УДК 004.056.5:007:343.9:351.86:659.2/.4:338.245:338.656

ЗАВЕРБНИЙ Андрій Степанович
доктор економічних наук, професор,
професор кафедри зовнішньоекономічної та митної діяльності,
Національний університет «Львівська політехніка», Україна
ORCID ID: 0000-0001-7307-536X
andrii.s.zaverbnyi@lpnu.ua

ОСОБЛИВОСТІ ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ПІДПРИЄМСТВ У ВОЄННИЙ ПЕРІОД: ТЕОРЕТИКО-ПРИКЛАДНИЙ АСПЕКТ

В статті досліджено особливості формування системи управління кібербезпекою підприємств у воєнний період. В роботі наведено теоретико-прикладний аспект даної проблеми.

Метою статті є дослідження особливостей і теоретико-прикладних аспектів формування системи управління кібербезпекою підприємств у воєнний період. Обґрунтовано важливість управління кібербезпекою підприємств для їх економічної безпеки та досягнення необхідного рівня національної безпеки. Проведено огляд, аналізування літературних джерел за проблемою визначення сутності поняття «кібербезпека». Доведено, що для ефективного управління кібербезпекою доцільно здійснити класифікування кібератак. Проаналізовано сучасні кібератаки та їх наслідки.

Сформовано ключові етапи побудови дієвої системи управління кібернетичною безпекою. Вказано ключові аспекти визначення політики безпеки підприємств, їх випереджального реагування на високо динамічні умови господарювання (перш за все у сфері кібернетичної безпеки) в умовах воєнного часу. Система управління кібернетичною безпекою підприємств і організація має передбачати можливість своєчасного обрання конкретних засобів, шляхів її забезпечення.

Проаналізовано функціонально-управлінський аспект формування системи управління кібербезпекою підприємств у воєнний період. Досліджено ключові заходи задля розвитку потенціалу сектору безпеки, оборони України.

В дослідженні запропоновано до використання концептуальну модель формування ефективної системи управління кібербезпекою підприємств у воєнний період. Охарактеризовано кожен із її етапів. Описано функції системи управління кібербезпекою підприємств у воєнний період.

Ключові слова: *ризики, безпека, кібербезпека, система управління, управління кібербезпекою, функції управління.*

JEL classification: D80; G14; H56; L86
DOI: https://doi.org/10.31649/ins.2024.1.13.21

1. ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Як показує дослідження, Україна, зокрема, органи її влади, вітчизняний бізнес, суспільство в цілому, постали під загрозами, небезпеками кібератак відразу після проголошення незалежності від 72 років окупації росією.

Із 2014 р. їх обсяги просто значно збільшилися і вже набули значних масштабів саме із початком повномасштабного вторгнення у 2022 р. [15].

За таких умов кожен орган державної влади, кожен представник бізнесу (не залежно від форм та видів) повинні систематично оцінювати вразливість для своєї діяльності до інцидентів кібербезпеки, технологічних збоїв та інших загроз, що можуть виникати через

атаки на системи, інфраструктуру тощо, бути наслідками воєнних дій [15].

При чому високий рівень загрози перш за все стосується тих підприємств, організацій, що належать до критичної інфраструктури України. Мова йде передусім про підприємства енергетичної, телекомунікаційної, медіа, фінансової сфер [15].

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблематику кібербезпеки підприємств, зокрема й в умовах війни, досліджували такі вчені як: Артеменко Н. [15], Бердибаєв Р. [4], Білявська Ю. [2], Вишнівський В. [3], Гнатюк С. [4], Грицюк Ю. [5], Давиденко Є. [6], Діордіца І. [7], Довгань О. [8], Доронін І. [8], Жигаревич О. [4], Завербний А. [16], Зануда А. [9], Кириченко А. [10], Кузьменко О. [14], Линник О. [15], Маклюк О. [14], Сидоренко В. [4], Смірнова Т. [4], Пешко М. [16], Пампуха А. [3], Франчук В. [18], Чернишова О. [14], Шестак Я. [2], Шира Т. [19] та інші.

3. ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ ОЗНАЧЕНА СТАТТЯ

Враховуючи важливість досліджень, необхідно зазначити, що не достатньо розкритою залишається проблематика щодо формування системи управління кібербезпекою підприємств і організацій (тобто, суб'єктів мікрорівня) в умовах воєнного стану.

4. ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження особливостей і теоретико-прикладних аспектів формування системи управління кібербезпекою підприємств у воєнний період.

5. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ З ПОВНИМ ОБҐРУНТУВАННЯМ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

Як показує дослідження, існують різні підходи щодо трактування сутності поняття «кібербезпека». Узагальнивши їх можна констатувати, що це «стан захищеності життєво важливих інтересів особи/суспільства/держави від зовнішніх/внутрішніх загроз, що є пов'язаними із застосуванням ресурсів інформаційно-телекомунікаційних систем (кіберпростору), за наявності якого забезпечуватимуться гарантовані умови щодо реалізування інформаційної політики» [4, с. 329-330, 18] на рівні держави, на рівні суб'єктів підприємництва тощо.

Спектр сучасних кібератак виступає досить різнорідним. Погоджуємося і з вченими, що для ефективного управління кібербезпекою доцільно здійснити класифікування кібератак [8, 15].

Вичерпне та деталізоване класифікування було здійснено за наступними ознаками [8, 15]: за специфікою їх реалізування; за рівнем складності; за інструментальними засобами, що використовуються при їх проведенні; за умовами їх ініціалізування; за дистанційністю здійснення; за процесами автоматизування; за зовнішнім проявленням; за скерованістю кінцевих результатів, за специфікою порушення базових характеристик діючих систем інформаційної безпеки.

Доцільно також ще додати класифікаційні ознаки: «за рівнем страхування», тобто чи можливо застрахуватися (перестархуватися) від самої загрози, її наслідків та «за рівнем збитковості», тобто рівнем втрат від кібератак.

Чітке класифікування, віднесення тієї чи іншої кібератаки до конкретної групи сприятиме ефективнішому управлінню кіберзахисту, реалізуванню превентивно розроблених і затверджених тих чи інакших правил чи процедур.

Адже, останнім часом наслідки кібератак, кіберзлочинів сягають значних за обсягами втрат. Зокрема, доцільно акцентувати увагу на найбільших з них, а саме [1]:

- витік даних із понад 3 млрд. акаунтів «Yahoo» спричинив втрату 1,3 1,3 млрд. дол. США ринкової капіталізації цієї компанії та виплату понад 120 млн. дол. США для врегулювання позовів, сплати штрафних санкцій тощо;

- через злам баз даних мережа «Marriott» отримала колективні судові позови, штрафні санкції розміром 24 млн дол. США;

- злам онлайн-сервісів «Sony PlayStation Network» призвів до втрат у 171 млн дол. США;

- злам криптовалют «Mt.Gox» оцінений у 440 млн. дол. США та закриття суб'єкту;

- глобальний же збиток від кібератаки «NotPetya» був оцінений в 10 млрд. дол. США [1].

До зазначеного переліку можемо віднести масштабну атаку на ПрАТ «Київстар» вже у 2023 р. Обсяги втрат поки не оприлюднені.

Отже, саме кібератаки виступають в сучасних умовах діджиталізування одним із найнебезпечніших ризиків для будь-якого бізнесу.

При чому, згідно аналізування статистичних даних, їх обсяги мають тенденцію до зростання.

Так, McKinsey спрогнозував, що вже до 2025 р. кіберзлочини щорічно спричинятимуть збитки аж на 10,5 трлн. дол. США. Це втричі перевищуватиме величину 2015 р. [1, 12].

Що стосується саме нашої країни, зокрема за період від російського повномасштабного вторгнення і до тепер (2024 р.), то кіберфахівця СБУ вже нейтралізовано понад 3500 кібератак (на електронні системи центральних органів влади, об'єкти критичної інфраструктури), при чому майже половина із нейтралізованих атак була виявлена в режимі «реального часу» [15].

Переважаюча більшість російських кібератак скеровувалися на знищення цифрових сервісів, дестабілізування роботи стратегічно важливих підприємств (енергетична, транспортна сфери) [15].

Саме тому актуальність і своєчасність розроблення систем управління кібербезпекою та їх застосування є надзвичайно високими.

