https://orcid.org/0000-0002-5080-1856
https://orcid.org/0000-0003-3604-2256

УДК 004.056.5

Ю.М. ЛИСЕЦЬКИЙ[*], С.І. БОБРОВ[*]

ДЕЯКІ АСПЕКТИ ПОБУДОВИ СИСТЕМИ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ

[*]ДП «ЕС ЕНД ТІ УКРАЇНА», м. Київ, Україна

Анотація. *В умовах сучасних кіберзагроз необхідно постійно вдосконалювати систему національної кібербезпеки. Цим питанням у даний час приділяється дуже серйозна увага на державному рівні в багатьох країнах, зокрема, і в Україні. Це цілком зрозуміло, тому що від рівня безпеки інформаційних систем державних і силових відомств, об'єктів критичної інфраструктури залежать не лише стабільність та надійність їх функціонування, але часто й життя багатьох людей. Указами Президента України і Законами України визначені стратегія кібербезпеки держави, основні засади забезпечення кібербезпеки, заходи забезпечення захисту об'єктів критичної інфраструктури та заходи щодо нейтралізації кіберзагроз, основні завдання нашої держави у сфері кібербезпеки, а також основні суб'єкти забезпечення кібербезпеки. Основою системи національної кібербезпеки є центри виявлення, управління та реакції на кіберзагрози. Використовуючи системний підхід, можна побудувати концептуальну модель системи національної кібербезпеки у вигляді трирівневої піраміди. В основу цієї моделі покладено концепцію єдиного інформаційного простору для обміну даними про кіберінциденти як в середині країни, так і за її межами, та принципи цілісності, ієрархічності, структуризації, множинності, системності. Для підвищення ефективності боротьби з кіберзагрозами на рівні країни організовано взаємодію центрів та обмін інформацією про виявлені кіберінциденти. Зважаючи на те, що останнім часом протистояння у кіберпросторі посилюється і становить реальну загрозу для держав, систему кіберзахисту в Україні необхідно розвивати та вдосконалювати з урахуванням рівня сучасних загроз. Державним організаціям, що відповідають за кіберзахист, треба постійно актуалізувати вимоги щодо кіберзахисту, яких мають дотримуватися всі об'єкти критичної інфраструктури, визначити повний список таких об'єктів і уточнювати його в разі потреби. Керівникам цих об'єктів необхідно впроваджувати досить надійну систему кіберзахисту з урахуванням усіх вимог.*

Ключові слова: *кіберзагрози, кіберінциденти, кіберпростір, кіберзахист, кібербезпека, критична інфраструктура, стратегія, центри протидій кіберзагрозам, інформаційний простір.*

Abstract. *Today's cybersecurity threats necessitate continuous improvement of the national cybersecurity system. A lot of attention is paid to this issue at the state level in many countries, including Ukraine. It is completely justified, since the level of security of information systems used by state and law enforcement agencies, as well as by critical infrastructure objects is essential not only for the stability and reliability of their operation but also and very often for the lives of people. Decrees of the President of Ukraine and Laws of Ukraine define national cybersecurity strategy, essential cybersecurity measures, measures to ensure cybersecurity of critical infrastructure objects and neutralize cybersecurity threats, main tasks of our state in the field of cybersecurity and major subjects which ensure cybersecurity. National system of cybersecurity is based on the centers of detection, management and response to cybersecurity threats. Based on the system approach, there can be built a concept of the national cybersecurity system visualized as a three-level pyramid. This model is based on the concept of the common information space to exchange data on cybersecurity incidents inside the country and internationally. The model also employs such principles as integrity, hierarchy, structuring, multiplicity and consistency. In order to increase efficiency of response to cybersecurity threats at the national level, co-operation of centers is established and exchange of information about detected cybersecurity incidents is made. Considering the fact that confrontation in the cyberspace intensifies and poses real danger to states, there is an urgent need for development and improvement of the cybersecurity system of Ukraine to respond to modern threats.*

