DOI: https://doi.org/10.17721/ISTS.2020.1.31-39
УДК 681.3.06

ПРОБЛЕМИ ЗАХИСТУ КРИТИЧНО ВАЖЛИВИХ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ

Лукова-Чуйко Наталія[1]
orcid.org/0000-0003-3224-4061

Наконечний Володимир[2]
orcid.org/0000-0002-0247-5400

Толюпа Сергій[3]
orcid.org/0000-0002-1919-9174

Зюбіна Руслана[4]
orcid.org/0000-0002-8654-6981

м. Київ, Київський національний університет імені Тараса Шевченко e-mai: [1]lukova@ukr.net, [2]nvc2006@i.ua, [3]tolupa@i.ua, [4]ziubina@knu.ua

Історія статті:
Надійшла до редакції 21.07.2019
Прийнято 29.07.2019

Ключові слова:
національна стратегія;
кібербезпека;
кібертероризм;
кіберзагроза;
критично важливий об'єкт інфраструктури

Анотація: *У роботі висвітлені актуальні питання, пов'язані із захистом критично важливих об'єктів інфраструктури, від функціонування яких залежить виживання людської спільноти. Показано, що стрімкий прогрес в сфері інформаційних технологій, з одного боку дозволяє сучасним економікам багатьох країн стати нерозривно взаємопов'язаними, з іншого боку цей процес піддає людство цілому ряду безпрецедентних загроз, які прагнуть дестабілізувати суспільне життя, втручаючись в роботу критично важливих об'єктів інфраструктури. Проведено аналіз того, що є істинними причинами такої пильної уваги до подібних об'єктів з боку кібертерористів. Представлені топ 10 основних загроз для промислових систем управління. Вказані кроки визначення відповідної критичності об'єктів інфраструктури. Наведено список 11 критично важливих секторів і 37 відповідних підсекторів, визначених Європейським Союзом. Запропоновано відповідь на питання, з якою метою країнам слід розробляти загальнонаціональні стратегії захисту критично важливих об'єктів інфраструктури. Запропонована стратегія кількісної оцінки рівня захищеності критично важливих об'єктів інфраструктури від ризику стороннього кібернетичного впливу. Обгрунтовано необхідність об'єднання державами різних елементів захисту критично важливих об'єктів інфраструктури. Зазначено, що політики в області кібербезпеки повинні займати центральне місце в захисті критично важливих об'єктів інфраструктури. Відзначено, що не всі національні стратегії кібербезпеки забезпечують однакове місце і значимість для критично важливих об'єктів інфраструктури. Зазначено, що при розробці національної стратегія щодо захисту критично важливих об'єктів інфраструктури, важливо скласти повний перелік всіх національних політик, що мають до неї відношення. Зроблено висновок про те, що є важливим інструментом для захисту критично важливих об'єктів інфраструктури, на сьогоднішній день.*

Abstract: *The paper deals with topical issues related to the protection of critical infrastructure, which depend on the survival of the human community. It is shown that rapid progress in the field of information technology, on the one hand, allows the modern economies of many countries to become inextricably interconnected; interfering with the work of critical infrastructure. The analysis of what are the true causes of such close attention to such objects by cyber terrorists. Top 10 major threats to industrial control systems are presented. The following steps determine the criticality of the infrastructure objects. The following is a list of 11 critical sectors and 37 relevant sub-sectors identified by the European Union. The answer is given to the question with which target countries should develop national strategies for the protection of critical infrastructure objects. A strategy for quantifying the level of security of critical infrastructure against the risk of third-party cybernetic exposure is proposed. The necessity to unite different elements of protection of critical infrastructure objects by states is substantiated. It is important that cybersecurity policies should be central to the protection of critical infrastructure. It is noted that not all national cybersecurity strategies provide the same place and relevance for critical infrastructure. It is noted that when developing a national strategy for the protection of critical infrastructure, it is important to compile a comprehensive*

list of all relevant national policies. It is concluded that today it is an important tool for the protection of critical infrastructure.

1. ВСТУП

Завдяки стрімкому прогресу в сфері інформаційних технологій (ІТ) сучасні економіки багатьох країн стали нерозривно взаємопов'язаними, що підвергає людство низці безпрецедентних загроз і чинників уразливості. Багато з них походять від терористичних груп і хакерів які прагнуть дестабілізувати суспільне життя, втручаючись в активи і процеси, від яких залежить виживання людської спільноти. Такі активи і процеси є центральними вузлами, відомими як критично важливі об'єкти інфраструктури (КВОІ).