Надважливість кібребезпеки, систем управління нею для України можна також визначити шляхом огляду, аналізування чинного вітчизняного законодавства в даній царині, його динамічність та своєчасність (прийняття, внесення змін та доповнень). Забезпечення необхідного рівня кібербезпеки виступає одним із пріоритетних напрямків системи національної безпеки нашої країни [18, 19]. Його реалізування повинне здійснюватися через «посилення спроможностей вітчизняної системи кібербезпеки для протидіяння кіберзагрозам сучасного безпекового середовища» [15].

Враховуючи, що «інформаційна безпека розглядається невід'ємною складовою кожної сфери національної безпеки», кібербезпека розглядається «невід'ємною складовою інформаційної безпеки» [4, с. 329-330, 18]. Сама кібербезпека охоплюватиме сектор інформаційної безпеки, в якому задля «оброблення інформації застосовуватимуться інформаційно-телекомунікаційні системи» [4, с. 329-330].

Керівництво всіх ланок, а також всі працівники суб'єктів критичної інфраструктури (енергетичної, фінансової, телекомунікаційної, медіа та інших сфер) повинні постійно перебувати у режимах підвищеної рівня готовності [15].

Адже саме ці сфери виступають пріоритетними у цілях кібератак. Особливо дана проблема загострюється у воєнний період (для нашої країни це відбувається починаючи із 2014 р.) [15].

Державний та приватні сектори вітчизняної економіки (передусім вказаних (критчиної інфраструктури) сфер) мають постійно (у режимі «он-лайн») бути готовими (технічно, інформаційно забезпеченими) до протидії кібервикликам і загрозам [15].

Спеціалізовані служби/підрозділи даних підприємств/організацій мають проводити систематичне деталізоване оцінювання (моніторинг) щодо рівня готовності до потенційних кіберінцидентів, здатності своєчасно відновлювати свою діяльність тощо [15]. Задля цього важливим аспектом є формування дієвої, гнучкої та динамічної системи управління кібербезпекою підприємств у воєнний період.

Ключовими заходами задля розвитку потенціалу сектору безпеки, оборони України виступають наступні [4, с. 329-330, 10, 12, 18, 19]:

- забезпечення надійного захисту об'єктів критичної інфраструктури, їх технологічних процесів від несанкціонованих доступів;

- державне стратегічне управління (в т.ч. й планування, хоча в нормативних актах деколи вказується «планування і управління», але планування виступає лишень однією із управлінських функцій, тому поняття «управління» включає також і його);

- формування єдиного центру управління кібербезпекою та підпорядкуванням йому сформованих підрозділів кіберзахисту та кібербезпеки у силових структурах, об'єктах

критичної інфраструктури тощо (функція організування кібербезпеки);

- забезпечення інтегрування, сумісності вітчизняної системи управління кібербезпекою із євроатлантичними;

- узгодження стратегії кібербезпеки з іншими стратегіями (передусім енергетичної, яка станом на сьогодні є розробленою на найдовший період (до 2050 р.);

- забезпечення систематичного контролювання (моніторингу) всіх процесів за допомогою застосування сучасних інформаційно-комунікаційних систем;

- організування швидкого реагування на кіберзагрози/кібератаки, використовуючи інформаційно-комунікаційні системи тощо.

Відповідно із вказаними стратегічними напрямками розвитку потенціалу державного сектору безпеки потрібно аналогічні дії узгоджено формувати і на мікрорівні (рівні підприємства/організації).

Тому нами запропоновано концептуальну модель формування ефективної системи управління кібербезпекою підприємств у воєнний період (див. рис. 1).

Також підприємствам критичної інфраструктури потрібно розробляти процедури та правила (як елемент функції планування) на випадок знання кібератак.