ISSN 1028-9763. Математичні машини і системи. 2021. № 2

Responsible for cybersecurity state bodies have to continuously update cybersecurity requirements for all objects of critical infrastructure, define the list of such objects and amend it when necessary. Top executives of such objects have to implement a fairly reliable cybersecurity system, taking into account all the requirements.
Keywords: *cybersecurity threats, cybersecurity incidents, cyberspace, cybersecurity, cybersecurity, critical infrastructure, strategy, centers of response to cybersecurity threats, information space.*

DOI: 10.34121/1028-9763-2021-2-15-22

1. Вступ

У червні 2015 року Україна зазнала кібератаки від вірусу-здирника Petya.A, яку було спрямовано на об'єкти критичної інфраструктури: Чорнобильську атомну станцію, міжнародні аеропорти «Бориспіль» та «Київ», Укрзалізницю, Київський метрополітен, Укрпошту, Ощадбанк та Укргазбанк.

Хоча кібератака Petya.A і не завдала непоправної шкоди, але саме тоді стало зрозуміло, наскільки ця зброя ефективна, що за її допомогою можна паралізувати практично всю країну. Стало також очевидним, що наступна масштабна кібератака може призвести і до людських жертв, оскільки за допомогою комп'ютера, перебуваючи за тисячі кілометрів від об'єкта атаки, можливо відключити електропостачання для цілого регіону, відкрити шлюзи на водосховищі, паралізувати рух авіаційного, залізничного та автомобільного транспорту [1]. Висновок беззаперечний: в Україні необхідно створювати надійну та ефективну систему кіберзахисту.

І це цілком зрозуміло, тому що від рівня безпеки інформаційних систем державних і силових відомств, об'єктів критичної інфраструктури залежать не лише стабільність та надійність їх функціонування, але часто й життя багатьох людей [2]. Тому проблема вдосконалення, підвищення надійності та ефективності системи національної кібербезпеки є актуальною як у теоретично-методичному, так і в організаційно-технічному аспекті.

Питання різноманітних загроз національній безпеці, зокрема, кіберзагроз, висвітлено в наукових працях зарубіжних і вітчизняних дослідників [3–9]. Разом із тим, організаційно-технічні аспекти проблеми удосконалення та підвищення ефективності системи національної безпеки в умовах сучасних гібридних загроз залишаються недостатньо дослідженими.

Мета даної статті – сформувати науково обґрунтовані погляди на систему національної кібербезпеки України в умовах сучасних загроз і запропонувати концептуальну модель системи національної кібербезпеки для підвищення її надійності та ефективності.

2. Основні завдання та суб'єкти забезпечення кібербезпеки України

Першим документом, який визначив стратегію нашої держави у сфері кібербезпеки, став Указ Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року № 96/2016 «Про Стратегію кібербезпеки України»», в якому було визначено такі основні завдання [10]:

• розвиток безпечного, стабільного та надійного кіберпростору;

• кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації;

• кіберзахист критичної інфраструктури;

• розвиток потенціалу сектора безпеки та оборони у сфері забезпечення кібербезпеки;

• боротьба з кіберзлочинністю.

Згідно з Указами Президента України № 8/2017, № 32/2017 та № 254/2017 введено в дію рішення Ради національної безпеки і оборони України «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» [11], «Про загрози кібербезпеці

держави та невідкладні заходи з їх нейтралізації» [12], «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [13].

5 жовтня 2017 року було прийнято закон «Про основні засади забезпечення кібербезпеки України», який набув чинності 9 травня 2018 року. Цей закон є основоположним нормативно-правовим актом у сфері забезпечення кібербезпеки держави, який [14]:

• визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства та держави, національних інтересів України в кіберпросторі;

• структурує положення про національну систему кібербезпеки;

• вводить механізми застосування сучасних європейських практик і стандартів;

• розподіляє функції між правоохоронними органами та спецслужбами щодо забезпечення кібербезпеки.

Закон також визначає основних суб'єктів забезпечення кібербезпеки України: Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), Служба безпеки України (СБУ), Міністерство внутрішніх справ (МВС) України, Міністерство оборони України (МОУ), розвідувальні органи України, Національний банк України (НБУ) [15].