Заміщення фізичного світу цифровим і настання епохи life 3.0, з одного боку, дозволяє людству здійснювати контроль інфраструктури з будь-якої точки світу, але з іншого боку, з'являються фактори уразливості до погроз. Це означає, що при високій взаємозалежності інфраструктури на рівні секторів і галузей, «вдала» атака на КВОІ з боку кібертерористів може привести до порушення або зруйнування життєво важливих систем безпосередньо в самій країні і, за ланцюговою реакцією, у всьому світі.

На думку групи урядових експертів з досягнень в області інформатизації і телекомунікації, в контексті міжнародної безпеки, «використання ІТ в терористичних цілях, крім вербування, фінансування, навчання і підбурювання, в тому числі для терористичних атак проти ІТ або ІТ-залежної інфраструктури, збільшує ймовірність того, що, якщо це залишити без уваги, може виникнути загроза загальному миру і безнебезпеці» [1].

Дана обставина є важливим фактором для кібертерористів і поряд з тим, що інфраструктура багатьох країн розвивається колосальними темпами, зброя кібертерористів також стає все більш витонченою. У зв'язку з цим, захист критично важливих об'єктів інфраструктури від навмисних кіберінцидентів зі сторони окремих осіб, організацій або країн є надзвичайно актуальною проблемою з якою зіткнулося людство XXI сторіччя.

2. ПОСТАНОВКА ПРОБЛЕМИ

Народження захисту КВОІ стало наслідком терористичних подій 11 вересня 2001 року. І хоча за своєю природою кіберзагрози відрізняються від фізичних погроз, кінцевий результат може бути однаково сумним.

Загрози щодо КВОІ можуть бути або окремими або випадковими діями, або частиною більш широкого плану по атаці на інфраструктуру в одному і тому ж секторі (наприклад, дамби, греблі, гідроелектростанції). Виявлення взаємозв'язків і закономірностей в подібних сценаріях часто вимагає наявності серйозних аналітичних інструментів і обробки інформації з великих і різнорідних джерел.

Однак, на жаль, інформація про більшість кібератак не публікується. Це зазначає ОБСЄ в «Керівництві по передовій практиці щодо захисту неядерної критично важливою енергетичної інфраструктури від терористичних атак з акцентом на загрози, які виходять з кіберпростору», щоб ще більше ускладнити ситуацію щодо енергетичного сектора, інформація про більшість кібератак не публікується, оскільки відповідні оператори не хочуть повідомляти про ці інциденти. Проте, здатність розпізнавати основну динаміку і методи якомога раніше є ключовим фактором, що дозволяє владі обмінюватися оперативною інформацією. Це підвищує здатність ефективніше реагувати на поточні атаки і запобігати неминучі атаки проти ймовірних жертв [2].

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Дотримання принципів безпеки дозволить сформувати низку вимог до системи кібербезпеки КВОІ, уникнути проблем пов’язаних з занадто високою вартістю реалізації цих вимог, неможливістю ефективного контролю за їх виконанням та важкістю їх засвоєння виконавцями, а також повністю нівелювати ризики усіх можливих загроз для КВОІ. Разом з цим саме контроль за виконанням вимог до кібербезпеки може привести, як відомо, до бажаного результату. Так, наприклад, якщо частина вимог не може бути реалізованою через брак коштів – саме ефективний контроль дозволить раціонально розподілити вирішення проблем, що виникають у процесі створення інформаційних систем КВОІ та її експлуатації. Відсутність ефективного контролю за виконанням вимог з боку виконавців може привести до оптимізації роботи останніх за рахунок ігнорування вимог по безпеці тощо.

У системах, де організований всеосяжний контроль усіх вимог, окрім величезної кількості інструкцій, наказів, законодавчих і підзаконних актів, у яких вони формулюються, як правило складаються списки вимог до підконтрольних структур і процесів. Наявність такого роду списків дозволить як контролерам, так і виконавцям швидше осягнути усю систему вимог, швидше їх освоїти й, відповідно, краще їх виконувати.

У деяких випадках то, що виглядає як окрема атака спрямована на відносно «неважливі» цілі, насправді, може бути частиною більш амбітних кримінальних стратегій [3].

Аналізуючи питання, що ж є причинами такої пильної уваги до КВОІ з боку кібертерористів,

можна припустити, що по-перше, вони можуть бути «привабливою метою» через свою стратегічну цінність для суспільства, особливо в високорозвинених індустріальних країнах. Втручання в функціонування КВОІ, з можливістю генерування каскадних ефектів, дозволить кібертерористам максимізувати збиток «вдалою» кібератакою і насаджувати страх до рівнів, які не могли б бути досягнуті, напавши на «рядові» об’єкти.

