ЕКОНОМІКА ТА УПРАВЛІННЯ НАЦІОНАЛЬНИМ ГОСПОДАРСТВОМ

УДК 338.22
DOI: https://doi.org/10.32782/business-navigator.71-3

Васильків Б.Л.
аспірант кафедри економіки України
Львівський національний університет імені Івана Франка

Vasylkiv Bohdan
PhD Student at the Department of the Ukrainian Economy
Ivan Franko Lviv National University

КІБЕРБЕЗПЕКА ЯК НАПРЯМОК ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОГО СЕКТОРУ В СУЧАСНИХ УМОВАХ

Васильків Б.Л. Кібербезпека як напрямок захисту інформаційно-комунікаційного сектору в сучасних умовах. У статті досліджено роль кібербезпеки у захисті інформаційно-комунікаційного сектору, який надає основні послуги, що забезпечують соціальну, економічну та політичну діяльність. Відповідно до Global ICT Regulatory Outlook, Україна посідає низьке місце в регулюванні досліджуваної сфери – 78 місце з 96 країн. Однак Україна досягла значного прогресу в кібербезпеці, як підкреслює Глобальний індекс кібербезпеки. У проведено аналіз прогресу України в кібербезпеці, зокрема у сфері управління інцидентами та кризовими ситуаціями, військових кібероперацій та базових показниках кібербезпеки. Незважаючи на позитивні зрушення, країна все ще стикається з проблемами, особливо у сфері захисту цифрових послуг, для якої відсутній компетентний наглядовий орган. Питання кіберзахисту економіки в умовах повномасштабного російського вторгнення в Україну набуває особливої актуальності та виділяється в окремий напрямок державної політики.

Ключові слова: інформаційно-комунікаційний сектор, кібербезпека, Глобальний індекс кібербезпеки, кіберзахист, військові кібероперації.

Vasylkiv Bohdan. Cyber security as a direction of protection of the information and communication sector in modern conditions. Ensuring the protection of the information and communication sector is an important component in the country's economic growth and further progress. The issue of cyber security of the information and communication sector stands out as an important direction both at the international and at the state level. In times of war, cyber threats can have serious consequences, including financial losses, reputational damage, legal liabilities, and risks to both national security and individual sectors. It is analyzed the progress of Ukraine in cyber security based on such indicators as general security indicators, basic cyber security indicators, incident and crisis management indicators in the article. According to the Global ICT Regulatory Outlook, Ukraine ranks low in the regulation of the studied area – 78th out of 96 countries. However, Ukraine has made significant progress in cyber security, as highlighted by the Global Cyber Security Index. According to most of the general indicators, full implementation is highlighted, among the basic indicators there is a need to increase the protection of digital services, according to the indicators of incident and crisis management, military cyber operations and cyber crisis management are the least developed. Cyber threats can result in significant consequences during times of war, including financial loss, reputational damage, legal liabilities, and risks to national security. At the beginning of the war, more than 120 powerful cyber attacks on the resources of state authorities and military administration of Ukraine, as well as IT systems of critical infrastructure facilities, communication operators and mass media. Despite the positive developments, the country still faces challenges, especially in the area of protection of digital services, for which there is no competent supervisory authority. The need for cyber security in the information and communication sector and measures that can be taken to increase cyber resilience are highlighted, especially in the area of protection of digital services. Parties should cooperate with the government to improve cyber resilience. Cooperation may include sharing threat information, best practices, and resources, and coordinating incident response and recovery efforts. The issue of cyber defense of the economy in the conditions of a full-scale Russian invasion of Ukraine is gaining special relevance and is allocated to a separate direction of state policy.

Key words: information and communication sector, cyber security, Global Cyber Security Index, cyber defense, military cyber operations.

Постановка проблеми. В останні роки світ став свідком експоненційного зростання інформаційного-комунікаційного сектору із використанням нових технологій та розширенням спектру діяльності. Це зростання принесло значні переваги, зокрема підвищення продуктивності, покращення зв'язку та покращення доступу до інформації. При цьому також формувалися нові форми кіберзагроз, які створюють серйозні ризики для конфіденційності, цілісності та доступності цифрової інформації. Кіберзагрози включають різні форми зловмисної діяльності, такі як хакерство, зловмисне програмне забезпечення, програми-вимагачі, фішинг і крадіжка особистих даних, що суттєво відображається на безпеці та захисті даних підприємств державного та приватного сектору. У результаті кібербезпека стала критичною необхідністю для всіх сторін у секторі інформації та комунікацій.