За стратегічне управління та координацію роботи відомств, що забезпечують кібербезпеку, відповідає Рада національної безпеки та оборони (РНБО). Їй підпорядкована ДССЗЗІ, що розробляє комплексну систему кіберзахисту стратегічних об'єктів та опікує компанії, які проводять аудит стратегічних об'єктів. ДССЗЗІ підпорядкований Державний центр кіберзахисту та протидії кіберзагрозам, підрозділ якого Оперативний центр реагування на кіберінциденти здійснює моніторинг і виявляє потенційні кіберзагрози.

Кіберзахистом також займаються МВС України, яке відповідає за запобігання кіберзлочинам та їх розслідування; МОУ і Генеральний штаб Збройних сил України (ГШ ЗСУ) забезпечують охорону військових об'єктів та об'єктів критичної інфраструктури під час війни та в період надзвичайного стану; СБУ має запобігати терористичним атакам у кіберпросторі, її наділено правом перевіряти об'єкти критичної інфраструктури, перелік яких визначає Кабінет Міністрів, а кібербезпека в банківській сфері – об'єкт уваги НБУ [15].

Власники об'єктів критичної інфраструктури вважаються виконавцями державної політики кібербезпеки, тобто зобов'язані впроваджувати її на своєму підприємстві. Якщо державні установи, включаючи міністерства, стануть об'єктом кіберзлочинців, відповідальність буде нести керівництво цих установ. Чиновники нарешті усвідомили, що різні галузі економіки та сфери життєдіяльності України стають дедалі більш вразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Слід зауважити, що зловмисники прямо чи опосередковано пов'язані з Російською Федерацією.

Як бачимо, повноваження органів, що відповідають за кібербезпеку, частково перетинаються, тому спробуємо точніше визначити, який орган і за що саме відповідає.

ДССЗЗІ відповідає за технічний захист інформації і криптозахист даних, що є власністю держави, та захист персональних даних. Ця служба ліцензує компанії, які мають право надавати послуги криптозахисту та технічного захисту інформації, видає атестати відповідності на засоби та комплексні системи захисту інформації. При ДССЗЗІ є Центр реагування на кіберзагрози для ресурсів держави – CERT.UA (підрозділ, який структурно належить до Державного центру кіберзахисту та протидії кіберзагрозам). На нього покладено функції попередження кібератак та ліквідації їх наслідків. При ДССЗЗІ також працює Центр антивірусного захисту інформації, який відповідає за захист інформаційних ресурсів держави.

СБУ відповідає за захист інтересів держави та прав громадян в інформаційному середовищі. В СБУ створено Ситуаційний центр забезпечення кібернетичної безпеки на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки цього відомства. Завдання Центру – запобігання хакерського втручання в роботу

об’єктів критичної інфраструктури та державних служб. Центр має власну лабораторію комп'ютерної криміналістики та реагування на кіберінциденти. Підрозділом МВС України є кіберполіція, яка веде розслідування у сфері розміщення протиправного контенту в Інтернеті, злому платіжних систем і майданчиків e-commerce. Цей підрозділ також зобов'язаний інформувати громадян про нові загрози та протидіяти їх поширенню.

У МО України теж є підрозділи, що відповідають за інформаційну безпеку. Спеціальні заходи щодо забезпечення національних інтересів в інформаційній сфері організовує і проводить Головне управління розвідки МОУ, а також Служба зовнішньої розвідки України.

Створено Центр кіберзахисту при НБУ для реагування на кіберінциденти в банківській системі України та аналогічний центр при Міністерстві інфраструктури – Галузевий центр цифровізації та кібербезпеки (ГЦЦК).

3. Основа системи національної кібербезпеки

Основою системи національної кібербезпеки є центри виявлення, управління та реакції на кіберзагрози. У світовій практиці існують декілька термінів на означення таких центрів: CERT (Computer Emergency Response Team), CSIRT (Computer Security Incident Response Team), SOC (Security Operation Center). Так, національні центри протидії кіберзагрозам майже завжди називають CERT. Ці центри створено державними структурами для боротьби з кіберзагрозами, спрямованими на державні органи управління та інші критично важливі об'єкти, або з кіберзагрозами державного масштабу. В Україні таких центрів два: CERT-UA в ДССЗЗІ, а також центр рівня CERT в СБУ. Такі центри є ядром системи кібербезпеки держави, вони взаємодіють у системі міжнародного обміну інформацією про кіберзагрози, шкідливі активності та тренди атак.