Інші КВОІ можуть бути «привабливими» для кібертерористів демонстрацією безсилля державних установ.

Третьою мотивацією, пов'язаною з двома попередніми, є бажання отримати більш високий рівень суспільного розголосу, що неможливо було б здійснити, зосередивши увагу на «звичайних» об'єктах.

Однак, як це не парадоксально, кібертерористи можуть домагатися контролю над КВОІ не для того, щоб завдавати шкоди або залякувати, а за зовсім іншою причиною - бажання встановити власну соціальну значущість.

В окремих випадках існує сукупність факторів, що спонукають кібертерористів здійснювати напади на КВОІ.

Остаточне рішення щодо цільової інфраструктури буде залежати від оперативних можливостей кібергрупи для запуску конкретної кібератаки. І захисні заходи, прийняті на певному КВОІ, природно, будуть, впливати на таке рішення., зосередивши увагу на «звичайних» об'єктах.

У той час як взаємопов'язані і інтегровані комп'ютеризовані системи управління істотно спростили методи роботи КВОІ і розширили можливості їх мережевої взаємодії, стало також можливим збільшення площі кібератаки і, отже, зросла вірогідність піддати КВОІ високому ризику порушення їх функціонування.

Відомі, як мінімум, 10 основних загроз для промислових систем управління, які представлені в таблиці 1 [2].

Таблиця 1. Топ 10 загроз для промислових систем управління

№	Загроза	Пояснення
1	Несанкціоноване використання точок доступу віддаленого обслуговування.	Точки доступу для технічного обслуговування - це спеціально створені зовнішні входи в мережу ІТ, які часто недостатньо захищені.
2	Мережеві атаки через офісні або корпоративні мережі.	Офісні ІТ зазвичай пов'язані з мережею декількома способами. У більшості випадків мережеві з'єднання з офісів в мережу ІТ також існують, тому зловмисники можуть отримати доступ по цьому маршруту.
3	Атаки на стандартні компоненти, що використовуються в мережі ІТ.	Стандартні ІТ-компоненти (комерційні готові продукти (COTS)), такі як системне програмне забезпечення, сервери додатків або бази даних, часто містять недоліки або уразливості, які можуть бути використані зловмисниками.
4	Атаки на мережеві компоненти.	Зловмисники можуть маніпулювати мережевими компонентами, наприклад, для проведення атак «зловмисник в середині» або для полегшення прослуховування.
5	Атаки типу "відмова в обслуговуванні".	Розподілені атаки типу "відмова в обслуговуванні" можуть послабити мережеві з'єднання і найважливіші ресурси і привести до відмови систем, наприклад, для порушення роботи ІТ.
6	Людська помилка і саботаж.	Умисні дії, вчинені як внутрішніми, так і зовнішніми зловмисниками, являють собою серйозну загрозу для будь-яких цілей захисту. Недбалість і людська помилка також є більшою загрозою, особливо щодо конфіденційності та доступності цілей захисту.
7	Впровадження шкідливого ПО через знімні носії і зовнішнє обладнання.	Використання знімних носіїв і мобільних ІТ-компонентів зовнішнього персоналу завжди тягне за собою великий ризик зараження шкідливим ПЗ.
8	Читання і опублікування новин в мережі ІТ.	Більшість компонентів управління в даний час використовують протоколи з відкритим текстом, тому зв'язок не захищений. Це дозволяє відносно легко читати і вводити команди управління.
9	Несанкціонований доступ до ресурсів.	Внутрішні зловмисники і наступні атаки після початкового зовнішнього проникнення роблять це особливо простим, якщо служби та компоненти в мережі процесів не використовують методи аутентифікації і авторизації або якщо ці методи небезпечні.
10	Форс-мажорні обставини або технічні несправності.	Перебої, викликані екстремальною погодою або технічними несправностями, можуть відбутися в будь-який час - ризик і потенційний збиток можуть бути зведені до мінімуму тільки в момент виникнення таких випадків.

У процесі захисту КВОІ надзвичайно важливе розуміння того, які об'єкти інфраструктури є критично важливими. Так в Резолюції Ради Безпеки 2341 (2017) прямо говориться про те, що «кожна держава визначає, що становить його критично важливі об'єкти інфраструктури».