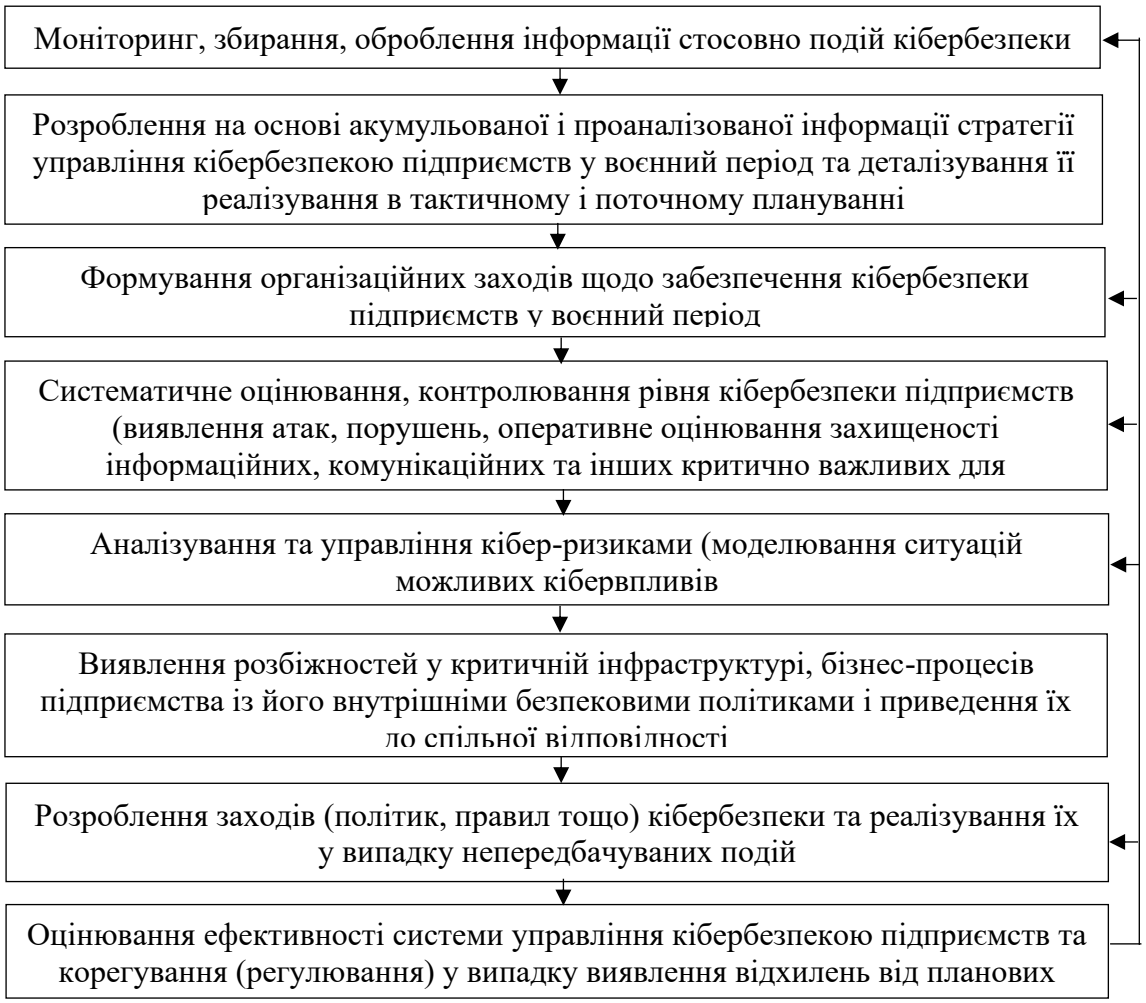

Рис. 1. Концептуальна модель формування ефективної системи управління кібербезпекою підприємств у воєнний період

Джерело: систематизовано автором на основі [4, с. 177, 5, 19, 20].

Формування дієвої системи управління кібернетичною безпекою (рис. 1) передусім вимагатиме від вітчизняних підприємств чіткого визначення їх політики безпеки, випереджального реагування на високо динамічні умови господарювання (перш за все у сфері кібернетичної безпеки).

Система управління кібернетичною безпекою підприємств і організація має передбачати можливість своєчасного обрання конкретних засобів, шляхів її забезпечення.

Слід наголосити, що формування системи управління кібербезпекою підприємств повинно базуватися на концепціях системи управління (обов'язково містити функції управління, методи, управлінські рішення тощо).