Крім центрів національного масштабу, система кібербезпеки держави включає галузеві команди реагування на комп’ютерні надзвичайні події (CSIRT). Такі команди рекомендовано створювати в кожній галузі, особливо, якщо галузь має велику кількість об’єктів критичної інфраструктури. Саме на ці центри покладено завдання реагувати на кіберінциденти на підприємствах критичної інфраструктури галузі відповідно до Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [16]. Цей документ визначає організаційно-методологічні, технічні й технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими для виконання підприємствами, установами та організаціями, які, відповідно до законодавства, віднесено до об’єктів критичної інфраструктури [16].

Загалом такі галузеві центри кібербезпеки покликані виявляти кіберзагрози на підприємствах галузі, реагувати на них та взаємодіяти з національними CERT.

Наступним рівнем системи кібербезпеки є центри управління кібербезпекою окремих організацій, державних чи комерційних підприємств, зокрема, інфраструктурних та фінансових установ, різноманітних об'єднань, підприємств та ін. Такі центри управління кібербезпекою називають SOC, вони покликані виявляти, локалізувати загрози та реагувати на кіберінциденти на окремому підприємстві, в організації, корпорації чи холдингу. Перевагами SOC є максимальна заглибленість у IT-інфраструктуру конкретного підприємства, тобто можливість швидко розібратися в сутності інциденту й локалізувати його наслідки. Тому такі центри є найбільш ефективними для боротьби з кіберзагрозами для підприємств, в яких кількість користувачів перевищує 500, а також для тих, які зберігають чи обробляють інформацію, втрата або виток якої буде критичним для підприємств, організацій або держави.

Ще одним компонентом системи кібербезпеки є комерційні SOC, що надають послуги з виявлення кіберзагроз та кіберінцидентів і, при можливості, реагування на них для

підприємств, які розуміють важливість забезпечення кібербезпеки, але з якихось причин не створюють свій SOC, а отримують ці послуги із хмари оператора. Такі оператори називаються MSSP (Managed Security Service Provider) або MDR (Managed detection and response), і такі комерційні центри можуть взаємодіяти з CERT національного рівня після перевірки щодо виконання вимог та умов взаємодії з точки зору забезпечення національної безпеки.

4. Концептуальна модель системи національної кібербезпеки

Використовуючи системний підхід, який полягає у застосуванні сукупності методологічних принципів і теоретичних положень, що дають змогу розглядати кожний елемент системи у його зв'язку і взаємодії з іншими елементами [17]; простежувати зміни, що відбуваються в системі в результаті зміни окремих її ланок; вивчати специфічні системні (емерджентні) властивості; робити обґрунтовані висновки про закономірності розвитку системи; визначати оптимальний режим її функціонування [18], можна побудувати концептуальну модель системи національної кібербезпеки у вигляді трирівневої піраміди (рис. 1).

