найважливішим та актуальнішим. Ці питання є стратегічними не лише для країн, в яких рівень кібербезпеки є найбільшим чи високим, а й країн, що розвиваються, та найбільше стосується країн, які відчувають саме зараз найбільші кібератаки на просторі свої країни, до яких саме належить Україна [2].

Тож державна політика щодо запобігання економічній злочинності має забезпечити високий рівень її ефективності, приносити економічну, соціальну та безпекову користь для суспільства та забезпечити гарантування економічної безпеки держави.

Для боротьби із економічними злочинами необхідно брати до уваги міжнародний досвід країн із низьким рівнем економічної злочинності, враховувати рівень якості життя населення, який формує рівень розвитку країни і є основою для економічної та національної безпеки.

_____--

1. Rybalchenko L., Kosychenko A. Ensuring economic security of enterprises taking into account the peculiarities of information security. Scientific journal «Philosophy, Economics and Law Review». 2022. 2 (1). S. 96–107.

2. Rybalchenko L. Cybercrime in the global space. *Науковий вісник ДДУВС*. 2022. Спец. вип. № 2. С. 524–530.

Рижков Едуард Володимирович
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ФОРМУВАННЯ СТРАТЕГІЇ КІБЕРЗАХИСТУ В УМОВАХ ВОЄННОГО СТАНУ

Державницькі зусилля щодо формування стратегії кіберзахисту в Україні мають свою історію й етапи. Але критерієм їх ефективності має бути не історичний опис, а конкретний результат здатності уповноважених суб'єктів протистояти посяганням на кіберпростір держави, а також їх відповідність ступеню та характеру небезпеки з урахуванням динаміки та складності існуючих загроз.

Безумовно, система наявних кіберсуб'єктів за останні 20 років набула сталих ознак та розвитку. Проте вона не задовольняла потреби нашого суспільства з огляду на загрози, що їх принесла із собою російська воєнна агресія. Основною проблемою стала недосконала координація дій вже наявних суб'єктів протидії кіберінцидентам з огляду на необхідність оперативного супроводу основного суб'єкту захисту держави в умовах воєнного стану – Збройних Сил України. Ситуація унеможливлювала ефективну реалізацію з

боку Збройних Сил України операцій протидії ворогові із використанням кіберсередовища. Тому в умовах, коли об'єктивно всі ознаки вказують на реальну кібервійну за участі України, виникла потреба у створенні такого нового суб'єкта, як кібервійська в структурі Збройних Сил України з наступною потребою їх кадрового забезпечення.

З боку керівництва держави було вжито певних заходів. Протягом 2021 року видана низка нормативних актів. Серед них Указ Президента України від 26 серпня 2021 року № 446/2021 «Про невідкладні заходи з кібероборони держави» та Указ Президента України від 26 серпня 2021 року№ 447/2021 «Про Стратегію кібербезпеки України» [1, 2].

Зазначеними нормативними актами було продекларовано створення в Україні кібервійськ. Рекрутування фахівців у сфері ІТ було розпочато у різних формах: від ананімного через спеціалізовані чат-боти до централізованого анкетування з формуванням відповідної бази фахівців [3]. Хоча і передбачається, що після ухвалення відповідного закону кібервійська будуть частиною Міноборони, наразі майбутніх кібербійців планується розподілити між різними структурами, що вже відповідають за кібербезпеку: Службою безпеки України, Державним спеціальним зв'язком, кіберполіцією, Радою національної безпеки та оборони, Національним банком України, Міністерством цифрофої трансформації, Міністерством оборони, Збройними Силами України та розвідкою.

Треба наголосити, що серед основних причин, які зумовили реалізацію ініціативи фахівців у створенні в Україні кібервіськ, є безумовно агресія росіян у кіберпросторі по відношенню до нашої держави, а також поступова та неухильна інтеграція країни до альянсу з НАТО та Європейської спільноти. Проте, доцільно зазначити що створення кібервійськ в державі та забезпечення їх ефективного функціонування – то справа не на місяці, а на роки. Зокрема, кібервійська США (United States Cyber Command або USCYBERCOM) офіційно сформувалися у 2009 році, а неофіційно – як мінімум 20–30 років тому. Основними завданнями USCYBERCOM – є централізоване проведення операцій кібервійни, управління і захист військових комп'ютерних мереж США [4]. Тобто підготовчий період офіційної появи зайняв термін, який Україна, враховуючи реалії військової ситуації, не може собі дозволити. Наразі у США у кібервійську 9 тисяч військовослужбовців, у Великобританії приблизно дві тисячі, у росії також десь тисяча.

На старті за різними оцінками експертів якість системи вітчизняного кіберзахисту у період війни коливається від достатнього (очами фахівців державницького сектору) до незадовільного (на думку незалежних фахівців). У цих умовах безумовним є той посил, що допомога ІТ-фахівців та реалізована з боку держави ініціатива була б дуже актуальною.