Проте, вона не рекомендує будь-який конкретний метод вибору для виділення КВОІ серед безлічі об'єктів інфраструктури, розташованих на їх територіях.

Інші міжнародні документи також не дають ніяких вказівок. Таким чином, країнам надається більша свобода дій при виборі критеріїв для визначення того, які об'єкти інфраструктури, що діють на їх території, відповідають порогу «критичності». Завдання досить складне.

Різниця між значущими об'єктами інфраструктури і тими, які повинні отримати статус «критично важливих», є ключовим фактором, що дозволяє розставити пріоритети щодо обмежених ресурсів для захисту величезних активів, систем і процесів.

З одного боку, включення занадто великої кількості інфраструктур в категорію «критично важливих» є фінансово нестійким і може стати некерованим завданням. З іншого боку, надто обмежувальний підхід може залишити ряд ключових активів і процесів незахищеними з потенційно катастрофічними наслідками в разі аварії.

Існує тенденція урядів розширювати досить вузькі національні списки КВОІ тому, що «занадто мало осіб, які приймають рішення, готові прийняти політичний ризик, який може виникнути при видаленні елемента з «критично важливого» списку, і виникає спокуса постійно розширювати коло об'єктів, які вважаються критично важливими.

Двозначність марнотратна, оскільки ресурси не направляються туди, де вони можуть надати найбільший вплив [4]

На сьогоднішній день Україна також зіткнулася з проблемою відбору своїх КВОІ. При цьому, в жодному із законодавчих документів України не прописано процедуру процесу ідентифікації КВОІ, тому, для відповіді на це питання можна звернутися до світового досвіду. Отже спробуємо розібратися в цьому процесі.

Першим кроком в процесах ідентифікації КВОІ зазвичай є прийняття всеосяжного визначення того, що мається на увазі під КВОІ. Це корисно для створення фундаменту, на якому будуть розроблятися подальші політичні та нормативні рамки.

В цілому, в той час як визначення деяких країн підкреслюють призначення інфраструктури (тобто критичність пов'язана з виконанням основних соціальних функцій), інші роблять упор на наслідки руйнування або збою (тобто критичність обумовлена конкретними наслідками переривання обслуговування).

КВОІ можуть бути визначені, серед іншого, з урахуванням тієї ролі, яку вони грають в просуванні і захисті прав людини, а також вплив на права людини, яке може статися через пошкодження, порушень або руйнувань об'єктів інфраструктури.

Такий підхід відповідає існуючим визначенням. Наприклад, Європейський Союз (ЄС) визначає КВОІ як «актив, систему або її частину», яка «необхідна для підтримання життєво важливих функцій суспільства, здоров'я, безпеки, збереження, економічного або соціального благополуччя людей», порушення або руйнування яких матиме значний вплив «в результаті недотримання цих функцій» [5].

Цей крок в Україні вже майже зроблений. В проекті закону України “Про критичну інфраструктуру та її захист” в пунктах 10 та 11 статті 1 цього проекту дається визначення критичній інфраструктурі та об’єкту критичної інфраструктури відповідно.

Критична інфраструктура - об’єкти, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Об’єкт критичної інфраструктури - визначений у встановленому законодавством порядку складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якої забезпечують реалізацію життєво важливих національних інтересів.

Одним із суб’єктів, що забезпечують захист КВОІ є діяльність РНБО України, яка повинна координувати роботу правоохоронних та інших органів у сфері кібербезпеки та, наприклад, її координаційний центр ніяк не може запрацювати на повну тільки тому, що у самому РНБО ніяк не вдається скоординувати блоки захисту, інформаційні та силові блоки в один вузол, щоб швидше реагувати на кіберзагрози.

Також є проблеми й в такому важливому процесі, як співробітництво спеціальних структур з приватним бізнесом, який має власний досвід і напрацювання протидії кіберзагрозам.

Силовики нерідко зловживають своїми повноваженнями створюючи перешкоди для бізнес-партнерів. Від цього довіра один до одного тільки втрачається і вже ні про яке співробітництво не може йти мова. А звідси – і про посилення кібербезпеки держави.

В свою чергу, на державному рівні питання кіберзахисту повинне набути системного характеру. Можна довго говорити про важливість і актуальність посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі і зростання ролі в цьому приватного сектора; встановлення контролю над кіберзброєю, а також посилення охорони критичної інфраструктури України; впровадження інновацій в сфері кібербезпеки та активізації дискусій щодо пошуку нових джерел фінансування засобів кібербезпеки; вдосконалення освітніх напрямів підготовки фахівців даної сфери діяльності; активізацію на національному та міждержавно-

му рівнях обміну інформацією про кібератаки, тощо.