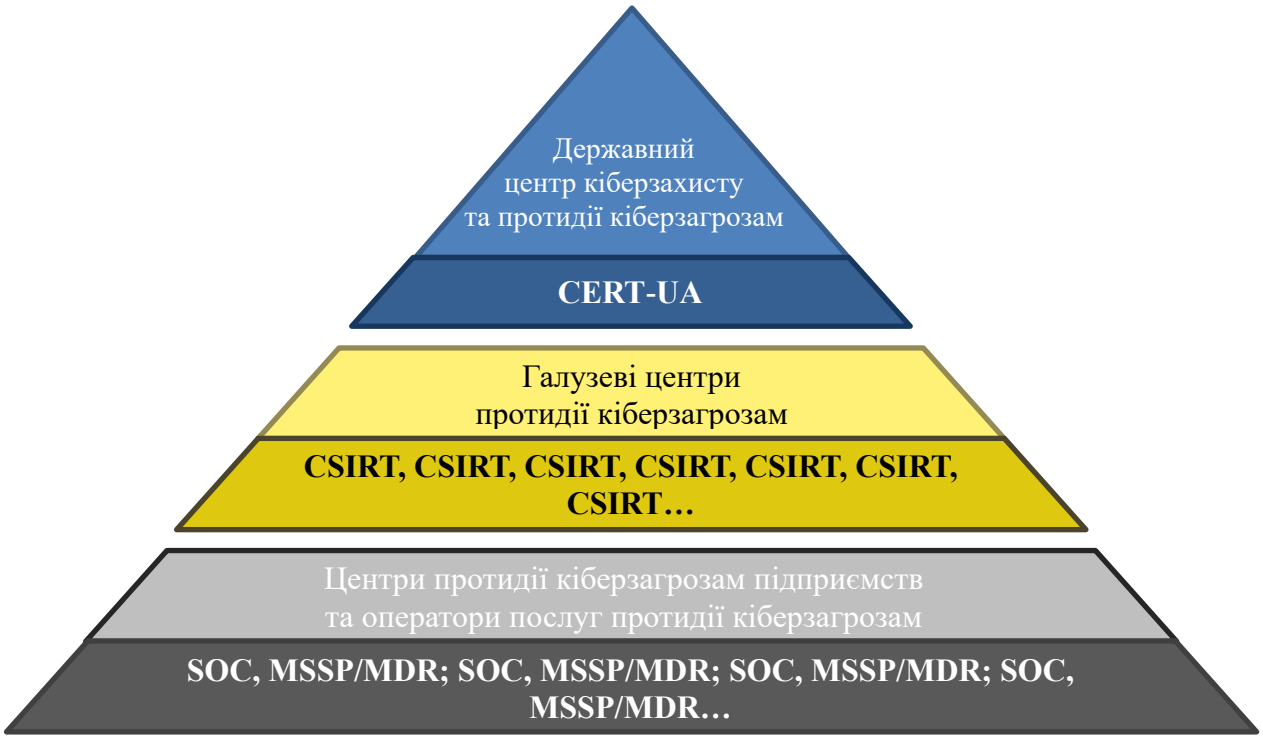

Рисунок 1 – Концептуальна модель системи національної кібербезпеки

В основу моделі покладено концепцію єдиного інформаційного простору для обміну даними про кіберінциденти як в середині країни, так і за її межами. Це такі принципи [19]:

• принцип цілісності – розгляд водночас системи як єдиного цілого і як підсистеми для вищих рівнів;

• принцип ієрархічності – наявність елементів, розташованих згідно з підпорядкуванням нижчого рівня вищому рівню;

• принцип структуризації – аналіз елементів системи та їх взаємозв'язку в рамках конкретної організаційної структури;

• принцип множинності – використання різних моделей для опису як окремих елементів, так і системи в цілому;

• принцип системності – володіння об'єктом всіх ознак системи.

Для підвищення ефективності боротьби з кіберзагрозами на рівні країни організовано взаємодію центрів та обмін інформацією про виявлені кіберінциденти, особливо, якщо

вони викликані не відомими раніше кіберзагрозами. У цих випадках якнайшвидше поширення такої інформації, внесення до бази індикаторів компрометації (indicators of compromise, IoC) правил кореляції та реакції кожного центру боротьби з кіберзагрозами є принципово важливим для запобігання масових атак і порушень у роботі інформаційно-технологічної інфраструктури державних установ та відомств.

5. Модель взаємодії центрів протидії кіберзагрозам та обміну інформацією

Модель взаємодії центрів протидії кіберзагрозам та обміну інформацією між ними представлена на рис. 2.