Аналіз останніх досліджень і публікацій. Питання якості кібербезпеки в інформаційно-комунікаційному секторі присвячено праці вітчизняних та закордонних дослідників, зокрема, сферу державного та міжнародного нормативного-правового регулювання виділено М. Василенком, позиції України у міжнародних рейтингах з кібербезпеки досліджували С. Онищенко, А. Глушко. Недостатню увагу приділено деталізованому аналізу кібербезпеки за показниками та підпоказниками відповідно до окремого міжнародного рейтингу.

Постановка завдання дослідження. Метою статті є визначення стану кібербезпеки України, та її впливу на інформаційно-комунікаційний сектор.

Виклад основного матеріалу дослідження. Інформаційно-комунікаційний сектор відіграє вирішальну роль у сучасній економіці, надаючи основні послуги, які забезпечують соціальну, економічну та політичну діяльність. Сектор охоплює широкий спектр організацій, включаючи телекомунікаційні, інтернет-провайдерів, платформи електронної комерції, фінансові установи, постачальників медичних послуг та державні установи, серед інших. Ці організації покладаються на ІКТ для зберігання, обробки та передачі конфіденційних даних, таких як фінансові записи, особиста інформація, комерційна таємниця та інформація про національну безпеку, Кіберзагрози можуть мати серйозні наслідки для інформаційно-комунікаційного сектору, зокрема фінансові втрати, репутаційні збитки, юридичні зобов'язання та ризики для національної безпеки.

Питання кібербезпеки інформаційно-комунікаційного сектору виділяється важливим напрямком як на міжнародному, так і на державному рівнях. У міжнародному контексті питання кібербезпеки виділяється у Резолюції Генеральної Асамблеї ООН, у якій було виділено розвиток у суспільствах культури кібербезпеки при застосуванні та використанні інформаційних технологій. Також необхідність формування, розвитку та впровадження глобальної культури кібербезпеки зазначено у Женевській декларації, та виділено співробітництво у даній сфері між усіма зацікавленими сторонами та компетентними міжнародними органами [1, с. 36–37].

У міжнародному вимірі розроблено глобальні індекси, що дають змогу оцінити можливості країн у сфері кіберзахисту та їх кіберпотужність, спроможність регуляторних заходів та засобів щодо досягнення стратегічних цілей кібербезпеки [2, с. 16].

За даними Global ICT Regulatory Outlook 2020 [3] Україна займала 78 позицію із 96 країн, що характеризує як низький рівень розвитку регулювання досліджуваної сфери. Прогрес і вдосконалення регулювання інформаційно-комунікаційних технологій є потужною заявою про прагнення до розвитку, і жодна країна не може дозволити собі втратити значну можливість, яку представляє все більш відкритий і динамічний ринок.

Згідно Global Cybersecurity Index (Глобальний індекс кібербезпеки) [4], що включає в себе три основні показники, а саме загальні показники безпеки, базові показники кібербезпеки, показники управління інцидентами та кризи, Україна займає 24 місце серед 161 країни.

Проведений аналіз показав, шо Україна значний розвиток зробила та останні роки за загальними показниками у аналізі кіберзагроз та інформації (створення Національного координаційного центру безпеки та веб-сайт із надання рекомендацій та технічної допомоги), за іншими підпоказниками відсотковість впровадження державою окремих заходів залишалася на однаковому рівні (рис. 1).

У 2022 році війська зв'язку та кібербезпеки набули статусу окремого роду військ відповідно до закону «Про основи національного спротиву». Війська зв'язку та кібербезпеки – спеціальні війська, призначені для планування та забезпечення розгортання, згортання, функціонування системи зв'язку та інформаційних систем, систем бойового управління та оповіщення, їх нарощування в мирний час, особливий період, в умовах надзвичайного та воєнного стану з метою вирішення завдань забезпечення управління військами (силами) Збройних Сил України, а також здійснення заходів функціонування національної системи кібербезпеки та відбиття воєнної агресії у кіберпросторі (кібероборони) [6, с. 88].