Передуватиме даному процесу планування, що має відбуватися виключно на основі аналізування отриманої інформації (дотримуючись всіх необхідних вимог і умов до неї, зокрема конфіденційності, повноти, релевантності, своєчасності тощо).

Що стосується організаційного забезпечення системи управління кібербезпекою, то необхідною є цілеспрямована діяльність кожного суб'єкта підприємництва, що стосується забезпечення необхідного рівня кібербезпеки. Організування кібербезпеки (як функція управління нею) має включати наступні елементи (рис. 1):

– формування елементів організаційної структур управління, які сприятимуть забезпеченню кібербезпеки;

– узгодження обов'язків та прав (передбачення можливості їх делегування у надзвичайно динамічних умов) кожного із них, чітке підпорядкування вищому керівництву;

– налагодження процесів в системі управління у сфері кібербезпеки,

– забезпеченням оптимальних умов для прийняття, реалізування управлінських рішень у цій сфері тощо.

Організаційне забезпечення системи кібербезпеки повинне характеризуватися місцем, роллю спеціальних суб'єктів (спеціалізованих підрозділів), їх функціональними обов'язками та повноваженнями, напрямами їх взаємодії з іншими підрозділами при здійсненні заходів щодо «забезпечення безпеки підприємства в кіберпросторі» [7, с. 113].

Важливою складовою системи управління кібербезпекою підприємств у воєнний період є функції контролювання та регулювання (зворотній зв'язок відображений стрілочками на рис. 1 від останнього блоку моделі до попередніх). Від своєчасності реагування на зміни і відхилення залежатиме рівень ефективності системи управління кібербезпекою. Деколи взагалі від цього залежить й подальше функціонування суб'єкта підприємництва. Адже невчасне реагування шляхом внесення коректи у планування, організування, мотивування може спричините втрати.

При формуванні системи управління кібербезпекою українських підприємств потрібно обов'язково враховувати такі елементи безпеки (окрім, зрозуміло, інформаційного) [6]: фізичний (доступ до об'єктів), кадровий (перевіряння персоналу при наборі на роботу), навчальний (підвищення рівня працівників у безпековій сфері), фінансовий (захист від махінацій, зловживань, шахрайств тощо), бізнес-контентний (дослідження потенційних партнерів, стейкхолдерів на предмет безпеки співробітництва), кооперуючий (співпраця з державними органами (правоохоронними, силовими тощо).

Задля захисту від кібератак вітчизняні підприємства повинні запроваджувати комплексні, структуровані, дієві заходи безпеки. Можливими варіантами даних заходів виступає регулярне оновлення програмного забезпечення всіх бізнес-процесів підприємства, запровадження мережевих, системних заходів кіберзахисту, навчання персоналу кібербезпеці, розроблення і запровадження стратегій реагування на кіберінциденти, кібератаки і кіберзлочини тощо.

Таким чином, запропонована концептуальна модель формування ефективної системи управління кібербезпекою (рис. 1) виступатиме надійним інструментом у процесі вирішення завдань щодо забезпечення кібербезпеки вітчизняних підприємств і організацій, зокрема у воєнний період.

6. ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМКУ

За сучасних умов кібератаки набувають серйозної загрози для безпеки підприємств, державних органів, суспільства в цілому. Вони призводять до серйозних наслідків для бізнес процесів (втрата конфіденційної інформації (власної, клієнтів та ін.), отримання фінансових збитків, зниження рівня репутації, призупинення/припинення бізнес процесів тощо) а також для держави в цілому (через органи влади, суб'єкти критичної інфраструктури, що перебувають у державній власності та ін.).

Підсумовуючи результати проведеного дослідження, можна констатувати, що важливим елементом забезпечення надійного рівня національної безпеки (включаючи безпеку підприємств, організацій, передусім критичної інфраструктури), населення тощо) має виступати формування злагодженої, ефективної системи управління кібербезпекою не лишень на макро рівні, але й на рівні суб'єктів підприємництва. Надзвичайно актуального значення для України, вітчизняного бізнесу дана проблема набуває в умовах воєнного стану, гібридних воєн тощо.