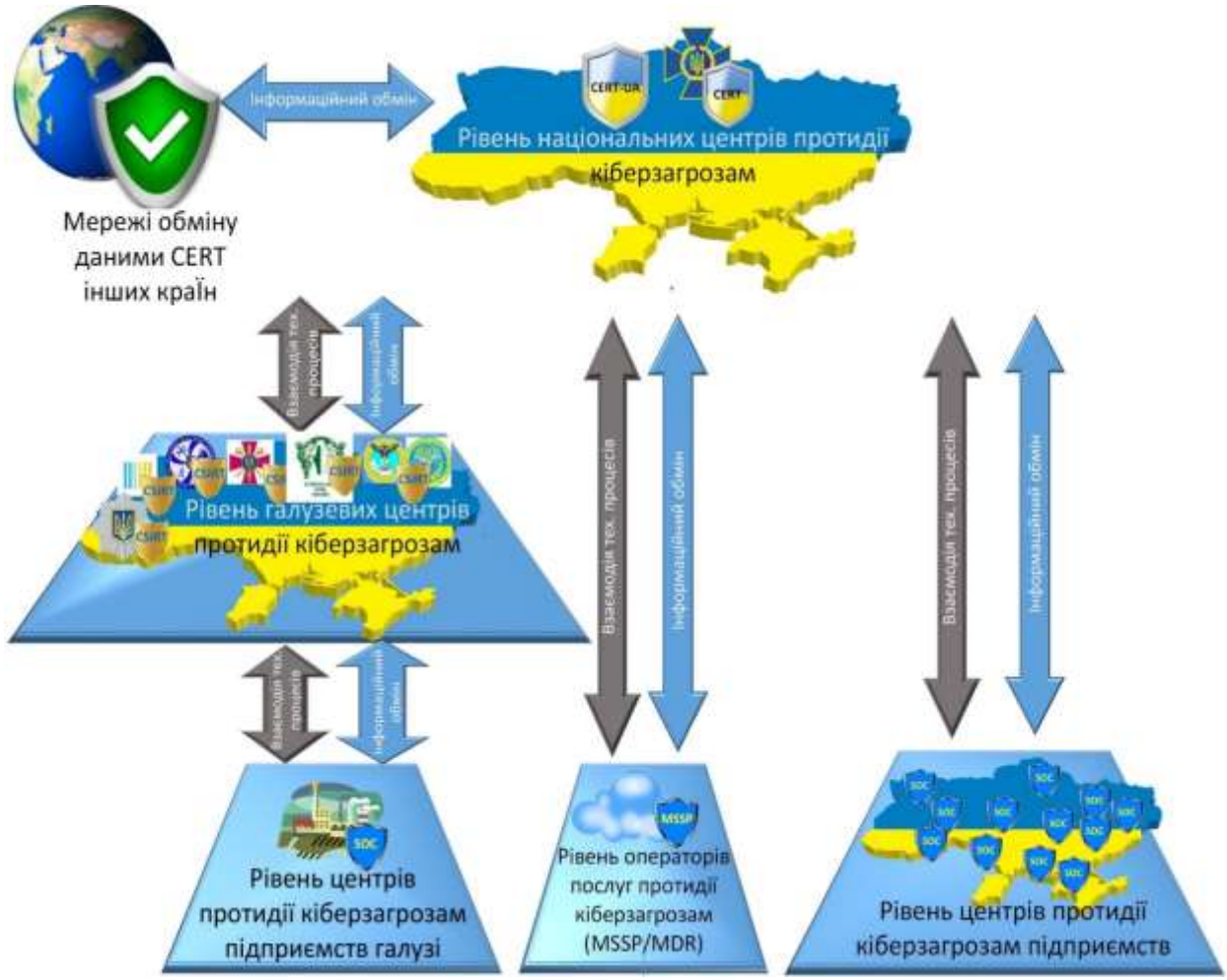

Рисунок 2 – Модель взаємодії центрів протидії кіберзагрозам та обміну інформацією між ними

Ядром цієї моделі є центри національного рівня CERT, які здійснюють обмін інформацією про загрози (IoC) з подібними національними та міжнародними центрами. CERT національного рівня є центром збору, аналізу, обробки, зберігання та обміну інформацією про загрози у країні. CERT також узгоджує протокол взаємодії і обміну інформацією в національній мережі та вимоги для підключення центрів до цієї мережі.

CSIRT галузевого рівня здійснюють обмін інформацією безпосередньо з центрами національного рівня. Підприємства галузі, які мають власний SOC, є третім рівнем системи національної кібербезпеки. Вони підключаються до національної мережі обміну інформацією з кібербезпеки через CSIRT відповідної галузі, якщо такий є, і безпосередньо з центром національного рівня CERT, якщо CSIRT галузі не функціонує.