За базовими показниками кібербезпеки протягом всіх років виділено стовідсоткове виконання захисту персональних даних у пунктах законодавства про захист персональних даних та органу із захисту персональних даних. За показником електронної ідентифікації та довірчих послуг, що допомогло збільшити виконання до ста відсотків, протягом 2017–2021 рр. було створено:

– ідентифікаційний номер платника податків;
– стандарти криптографічного захисту інформації;
– інтегрована система електронної ідентифікації (id.gov.ua);
– електронний цифровий підпис;
– законодавство про електронні довірчі послуги;
– створення Державної служби спеціального зв'язку та захисту інформації України.

Аналогічне збільшення відбувалося також за захистом основних послуг, що передбачало нормативно-правовий акт щодо ідентифікації життєвонеобхідних послуг (Постанова КМУ «Порядок формування переліку об'єктів критичної інформаційної інфраструктури»), Закон України «Про основні засади забезпечення кібербезпеки України», створення компетентного органу у сфері кібер/інформаційної безпеки (Державне агентство з питань електронного урядування України).

Важливим аспектом у захисті інформаційно-комунікаційного сектору є те, що при вільному ринку технічних засобів надається доступ іноземним розвідкам та кримінальним структурам до великого обсягу даних через електронну комунікацію, що на постійні основі створює нові загрози та виклики. При цьому новими викликами стають передумови того, що при отриманні необхідної інформації, державні та приватні служби мають можливість «зламувати» не тільки канали зв'язку, а у людський мозок [7, с. 51].

За показником захисту цифрових сервісів наявна невідповідність у пунктах створення стандарту кібербезпеки для державного сектору та відсутність компетентного наглядового органу (рис. 2).

Питання кіберзахисту економіки в умовах повномасштабного російського вторгнення в Україну набуває окремої актуальності, та виділяється в окремий напрямок діяльності державної політики. Відповідно до показників управління інцидентами та кризовими ситуаціями спостерігається, що найбільшого значення