В дослідженні запропоновано концептуальну модель формування ефективної системи управління кібербезпекою підприємств у воєнний період, при створенні якої враховано особливості, потенційні можливості, потреби вітчизняних та іноземних суб'єктів кібербезпеки,

Формування дієвої, гнучкої (динамічної) та ефективної системи управління кібербезпекою сприятиме забезпечення надійного захисту суб'єктів підприємництва, державних органів, сприятиме підвищенню рівня економічної та вцілому й національної безпеки нашої країни в умовах воєнного стану тощо.

Література

1. 6 гучних кібератак на бізнес: кейси Yahoo, GitHub і Marriott. URL: https://hub.kyivstar.ua/articles/6-guchnyh-kiberatak-na-biznes-kejsy-yahoo-github-i-marriott
2. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. Товари і ринки. 2022. № 3. С. 47–59.
3. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. Цифрова трансформація кібербезпеки: науково-практична інтернет-конференція, 20 квітня 2022, Державний університет телекомунікацій Навчально- наукового інститут захисту інформації. Київ, 2022. С. 31–33.
4. Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., Смірнова Т.В. Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури. Кібербезпека: освіта, наука, техніка. № 3 (19). 2023. С. 76-196.
5. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. Науковий вісник НЛТУ України. 2016. Вип. 26.8. С. 327-337.
6. Давиденко Є. Корпоративна безпека на українських підприємствах в умовах війни. Економіка та суспільство. 58. 2023. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3310
7. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. Підприємництво, господарство і право. 4. 2017. С. 99-107.
8. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. НАПрН України, НДІІП. Київ : Видавничий дім «АртЕк», 2017. 107 с.
9. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
10. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами від 28.07.2022 р. № 2470-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian)
11. Зануда А. Атака на Київстар. Які небезпеки вона несе, окрім відсутності зв'язку. 2023. URL: https://www.bbc.com/ukrainian/articles/cglp7kz0rjmo
12. Кириченко А. Кібербезпека в Україні: шляхи розвитку та можливості. Укрінформ. 2023. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

13. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html.

14. Кібербезпека: як українському бізнесу захиститися від атак російських хакерів під час війни. Поради від ІТ-фахівців. URL: https://uaspectr.com/2022/07/27/yak-ukrayinskomu-biznesu-zahystytysya-vid-atak-hakeriv.

15. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. Економіка та суспільство. 44. 2022. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1790

16. Линник О. І., Артеменко Н. В. Стратегія економічної безпеки підприємства як фактор зменшення впливу зовнішніх та внутрішніх загроз. Вісник Національного технічного університету ХПІ. Сер.: Технічний прогрес та ефективність виробництва. 2013. № 67. С. 159–169.

17. Пешко М., Завербний А. Діджиталізація української економіки в умовах євроінтеграції. Економіка та суспільство. 47. 2023. URL: https://www.economyandsociety.in.ua/index.php/journal/article/view/2136

18. Розпорядження Кабінету міністрів України від 19 грудня 2023 р. № 1163-р «Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text

19. Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12.

20. Франчук В.І. Теоретичні засади корпоративної безпеки. Актуальні проблеми економіки. 2009. № 7. С. 161–167.

21. Шира Т.Б. Корпоративна безпека підприємств в Україні: визначення ключових загроз. Вчені записки Таврійського національного університету імені ВІ Вернадського. Серія: Економіка і управління. 2018. Том 29 (68). № 6. С. 93–96

References

1. 6 gnuchkykh kiberatak na biznes: kejsy Yahoo, GitHub i Marriott [6 high-profile cyberattacks on business: cases of Yahoo, GitHub, and Marriott.1. 6 high-profile cyberattacks on business: cases of Yahoo, GitHub, and Marriott.]. URL: https://hub.kyivstar.ua/articles/6-guchnyh-kiberatak-na-biznes-kejsy-yahoo-github-i-marriott (in Ukrainian)

2. Biljavsjka, Ju., Shestak, Ja. (2022). Kiberbezpeka ta kiberghighijena: nova era cyfrovykh tekhnologhij [Cyber security and cyber hygiene: a new era of digital technologies]. Tovary i rynky. Goods and markets, 3, pp. 47–59. (in Ukrainian)