SOC окремих підприємств, корпорацій та холдингів також взаємодіє безпосередньо з центром національного рівня CERT, підключається до мережі згідно з затвердженими протоколами взаємодії після виконання відповідних вимог.

Підключення до національної мережі для обміну інформацією щодо кібербезпеки операторів, які надають послуги SOC, здійснюється за тими ж принципами, що й підключення SOC підприємств, але перед цим потрібно провести аналіз і контроль усіх замовників їх послуг, тому що такі оператори можуть надавати послуги організаціям і установам різних країн.

6. Висновки

Зважаючи на те, що останнім часом протистояння у кіберпросторі посилюється і становить реальну загрозу для держав, систему кіберзахисту в Україні необхідно розвивати та вдосконалювати з урахуванням рівня сучасних загроз. Державним організаціям, що відповідають за кіберзахист, треба постійно актуалізувати вимоги щодо кіберзахисту, яких мають дотримуватися всі об'єкти критичної інфраструктури, визначити повний список таких об'єктів і уточнювати його при необхідності. Керівникам цих об'єктів слід впроваджувати досить надійну систему кіберзахисту з урахуванням всіх вимог.

Не можна забувати про захист і керівникам підприємств та організацій, які не входять до переліку об’єктів критичної інфраструктури. Слід пам’ятати, що захист від кіберзагроз тепер стосується кожного. Отже, варто подбати про нього і пересічним громадянам.

СПИСОК ДЖЕРЕЛ

1. Лисецкий Ю.М., Бобров С.И. Новые угрозы информационной безопасности или оружие массового заражения. *Математичні машини і системи*. 2018. № 1. С. 41–50.
2. Лисецький Ю.М. Комплексная безопасность корпоративных информационных систем. *Управляющие системы и машины*. 2019. № 1. С. 145–148.
3. Шейн Х. Кибервойн@. Пятый театр военных действий. Москва: Альпина нон-фикшн, 2016. 392 с.
4. Глазов О.В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. *Наукові праці Чорноморського державного університету імені Петра Могили. Політологія.* 2011. Т. 155, Вип. 143. С. 42–46.
5. Мартинюк В. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і східного партнерства. Київ, 2018. 106 с.
6. The National Security Strategy of the United States of America. Washington, 2006. 54 p.
7. Богданович В.Ю., Семенченко А.І., Єгоров Ю.В., Бортник О.О. Теоретико-методологічні засади забезпечення національної безпеки держави в її визначальних сферах: монографія. Київ: Вид-во Кий, 2007. 370 с.
8. Богданов А.М., Мохор В.В. О кибербезопасности в широком смысле. *Information Technology and Security*. 2013. № 1 (3). С. 51–58.
9. Сейранова С.Н. Киберугрозы как серьезный вызов национальной безопасности КНР. *Актуальные проблемы современных международных отношений.* 2017. № 2. С. 131–134.
10. Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року № 96/2016 «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text.
11. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури»: Указ Президента України від 16.01.2017 р. № 8/2017. URL: https://www.president.gov.ua/documents/82017-21058.
12. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»: Указ Президента України № 32/2017. URL: https://www.president.gov.ua/documents/322017-21282.
13. Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про

загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32»: Указ Президента України № 254/2017. URL: https://www.president.gov.ua/documents/2542017-22502.
14. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
15. Діордіца І.В. Детермінованість кібербезпекової політики кібернетичною функцією. URL: https://goal-int.org/determinovanist-kiberbezpekovoyi-politiki-kibernetichnoyu-funktsiyeyu/.
16. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 518 URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.
17. Блауберг И.В. Проблема целостности и системный подход. Москва: Эдиториал УРСС, 1997. 448 с.
18. Шрейдер Ю.А., Шаров А.А. Системы и модели. Москва: Радио и связь, 1982. 150 с.
19. Берталанфи Л. Общая теория систем – обзор проблем и результатов. *Системные исследования*. Москва: Наука, 1969. С. 34–35.

Стаття надійшла до редакції 08.04.2021