Однак без системного та комплексного підходу всі зазначені кроки не дозволять вивести рівень кібербезпеки, а звідси – і національної безпеки України загалом, на новий якісний рівень.

Другий етап в ідентифікації КВОІ є найбільш складним, з огляду на те, що саме тут відбувається «розстановка пріоритетів». Цей етап, як правило, спрямований на виявлення секторів, які розглядаються як критично важливі.

Початковий підхід міг би полягати в розгляді інших країн, які мають схожі соціальні, географічні особливості, а також порівняний рівень технічного і економічного розвитку.

Ряд секторів, швидше за все, будуть розглядатися як «критично важливі» у всіх країнах. При цьому важливо відзначити, що певний сектор або підсектор може мати вирішальне значення для однієї конкретної сфери, але не для іншої. Розмір і особливості певної національної економіки можуть визначити, що є критичним, а що менш критичним. Крім того, той факт, що певний сектор позначений як критично важливий, не повинен автоматично означати, що всі базові служби є критично важливими. Беручи до уваги ці відмінності, країни в значній мірі приходять до аналогічних висновків.

У таблиці 2 наведено список з 11 секторів і 37 відповідних підсекторів, визначених ЄС [6].

Таблиця 2. Орієнтовний список секторів і підсекторів, визначених ЄС

1	Енергетика	1 Видобуток, переробка, обробка та зберігання нафти і газу, включаючи трубопроводи. 2 Виробництво електроенергії. 3 Передача електроенергії, газу та нафти. 4 Розподіл електроенергії, газу та нафти.
2	Інформаційні, комунікаційні технології.	5 Інформаційна система і захист мережі. 6 Інструменти автоматизації і управління системами. 7 Інтернет. 8 Надання фіксованих телекомунікаційних послуг. 9 Надання мобільного зв'язку. 10 Радіозв'язок і навігація. 11 Супутниковий зв'язок. 12 Телерадіомовлення.
3	Вода.	13 Забезпечення питною водою. 14 Контроль якості води. 15 Розробка свердловин і контроль кількості води.
4	Їжа.	16 Забезпечення продовольством і продовольчої безпеки.
5	Охорона здоров'я.	17 Медична і лікарняна допомога. 18 Ліки, сироватки, вакцини та фармацевтика. 19 Біолабораторії й біоагенти.
6	Фінансування.	20 Платіжні послуги / платіжні структури (приватні). 21 Державне фінансове асигнування.
7	Громадський та правовий порядок і безпека.	22 Підтримка громадського та правового порядку, охорони і безпеки. 23 Виконання правосуддя і утримання під вартою.
8	Громадська адміністрація.	24 Урядові функції. 25 Збройні сили. 26 Послуги цивільної адміністрації. 27 Служби порятунку. 28 Поштові та кур'єрські послуги.
9	Транспорт	29 Дорожній транспорт. 30 Залізничний транспорт. 31 Повітряне сполучення. 32 Водний транспорт у внутрішньому сполученні. 33 Морський та каботажний транспорт.
10	Хімічна і атомна промисловість.	34 Виробництво і зберігання/переробка хімічних і атомних речовин. 35 Трубопроводи небезпечних вантажів (хімічні речовини).
11	Космос	36 Космос. 37 Дослідження.

Третій крок пов'язує раніше встановлені сектори і підсектори зі списком окремих інфраструктурних активів, систем і процесів. Країни розробили безліч наборів показників для визначен-

ня певних інфраструктур як «критично важливих». Ці індикатори зазвичай прагнуть «виміряти» наслідки руйнування об'єктів інфраструктури або функціонального збою і включають комбінацію з географічного охоплення впливу, його тривалості, а також тяжкості потенційних наслідків з точки зору:

- економічних наслідків (вплив на ВВП, прямі і непрямі економічні втрати, чисельність зайнятого персоналу, податкові надходження);
- кількості жертв і масштаби евакуації населення;
- порушення державного управління; шкоди навколишньому середовищу.

Для обґрунтування третього кроку застосовують різноманітні методології. Так, наприклад, консорціум на чолі з голландською дослідницькою організацією, спробував згрупувати їх за трьома основними типами [7]:

1) підхід, заснований на послугах (наприклад, Швейцарія), де уряд ідентифікує критично важливі активи на основі галузевих критеріїв, що визначають порогові значення / кількісне вироблення рівня обслуговування активів, наприклад, кількість доставлених мегават;

2) підхід, заснований на операторі (наприклад, Франція), де завдання визначення того, які активи або послуги є критично важливими, залишається за окремими операторами КВОІ;

3) підхід, заснований на активах або гібридах (наприклад, у Великобританії), в якому використовуються елементи підходів, орієнтовані як на послуги, так на оператора.