3. Vyshnivsjkyj, V.V., Pampukha, A. I. (2002). Kiberbezpeka v Ukrajini [Cybersecurity in Ukraine]. Cyfrova transformacija kiberbezpeky: naukovo-praktychna internet-konferencija – Digital transformation of cyber security: scientific and practical internet conference, 20 kvitnja 2022, Derzhavnyj universytet telekomunikacij Navchaljno-naukovogho instytut zakhystu informaciji, m. Kyjiv, pp. 31–33. (in Ukrainian)

4. Gnatiuk S.O., Berdybajev R.Sh., Sydorenko V.M., Zhygarevych O.K., Smirnova T.V. (2023). Systema koreliuvania podij ta upravlinia incydentamy kiberbezpeky na objektakh krytychnoji infrastruktury [System for correlating events and managing cybersecurity incidents at critical infrastructure facilities]. Kiberbezpeka: osvita, nauka, tekhnika. № 3 (19). pp. 76-196. (in Ukrainian)

5. Грицюк Ю.І. (2016). Kiberintervencija ta kiberbezpeka Ukrajiny: problemy ta perspektyvy jikh podolania [Cyber intervention and cybersecurity in Ukraine: problems and prospects for overcoming them]. Naukovyj visnyk NLTU Ukrajiny. 26.8. pp. 327-337. (in Ukrainian)

6. Davydenko Ye. (2023). Korporatyvna bezpeka na ukrajins`kykh pidpryjemstvakh v umovakh vijny [Corporate security at Ukrainian enterprises in times of war]. Ekonomika ta suspil`stvo. 58. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3310 (in Ukrainian)

7. Diordica I. (2017). Poniatia i zmist kiberzagroz na suchasnomu etapi [The concept and content of cyber threats at the present stage]. Pidpryjemnyctvo, gospodarstvo i pravo. 4. pp. 99-107. (in Ukrainian)

8. Dovghanj O.D., Doronin I.M. (2017). Eskalacija kiberzaghroz nacionaljnym interesam Ukrajiny ta pravovi aspekty kiberzakhystu: monoghrafija [Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber protection: monograph]. NAPrN Ukrajiny, NDIIP. Kyiv: Vydavnychyj dim «ArtEk». 107 p. (in Ukrainian)

9. Zhylin A.V., Shapoval O.M., Uspens`kyj O.A. (2021). Tekhnologiji zakhystu informaciji v informacijno-telekomunikacijnykh systemakh: navch. posib. [Technologies of information protection in information and telecommunication systems: a textbook]. Kyjiv: KPI im. Igora Sikors`kogo, V-vo «Politekhnika», 213 p. (in Ukrainian)