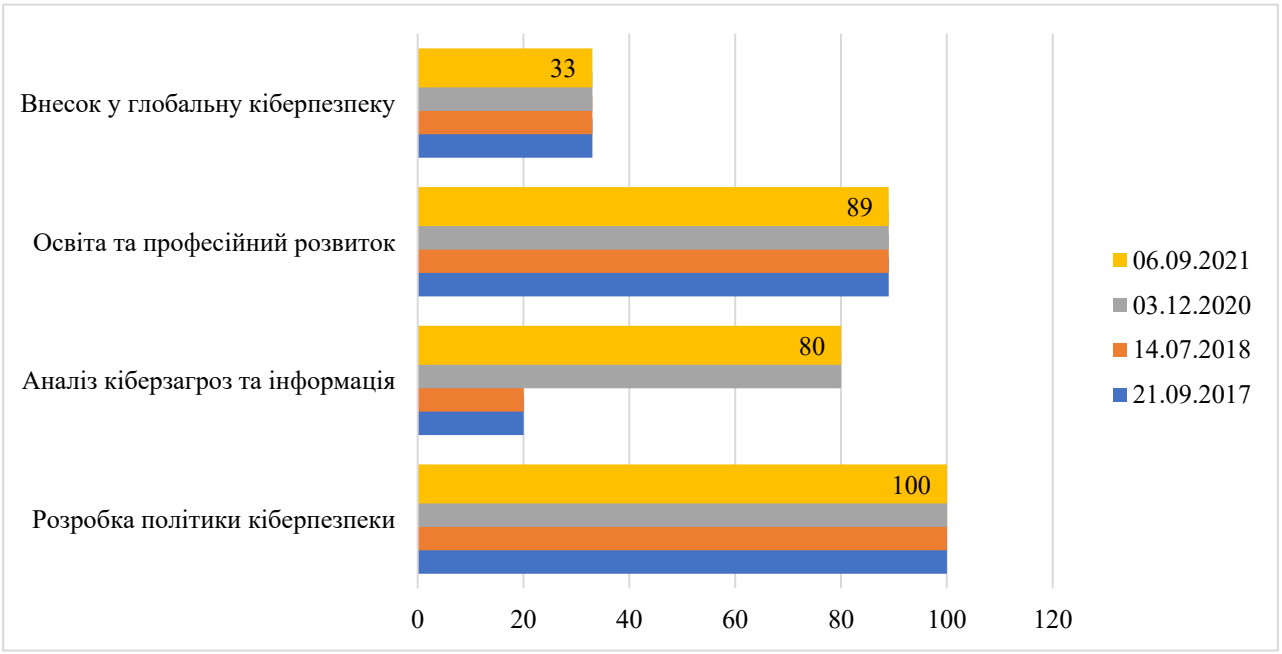

Рис. 1. Загальні показники кібербезпеки, у %

Джерело: розроблено автором на основі [5]

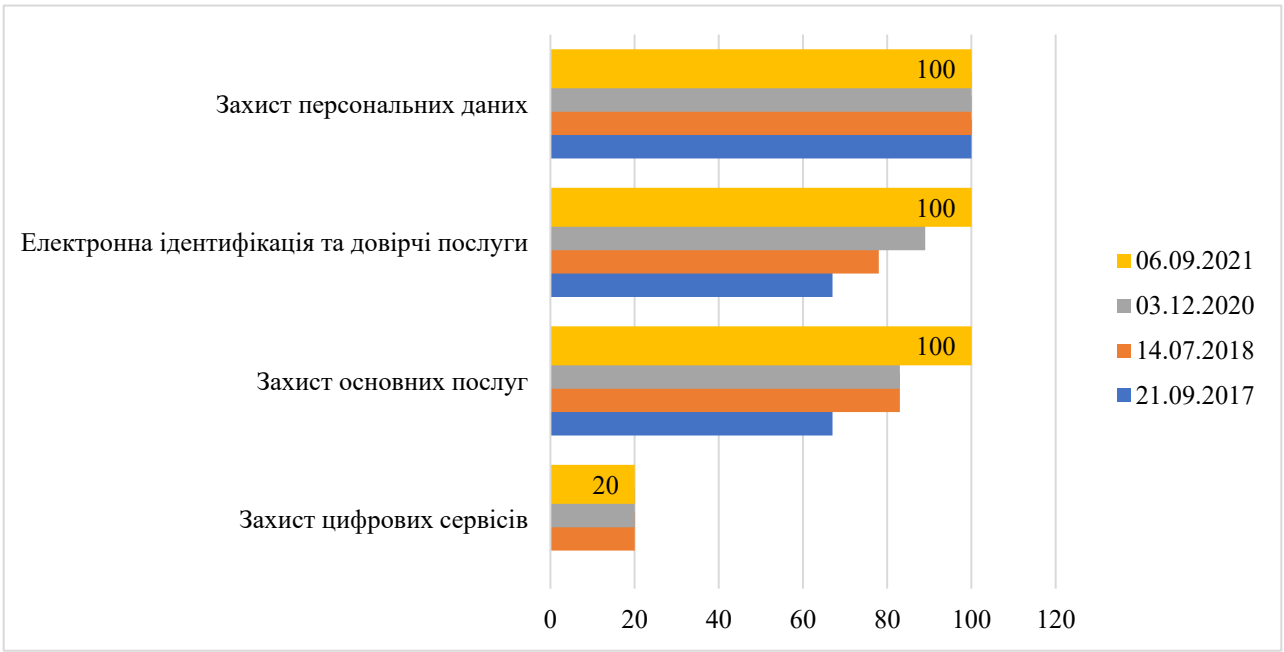

Рис. 2. Базові показники кібербезпеки, у %

Джерело: розроблено автором на основі [5]