Завдання на предмет оцінювання рівня захищеності КВОІ від ризику стороннього кібервпливу належать, як відомо, до класу багатокритеріальних [8]. Для їх колегіального рішення в умовах невизначеності і конфлікту серед існуючих методів математичного моделювання, методів формування та дослідження узагальнених показників якості з використанням графоаналітичного і ним подібних підходів, експертних методів вирішення складних завдань оцінювання та вибору будь-яких об’єктів, в тому числі спеціального призначення, а також аналізу та прогнозування ситуацій з великою кількістю значимих факторів, найбільш раціональними і визначальними є саме експертні методи. Вони дають можливість більш глибоко вивчити явища, які істотно впливають на рівень захищеності як держави в цілому, так і окремих об’єктів її інформаційної та кіберінфраструктури від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз, виявити найбільш важливе та істотне у цих процесах, не опускаючи тих деталей і взаємозв’язків, без яких не може бути побудована модель досліджуваної проблеми.

Метою такої моделі є оцінювання готовності об’єктів інформаційної і кіберінфраструктури до безпечного функціонування в умовах стороннього кібервпливу та встановлення на підставі так званого “індексу кіберпотужності” вимог до власних систем кібербезпеки [9].

Індекс кіберпотужності ($G_{рів.захищ.}$) з точки зору експертів може бути обчислений за формулою:

$$G_{рів.захищ} = (\sum_{i=1}^{n}(g_i \times G)) \times 100\%$$

де g_i – вагові коефіцієнти категорій другого рівня ієрархії $G_{iфакт}$; n – число категорій.

Прийняття рішення щодо здатності держави протистояти кібератакам має здійснюватися за 100-бальною шкалою на підставі такого правила:

- якщо $90 < G_{рів.захищ} < 100$, то рівень захищеності держави від ризику стороннього кібервпливу вважається достатньо високим для підтримки безпечного функціонування об’єктів її інформаційної і кіберінфраструктури;
- якщо $45 < G_{рів.захищ} < 90$, то рівень захищеності держави від ризику стороннього кібервпливу вважається допустимим для підтримки безпечного функціонування об’єктів її інформаційної і кіберінфраструктури;
- якщо $G_{рів.захищ} < 45$, то рівень захищеності держави від ризику стороннього кібервпливу вважається недостатнім.

Таким чином, запропонована стратегія оцінки дає можливість одержати кількісну оцінку рівня захищеності КВОІ від ризику стороннього кібернетичного впливу, встановити вимоги до формування ними власних систем кібернетичної безпеки та розробити заходи спрямовані на підвищення їх результативності.

Підставою таким діям може слугувати виявлення відхилень від штатного режиму функціонування державних інформаційних ресурсів, ІТ систем і мереж, а також відповідних програмних і апаратних засобів [10].

Для захисту КВОІ країни повинні мати відповідну загальнонаціональну стратегію. Досвід показує, що більшість країн забезпечували заходи безпеки для своїх КВОІ задовго до того, як їх захист затвердився в якості самостійного політичного поля.

Відповідні захисні заходи, як правило, приймалися поетапно в формі нормативних актів, що охоплюють конкретні загрози. В окремих випадках державна політика досягала значного рівня складності, відповідаючи високим міжнародним стандартам. Наприклад, в атомній енергетиці Україна розробила сучасну і ефективну систему фізичного захисту ядерних об'єктів і матеріалів.

Виникає питання, для чого таким країнам слід розробляти загальнонаціональні стратегії захисту КВОІ, коли в них уже введені і функціонують подібні нормативні акти, політика і практика, що охоплюють практично всі, критично важливі сектора.

Відповідаючи на це питання, можна припустити, що основна причина цього полягає в тому, що в сучасних суспільствах безпека КВОІ стає все більш складним завданням. Взаємозалежність між секторами з потенціалом для каскадних ефектів в разі кібератак, аварій природного або техногенного походження вимагає необхідності контролювати загальну картину для ефективної координації дій щодо запобігання, реагування і відновлення між секторами.

