2011) "Zavdannya, formy ta sposoby vedennya voyen u kibernetychnomu prostori", [*Tasks, forms and methods of conducting wars in cybernetic spacious*], "Nauka i oborona", [*Science and Defense*], № 3, p. 35-42.

11.Grytsuk, Yu. (2016) "Kiberinterventsiya ta kiberbezpeka Ukrayiny: problemy ta perspektyvy yikh podolannya" [*Ciber iintervention and cyber security of Ukraine: problems and prospects for their overcoming*], Naukovyy visnyk NLTU Ukrayiny, [*Scientific Bulletin of NLTU of Ukraine*], vol. 26.8 National Forestry University of Ukraine http://nltu.edu.ua/nv/Archive/2016/26_8/52.pdf

12.Grishchuk, R and. Danyk Yu. (2016) "Osnovy kibernetychnoyi bezpeky"[*The basics of cybernetic security*], Monograph., Zhytomyr. ZHNAEU, 636 pp.

13.Dubov, D and Ozhevan,M (2011) "Kiberbezpeka : svitovi tendentsiyi ta vyklyky dlya Ukrayiny", [*Cybersecurity. World Trends and Challenges for Ukraine*], Kyiv,View NISD, 2011, 30 p.p.

14.Dubov,D (2013) "Stratehichni aspekty kiberbezpeky Ukrayiny" [*Strategic Aspects of Cyber security of Ukraine*], "Stratehichni priorytety" [*Strategic Priorities: Sciences*], Kyiv,View NISD, № 4 (29), p. 119-126.

15.Dubov,D (2014) "Kiberprostir yak novyy vymir heopolitychnoho supernytstva", [Cyberspace as a new dimension of geopolitical rivalry], Monograph, Kyiv, View NISD, 328 p.p, Access Mode: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

16.Lukyanchuk,R. (2015) "Derzhavna polityka u sferi zabezpechennya kibernetychnoyi bezpeky v umovakh provedennya antyterorystychnoyi operatsiyi" [*State policy in the field of providing cybernetic security in the context of anti-terrorist operation*], "Visnyk NADU" zb. nauk. prats, [*Visnyk NADU*] sciences works p. 110-116

17.Lukyanchuk, R (2013) "Deyaki pytannya reformuvannya systemy derzhavnoho upravlinnya u sferi zabezpechennya kibernetychnoyi bezpeky: suchasnyy pohlyad" [*Some issues of reforming the system of public administration in the field of cybernetic security: modern view*], "Visnyk NADU" zb. nauk. prats, [*Visnyk NADU*] sciences works, Issue 2. - p. 81 -92.

18.Petrov,V (2013) "Shchodo formuvannya natsionalnoyi systemy kiberbezpeky Ukrayiny" [*Concerning the National Cybersecurity System of Ukraine*], nauk.-analit. zb. "Stratehichni priorytety", [*Strategic Priorities*] Science-analyst. every quarter save, Kyiv, View of NISS, No. 4 (29), p. 127-130.

19.Shelomentsev,V (2012) "Pravove zabezpechennya systemy kibernetychnoyi bezpeky Ukrayiny ta osnovni napryamy yiyi udoskonalennya" [*Legal support of the system of cybernetic security of Ukraine and the main directions of its improvement*], "Borotba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka)" zb. nauk. prats, [*Fighting organized crime and corruption (theory and practice)*] sciences works save. No. 1 (27). - P. 312-320.

20.Yatsyshyn,M. (2015) "Mizhnarodno-pravova protydiya kiberviynam" [*International legal counteraction to cyberwarfaces*], zbirnyk prats Natsionalnoho aviatsiynoho universytetu [*The National Aviation University publication collection*] № 1, p. 67-71.

21.Vdovenko,S and Danyk,Y (2017) "Kontseptualni napryamy kompleksnoho vyrishennya problemy zakhystu informatsiyi v systemi skrytoho upravlinnya Zbroynykh syl" [*Conceptual approaches for complex solution of information security in the code c2 of the armed forces*], *Modern Information Technologies in the Sphere of Security and Defence № 2 (29)/2017*

22.Vdovenko,S and Danyk,Y (2017) "Kontseptualni napryamky kompleksnoho vyrishennya problemy zakhystu vid nesanktsionovanoho dostupu v skladnykh systemakh spetsialnoho pryznachennya." [*Conceptual directions of the complex solution of the problem of protection against unauthorized access in complex systems of special purpose*], Abstracts of the 6th International Scientific and Technical Conference, Vinnytsia, 24-25.10.2017, p. 61-64.