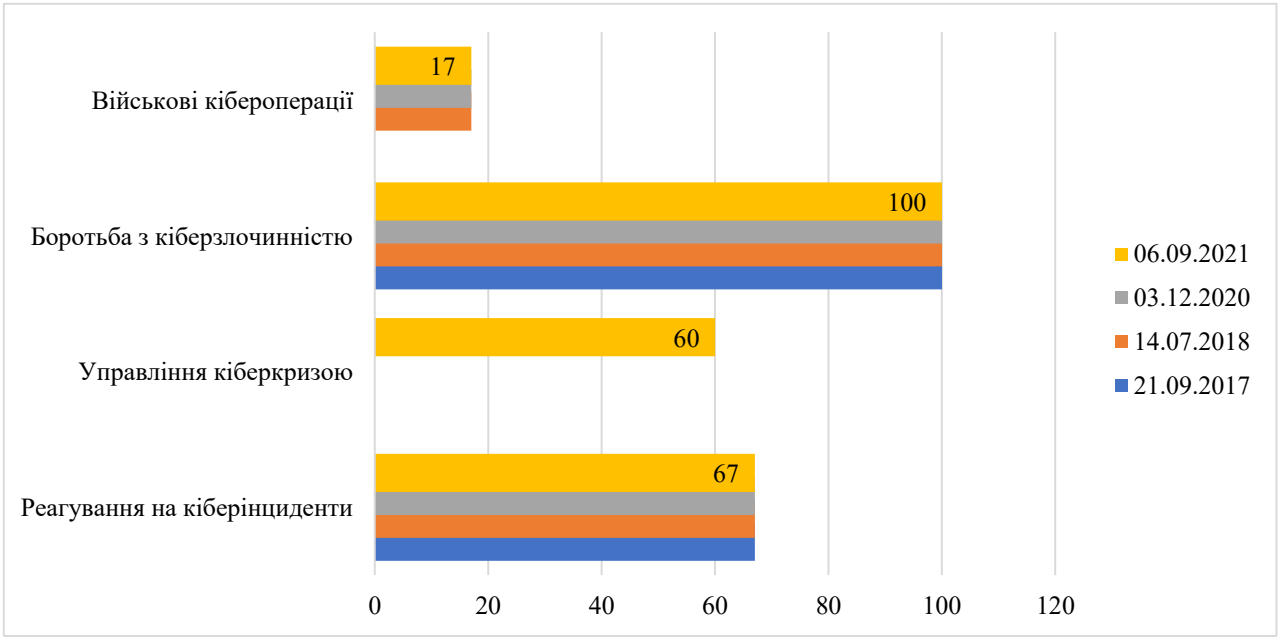

Рис. 3. Показники управління інцидентами та кризовими ситуаціями, у %

Джерело: розроблено автором на основі [5]

набуває тільки боротьба з кіберзлочинністю, а саме у визначення кіберзлочинів у законодавстві, підрозділи боротьби із кіберзлочинністю, цифрової криміналістики та міжнародний цілодобовий контактний пункт для боротьби з кіберзлочинами.

З початку повномасштабного російського вторгнення виявили та нейтралізували понад 120 потужних кібератак на ресурси органів державної влади та військового управління України, а також ІТ-систем об'єктів критичної інфраструктури, операторів зв'язку та ЗМІ. За місяць війни сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року. Найпопулярнішими видами атак залишаються фішингові розсилання, розповсюдження шкідливого програмного забезпечення, DDoS-атаки [8, с. 213].

В останній рік суттєво збільшилося управління кіберкризою у напрямках національного та міжнародного навчань. У реагуванні на кіберінциденти створено підрозділ, який спеціалізується на виявленні та реагуванні на кіберінциденти на національному рівні та звітність щодо інцидентів кібербезпеки, недоліком виступає відсутність єдиної контактної точки для міжнародної координації (рис. 3).

У пункті військових кібероперацій, до початку війни, військова команда приймала участь у міжнародних навчаннях з кібероперацій. Однак, через російське вторгнення в Україну, міжнародні, державні та приватні структури активізували заходи підтримки в даному напрямку, а саме: створення кіберлабораторії Європейським Союзом у Києві для вдосконалення практичних навичок військових фахівців із кіберзахисту [9], поява ІТ-армії, створення спільного проєкту кіберполіцією України, волонтерами та небайдужими громадянами «MRIYA» [10].

Учасники інформаційно-комунікаційного сектору в теперішніх умовах постійної кіберзагрози повинні співпрацювати між собою та з урядом для підвищення кіберстійкості. Співпраця може включати обмін інформацією про загрози, найкращими практиками та ресурсами, а також координацію заходів щодо реагування на інциденти та відновлення.