Така всеосяжна стратегія спрямована, перш за все, на більш ефективний розподіл фінансових і людських ресурсів, раціоналізацію робочих потоків навколо заздалегідь визначених цілей. Це не означає, що загальнодержавні стратегії по захисту КВОІ повинні автоматично замінювати існуючі галузеві заходи захисту, особливо коли ці заходи виявилися успішними чи відповідають обов'язковим міжнародним нормативним рамкам.

Необхідно, щоб держави об'єднували різні елементи захисту КВОІ під загальною егідою і зробили їх частиною єдиної системи управління.

Оскільки захист КВОІ пов'язаний з декількома різними сферами діяльності, основними цілями загальнодержавної стратегії є:

- визначення організаційних структур;
- встановлення вимірюваних цілей і термінів;
- закладка основи для ефективного запобігання та управління інцидентами шляхом гармонізації завдання між різними областями політики.

Більшість країн, у тому числі ті, які не мають спеціальних стратегій захисту критично важливих об'єктів інфраструктури, розглядають питання пов'язані із захистом КВОІ в різних політичних нормативних документах, введених різними урядовими установами. Ці документи зазвичай включають в себе національні, в тому числі і кіберстратегії в області боротьби з тероризмом.

Хоча такі різні політики могли бути прийняті в різний час і різними державними установами, вкрай важливо, щоб вони стали частинами єдиного підходу до захисту КВОІ. Це вимагає визначення країнами:

- взаємодії між цими іншими політиками і спеціальною стратегією захисту КВОІ;
- ступінь, в якій ці інші політики або сама стратегія безпеки КВОІ були скориговані і оптимізовані для запобігання конфліктам та забезпечення загальної координації політики на національному рівні.

Політики в області кібербезпеки займають центральне місце в системі безпеки критично важливих об'єктів інфраструктури, оскільки забезпечують основу, в якій країни визначають цілі і засоби захисту КВОІ і критично важливих інформаційних інфраструктур.

Ряд регіональних інструментів пов'язують концепції кібербезпеки з КВОІ. Стратегія кібербезпеки ЄС 2013 року, відповідно до якої Європейська комісія взяла на себе зобов'язання «продовжувати свою діяльність, що проводиться спільним дослідницьким центром в тісній координації з владою держав-членів і власниками і операторами критично важливої інфраструктури, щодо виявлення уразливості європейських критично важливих об'єктів інфраструктури та стимулювання розвитку відмовостійких систем» [11].

Відповідно до директиви Європейського Союзу 2016/1148 про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем по всьому Союзу, держави-члени ЄС повинні призначити операторів послуг життєзабезпечення (OES) і ввести нові вимоги до безпеки і звітності для таких організацій.

З огляду на це, не всі національні стратегії кібербезпеки забезпечують однакове місце і «вагу» для КВОІ. Між країнами існують значні відмінності. Деякі стратегії були написані тільки з точки зору кіберзлочинності і, як правило, не беруть до уваги національні явища дестабілізації, міжгалузеві впливи і антикризове управління для КВОІ. Стратегії, написані з точки зору кібербезпеки, засновані на національній оцінці ризику, візьмуть ширшу перспективу, яка дасть місце для захисту КВОІ ... » [12].

Важливим інструментом, запропонованим міжнародним союзом електрозв'язку (МСЕ), є сховище національних стратегій з кібербезпеки (NSC). Воно включає в себе велику колекцію національних стратегій з кібербезпеки, чи то у формі одного або декількох документів, або як частина більш широких стратегій в сфері ІТ або національної безпеки [13].

З огляду на розмаїття підходів між різними існуючими стратегіями щодо захисту КВОІ і кібербезпеки, МСЕ в даний час очолює зусилля з різними глобальними учасниками по створенню загального довідкового керівництва національних стратегій з кібербезпеки.

Цей документ покликаний дати країнам чітке уявлення про мету і зміст національної стратегії з кібербезпеки, показати в загальних рисах існуючі моделі і ресурси, спрямовувати країни в процесі розробки своїх стратегій та їх оцінки [13].

4. ВИСНОВКИ

Проведений в даній роботі аналіз дозволяє зробити висновок про актуальність проблеми захисту КВОІ. При цьому показано, що зі збільшенням прогресу в сфері ІТ з'явилася можли-

вість сучасним економікам багатьох країн стати нерозривно взаємопов'язаними. Проте цей процес, в свою чергу, ставить перед людством цілу низку безпрецедентних загроз, які впливаючи на роботу КВОІ дестабілізують суспільне життя.