23. Guk O., Cherednychenko O,, Shtonda R. and, Duba I. (2017) "Dii v kiberprostori pid chas pidgotovki ta vedennia merezhecentrychnoi vijny" [*Action in cyberspace during the preparation and conduct of network centric war*], *Modern Information Technologies in the Sphere of Security and Defence № 2 (29)/2017*

24. Andress,J., Winterfeld,S. and Rogers,R. (2011) "Cyber warfare: Techniques, tactics and tools for security practitioners" , – Amsterdam: Syngress/Elsevier, 2011. – 289 p

25.The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0. Tallinn 2016. Режим доступу - http://csef.ru/media/articles/3990/3990.pdf

26.Zakon Ukrayiny "Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny" № 2163-VIII 10/05/2017, [*Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine*] No. 2163-VIII of October 5, 2017. Available: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi

27.Stratehiia kiberbezpeky Ukrainy [*The strategy cyber security of Ukraine*.], of was approved by the Decree of the President of Ukraine dated March 15, 2016, No. 96/2016

28.Kontseptsiia rozvytku sektoru bezpeky i oborony Ukrainy [*Concept of development of the security and defense sector of Ukraine*], put into effect by the Decree of the President of Ukraine dated March 14, 2016, No. 92/2016.

29. Available: https://glavcom.ua/world/observe/venesuela-zalishilasya-bez-elektriki-575648.html

30. Available: https://vesti-ukr.com/mir/328311-blekaut-v-venesuele-khuan-huajdo-reshil-vvesti-rezhim-chp

31. Available:https://www.facenews.ua/news/2019/443568/

д.т.н., проф. Даник Ю.Г, Вдовенко С.Г.

ЭФФЕКТ ЦЕПНЫХ РЕАКЦИЙ В КИБЕРДЕЙСТВИЯХ

В статье представлены результаты исследований особенностей гибридной войны, которая происходит в Украине и других государствах в киберпространстве. Установлены роль и место цепных эффектов и асимметричных деструктивных действий в сфере информационной и кибербезопасности. В связи с тем, что в настоящее время энергетика является базовой отраслью национальной экономики и национальной безопасности любого государства, особенности комплексных деструктивных кибер, информационных и когнитивных действий и влияний в киберпространстве и через киберпространство рассмотрены на примере энергетической сферы с учетом угроз, рисков и особенностей кибервоздействий на системы и объекты критической инфраструктуры топливно-энергетического комплекса. Актуальность обеспечения энергобезопасности стран мира растет, о чем свидетельствует обзор энергетических стратегий развития Евросоюза, США и других стран. По взглядам ряда отечественных и иностранных специалистов, энергетика в области экономики превратилась в инструмент геополитики. От ее эффективного, надежного и устойчивого функционирования в значительной степени зависят уровень национальной безопасности государства в целом, темпы структурных преобразований в экономике, обеспечение потребностей населения, общественного производства и обороны. Применение на объектах критической инфраструктуры государства современных компьютерных, информационно-телекоммуникационных и кибертехнологий требует внедрения и осуществления мероприятий по кибербезопасности, противодействия кибертерроризму и обеспечения кибероборонны. Определены наиболее важные аспекты защиты от этих воздействий, предложенные подходы по разработке обоснованных организационных и технических мероприятий по обеспечению кибербезопасности общества и государства в современных условиях.

Ключевые слова: кибербезопасность, кибероборона, комплексные информационно-кибернетические воздействия, объекты энергетики, распределенно-сосредоточенные кибервоздействия, кибервоздействия с эффектом цепных реакций.

prof. Y. Danyk, S.Vdovenko

A CHAIN EFFECTS IN THE CYBER-ACTIONS

The article presents the results of research on the features of the hybrid war that occurs in Ukraine and other states in cyberspace. Established role and place of chain effects and asymmetric destructive actions in the field of information and cyber security. Due to the fact that at present energy is the basic industry of national economy and national security of any state, the features of complex destructive cyber-, informational and cognitive actions and influences in cyberspace and through cyberspace are considered on the example of the energy sphere taking into account threats. , risks and features of cyber-impacts on systems and objects of the critical infrastructure of the fuel and energy complex. The urgency of ensuring energy security of the countries of the world is increasing, as evidenced by the revision of energy development strategies of the European Union, the United States, and other countries. According to the views of a number of domestic and foreign specialists, energy in the field of economics has become an instrument of geopolitics. The level of national security in general, the pace of structural transformation in the economy, the provision of the needs of the population, social production and defense depend to a large extent on its effective, reliable and sustainable functioning. The use of state-of-the-art computer, information-telecommunication and cyber-tech equipment in state critical infrastructure objects requires the implementation and implementation of measures on cyber security, countering cyberterrorism and providing cyber defense. The most important aspects of these influences are identified, approaches are offered for the development of sound organizational and technical measures to ensure the cyber security of society and the state in modern conditions.

Keywords: cybersecurity, cyber defense, integrated information-cybernetic influence, energy objects, distributed-concentrated cyber impact, cyber impact with chain effect.