Висновки. Проведений аналіз показує, що Україна має як позитивні, так і негативні зміни в регулюванні забезпечення кіберзахисту, що впливає на результативний розвиток інформаційно-комунікаційного сектору. Співпраця може бути досягнута шляхом партнерства між собою та з урядом для обміну інформацією про загрози, найкращими практиками та ресурсами. Крім того, заходи з реагування на інциденти та відновлення мають бути скоординовані між зацікавленими сторонами, щоб запобігти кіберзагрозам, які спричиняють значні фінансові втрати, шкоду репутації, юридичні зобов'язання та ризики національній безпеці. Дуже важливо, щоб Україна продовжувала надавати пріоритет кіберзахисту в інформаційно-комунікаційному секторі. Уряд має інвестувати у покращення нормативно-правової бази та впровадження ефективних стратегій кібербезпеки. Крім того, приватний сектор повинен надавати пріоритет кібербезпеці у своїй діяльності та інвестувати в необхідні ресурси та технології для пом'якшення кіберзагроз. Співпраця між усіма зацікавленими сторонами є важливою для того, щоб інформаційно-комунікаційний сектор України був стійким до кіберзагроз і міг сприяти економічному зростанню та розвитку країни.

Список використаних джерел:

1. Василенко М. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення. *Юридичний вісник*. 2018. № 4. С. 35–41.
2. Онищенко С. В., Глушко А. Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон.* 2022. № 1 (84). С. 13–20.
3. Global ICT Regulatory Outlook 2020. URL: https://www.itu.int/pub/D-PREF-BB.REG_OUT01-2018.
4. Global Cybersecurity Index. URL: https://ncsi.ega.ee/country/ua.
5. The National Cyber Security Index. URL: https://ncsi.ega.ee/country/ua/529/#details.
6. Островський С. О. Правовий статус військ зв'язку та кібербезпеки в системі збройних сил України. Київський часопис права. 2022. № (3). С. 86–91.
7. Соснін О. В. До питання протидії стійкості інформаційно-комунікаційним загрозам. *Юридична Україна.* 2019. № 11. С. 49–59.
8. Філіпенко Н. Є. Протидія кібератакам на об'єкти критичної інфраструктури та життєзабезпечення під час військової агресії проти України. *Український дослідницький простір в умовах війни: адаптація й перезавантаження технічних і юридичних наук*. Харків-Рига. 2022. С. 213–216.
9. Для ЗСУ створили кіберлабораторію. URL: https://mil.in.ua/uk/news/dlya-zsu-stvoryly-kiberlaboratoriyu.
10. Платформа MRIYA. URL: https://mriya.social.

References:

1. Vasylenko M. (2018) Quality of Cybersecurity of Information and Communication Systems (ICS) and Some Legislative Issues for its Enhancement. *Juridical Herald.* № 4. P. 35–41.
2. Onyshchenko S. V., Hlushko A. D. (2022) Analytical Dimension of Cybersecurity of Ukraine in the Conditions of Growing Challenges and Threats. *Economy and Region.* № 1 (84). P. 13–20.
3. Global ICT Regulatory Outlook 2020. Available at: https://www.itu.int/pub/D-PREF-BB.REG_OUT01-2018.
4. Global Cybersecurity Index. Available at: https://ncsi.ega.ee/country/ua.
5. The National Cyber Security Index. Available at: https://ncsi.ega.ee/country/ua/529/#details.
6. Ostrovsky S. O. (2022) The legal status of communications and cyber security forces in the system of the armed forces of Ukraine. Kyiv. *Journal of Law.* № (3). P. 86–91.
7. Sosnin O. V. (2019) On the Issue of Resistance to Information and Communication Threats. *Juridical Ukraine*. № 11. P. 49–59.
8. Filipenko N. Ye. (2022) Countering Cyber Attacks on Critical Infrastructure and Life Support During Military Aggression Against Ukraine. Ukrainian Research Space in the Conditions of War: Adaptation and Restart of Technical and Legal Sciences. Kharkiv-Riga. P. 213–216.
9. A cyber laboratory was created for the Armed Forces of Ukraine. Available at: https://mil.in.ua/uk/news/dlya-zsu-stvoryly-kiberlaboratoriyu.
10. Platforma MRIYA. Available at: https://mriya.social.