Проведений в роботі аналіз виявив справжні причини пильної уваги до КВОІ з боку кібертерористів. При цьому, виявлені як мінімум три основні причини такої «привабливості». В роботі представлені топ 10 основних загроз для промислових систем управління. Запропоновані кроки визначення відповідної критичності об'єктів інфраструктури і наведено список 11 секторів і 37 відповідних критично важливих підсекторів, визначених ЄС.

Запропонована стратегія кількісної оцінки рівня захищеності критично важливих об’єктів інфраструктури від ризику стороннього кібернетичного впливу.

Дана відповідь на питання, з якою метою країнам слід розробляти загальнонаціональні стратегії захисту критично важливих об'єктів інфраструктури та обґрунтовано необхідність об'єднання державами різних елементів захисту КВОІ під загальною егідою з метою зробити їх частиною єдиної системи управління.

Показано, що політики в області кібербезпеки повинні займати центральне місце в захисті КВОІ. При цьому зазначено, що не всі національні стратегії кібербезпеки забезпечують однакове місце і значимість для КВОІ.

Показано, що при розробці національної стратегія щодо захисту КВОІ, важливо скласти повний перелік всіх національних політик, що мають до неї відношення.

Зроблено висновок про те, що важливим інструментом для захисту КВОІ, на сьогоднішній день, є сховище національних стратегій з кібербезпеки, запропонований міжнародним союзом електрозв'язку.

5. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] GGE 2015, Report of the Group of Governmental Experts on Information and Telecommunication Events in the Context of International Security, General Assembly, [Online].: https://ccdcoe.org/sites/default/files/documents/UN-150722- GGEReport2015.pdf.

[2] OSCE 2013, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, , 2013, [Online], : www.osce.org/atu/103500?download=true.

[3] Ackerman 2007, Assessing Terrorist Motivation for Attacking Critical Infrastructures, Nonproliferation Research Center, Monterey Institute for International Studies, [Online]. https://e-reports-ext.llnl.gov/pdf/341566.pdf.

[4] Clemente, 2013, Cybersecurity and Global Interdependence: What is Critical? Chatham House, February 2013, [Online]. www.chathamhouse.org/sites/files/chathamhouse/pulic/Research/International%20Security/0213prcvber.pdf.

[5] Council Directive 2008/114 / EC, Life Safety, General Secretariat for Defense and National Security). Article 2.

[6] European Commission 2005, Green Paper on the European Program for the Protection of Critical Infrastructure, COM (2005) 576 total.

[7] RECIPE 2011, Good Practice Guide for PKI Policies and for Politicians in Europe, [Online]. https://Users/SM/Downloads/RECIPE_manual%20(1).pdf.

[8] Бурячок В.Л., Толюпа С.В., Толубко В.Б., Хорошко В.О. «Інфо-рмаційна та кібербезпека: соціотехнічний аспект» // Навчальний посібник. – К.: Наш формат, 2015. – 288с.

[9] Serhii Toliupa, Hanna Shvedova and Ivan Parkhomenko. Security and Regulatory Aspects of the Critical Infrastructure Objects Functioning and Cyberpower Level Assesment. 3rd IEEE International Conference On Advanced Information and Communication Technologies (AICT) – 2019. Lviv, Ukraine. Scopus/

[10]. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

[11] European Commission 2013 bis. Working Paper on a New Approach to the European Critical Infrastructure Protection Program - Building a Safer European Critical Infrastructure, SWD (2013) 318 total/ [Online]. https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

[12] The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, [Online]. https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

[13] National Cybersecurity Strategies Repository, [Online]. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

Лукова-Чуйко Наталія Вікторівна
Доктор технічних наук , доцент, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
Інтереси: інформаційні технології, криптографія, інформаційна та кібербезпека.
Наука: автор більше 60 наукових праць.

Наконечний Володимир Сергійович
Доктор технічних наук, старший науковий співробітник, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
Інтереси: системи розпізнавання багатопозиційного базування, системи технічного захисту інформації, кібербезпека та кіберзахист.
Наука: автор більше 130 наукових праць.

Толюпа Сергій Васильович
Доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
Інтереси: інтелектуальні системи управління, напрямки підвищення ефективності функціонування інформаційних технологій, системи технічного захисту інформації, кібербезпека та кіберзахист..
Наука: автор більше 160 наукових праць.

Зюбіна Руслана Віталіївна,
Вищу освіту здобула у Національному авіаційному університеті у 2013 році. , Зараз працює асистентом кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченко. Наукові інтереси: інформаційна безпека, кібербезпека, інформаційні технології.