10. The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" as amended on 28.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian)
11. Zanuda A. (2023). Ataka na Kyjivstar. Yaki nebezpeky vona nese, okrim vidsutnosti zvjazku ? [Attack on Kyivstar. What dangers does it pose, besides the lack of communication?]. URL: https://www.bbc.com/ukrainian/articles/cglp7kz0rjmo (in Ukrainian)
12. Kyrychenko A. (2023). Kiberbezpeka v Ukrajini: shliakhy rozvytku ta mozhlyvosti [Cybersecurity in Ukraine: ways of development and opportunities]. Ukrinform. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (in Ukrainian)
13. Business cybersecurity in an unstable environment. URL: https://www.pwc.com/ua/uk/publications/2022/ cybersecurity-uncertainty-state.html. (in Ukrainian)
14. Kiberbezpeka: jak ukrajinsjkomu biznesu zakhystytysja vid atak rosijsjkykh khakeriv pid chas vijny. Porady vid IT-fakhivciv [Cyber security: how Ukrainian businesses can protect themselves from attacks by Russian hackers during the war. Advice from IT experts]. URL: https://uaspectr.com/2022/07/27/yak-ukrayinskomu-biznesu-zahystytysya-vid-atak-hakeriv. (in Ukrainian)
15. Kuz`menko O., Makliuk O., Chernyshova O. (2022). Kiberbezpeka biznesu pid chas vijny. Ekonomika ta suspil`stvo. 44. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1790 (in Ukrainian)
16. Lynnyk, O.I., Artemenko, N.V. (2013). Stratehiya ekonomichnoyi bezpeky pidpryyemstva yak faktor zmenshennya vplyvu zovnishnikh ta vnutrishnikh zahroz [Enterprise economic security strategy as a factor in reducing the impact of external and internal threats]. Visnyk Natsional′noho tekhnichnoho universytetu KHPI. Ser.: Tekhnichnyy prohres ta efektyvnist′ vyrobnytstva, (67), pp. 159–169. (in Ukrainian)
17. Peshko M., Zaverbnyj A. (2023). Didzhytalizacija ukrajins`koji ekonomiky v umovakh evrointegraciji [Digitalization of the Ukrainian economy in the context of European integration]. Ekonomika ta suspil`stvo. 47. URL: https://www.economyandsociety.in.ua/index.php/journal/article/view/2136 (in Ukrainian)
18. Order of the Cabinet of Ministers of Ukraine of December 19, 2023. N. 1163-r "On Approval of the Action Plan for 2023-2024 for the Implementation of the Cybersecurity Strategy of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text (in Ukrainian)
19. Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 14 travnja 2021 roku «Pro Strateghiju kiberbezpeky Ukrajiny»: Ukaz Prezydenta Ukrajiny; Strateghija vid 26.08.2021 № 447/2021 [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine; Strategy dated August 26, 2021. № 447/2021]. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12. (in Ukrainian)
20. Franchuk, V.I. (2009). Teoretychni zasady korporatyvnoyi bezpeky [Theoretical foundations of corporate security]. Aktual′ni problemy ekonomiky, (7), pp. 161–167. (in Ukrainian)
21. Shyra, T. B. (2018). Korporatyvna bezpeka pidpryyemstv v Ukrayini: vyznachennya klyuchovykh zahroz [Corporate Security of Enterprises in Ukraine: Identification of Key Threats]. Vcheni zapysky Tavriys′koho natsional′noho universytetu imeni VI Vernads′koho. Seriya: Ekonomika i upravlinnya, (29 (68), № 6), pp. 93–96. (in Ukrainian)

Abstract

ZAVERBNYJ Andrij

Peculiarities of forming a cybersecurity management system for enterprises in wartime: theoretical and applied aspect

The article examines the peculiarities of forming a cybersecurity management system for enterprises in wartime. The paper presents the theoretical and applied aspect of this issue.

The purpose of the article is to study the peculiarities and theoretical and applied aspects of forming a cybersecurity management system for enterprises in wartime. The main methods used in the study are analysis, synthesis, statistical methods, etc.

The importance of enterprise cybersecurity management for their economic security and achievement of the required level of national security is substantiated. A review and analysis of literary sources on the problem of defining the essence of the concept of "cybersecurity" is carried out. It is proved that for effective cybersecurity management it is advisable to classify cyberattacks. It is also advisable to add the following classification features to the existing classification features: "by the level of insurance", i.e. whether it is possible to insure (over-insure) against the threat itself and its consequences, and "by the level of loss", i.e. the level of losses from cyber attacks.

Modern cyberattacks and their consequences are analyzed. The key stages of building an effective cybersecurity management system are formed. The key aspects of determining the security policy of enterprises, their proactive response to highly dynamic economic conditions (primarily in the field of cybersecurity) in wartime are indicated. The system of enterprise cybersecurity management and organization should provide for the possibility of timely selection of specific means and ways to ensure it.

The author analyzes the functional and managerial aspect of forming a cybersecurity management system for enterprises in wartime. The key measures to develop the potential of the security and defense sector of Ukraine are investigated.

The study proposes a conceptual model for the formation of an effective cybersecurity management system for enterprises in wartime. Each of its stages is characterized. The functions of the cybersecurity management system of enterprises in wartime are described.

***Key words**: risks, security, cybersecurity, management system, cybersecurity management, management functions.*

Стаття надійшла до редакції 01.03.2024 р.

Бібліографічний опис статті:

Завербний А. С. Особливості формування системи управління кібербезпекою підприємств у воєнний період: теоретико-прикладний аспект. *Innovation and Sustainability*. 2024. № 1. С. 13-21.

Zaverbnyj A. (2024) Peculiarities of forming a cybersecurity management system for enterprises in wartime: theoretical and applied aspect. *Innovation and Sustainability*, no. 1, pp. 13-21.