До сьогодні немає закону про кібервійська. Є лише законопроєкт. Тому цифровізація ЗСУ відбувається за іншим сценарієм. Новітнє західне озброєння, волонтерська допомога, новаторські рішення на рівні програмного

забезпечення поступово призвели до розуміння необхідності та поступового втілення цифри у фронтові реалії. І на сьогодні «КРОПИВА», як приклад прикладного програмного забезпечення у військах, є звичною та незамінною.

Поступово в ЗСУ без спеціалізованого закону формується відповідна кіберінфраструктура та на теоретичному рівні вимальовується перспективна структура Кіберкомандування кіберсил ЗСУ [4].

В умовах військової мобілізації до лав Збройних Сил України потрапляє певна кількість фахівців у сфері інформаційних технологій, для яких з огляду на державницький інтерес комп'ютер більш раціональна зброя, ніж будь-яка інша. Механізм виявлення та залучення таких фахівців до кібервійськ чи його резерву повинен працювати на випередження їх можливої втрати на полі бою.

Треба зазначити, що положення офіційної Стратегії кіберзахисту доповнюються законодавчими ініціативами, що здатні суттєво змінити баланс пріоритетів створення та функціонування уповноважених суб'єктів кіберзахисту та послабити роль кіберпідрозділів ЗСУ.

У 2023 р. Верховна Рада України ухвалила у першому читанні за основу проєкт Закону про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури (реєстр. № 8087).

У проєкті пропонується внести зміни до низки законів України,

спрямовані на нормативне забезпечення захищеності від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, на створення належної правової основи для здійснення заходів з попередження, виявлення і припинення актів агресії у кіберпросторі в умовах війни російської федерації проти України, а також на загальне удосконалення нормативно-правової бази у сфері кібербезпеки та захисту інформації задля посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам.

Зокрема, запропоновані зміни до законів України «Про Державну службу спеціального зв'язку та захисту інформації України» та «Про основні засади забезпечення кібербезпеки України» передбачають створення та забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та визначення Державної служби спеціального зв'язку та захисту інформації України уповноваженим органом, що здійснює забезпечення функціонування цієї системи.

Серед іншого пропонується: створити в органах державної влади, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, підрозділи із кіберзахисту; призначати у вищевказаних органах офіцерів із кіберзахисту, яким безпосередньо підпорядковуються підрозділи із кіберзахисту; надати право Держспецзв'язку визначати функції, повноваження, загальні вимоги до підрозділів із кіберзахисту та їх співробітників, а також особливості правового статусу та загальні вимоги до офіцерів із кіберзахисту [5].

У березні 2023 р. Держспецзв'язку заявило, що в кіберармії України перебувають 400 тисяч людей, які самі організувалися для боротьби з росією. Нехай повноцінні війська зібрати так і не встигли, але оборонний потенціал у кіберпросторі українці мають [6].

Проте по факту маємо ситуацію, в якій залучено до співпраці лише десятки фахівців з тисяч. Виникає питання, чому склалася така ситуація? Чому у глухому «резерві» вже протягом року перебувають дуже цінні для країни фахівці, які не можуть знайти собі прямого застосування, щоб протидіяти ворогові у кіберпросторі? Або кураторів з числа представників державницького сектору у спеціалізованих суб'єктів не вистачає, або мета анкетування була зовсім не та, що продекларована? Картинка налагодження співпраці з представниками населення є, але результат зовсім не той, що очікували [7, с. 58].

Така протилежність оцінок ситуації та різна спрямованість державницьких зусиль зумовлена зволіканням законотворців та інших суб'єктів, які так і не реалізували до цього часу положення офіційної Стратегії кіберзахисту України в частині ухвалення Закону «Про кібервійська України», що є неприпустимим з огляду на сучасні загрози нашій державності. Збройні

Сили України, їх кіберпідрозділи, а у найближчий час і кібервійська повинні бути основним пріоритетом державницької політики щодо розвитку суб'єктів кіберзахисту в період воєнного протистояння з російським ворогом.

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» : Указ Президента України від 26 серпня 2021 року № 446/2021. URL: https://www.president.gov.ua/documents/4462021-40009

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

3. Українців запросили долучитися до кібервійськ – заступник секретаря РНБО. URL: https://fakty.com.ua/ua/ukraine/suspilstvo/20220217-ukrayincziv-zaprosyly-doluchytysya-do-kibervijsk-zastupnyk-sekretarya-rnbo/

4. Леднєй Вадим: «Метою діяльності кіберсил ЗСУ є захист суверенітету держави та відсіч збройної агресії в кіберпросторі». URL: https://lb.ua/news/2023/01/31/544318_vadim_liedniey_metoyu_diyalnosti.html

5. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури : проєкт закону. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40553

6. В Україні досі немає кібервійськ: експерт розповів, коли вони з'являться і навіщо потрібні. URL: https://focus.ua/uk/digital/518279-v-ukraine-do-sih-por-net-kibervoysk-ekspert-rasskazal-kogda-oni-poyavyatsya-i-zachem-nuzhny

7. Ryzhkov E. Problematic issues of staffing cyber troops of Ukraine under martial law. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2022. Special Issue. № 1 (120). S. 55–60. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/04/S1/NV_DDUVS_spec_1_2022-55-60.pdf