Система має миттєвий доступ до відеокамер на інтерактивній мапі як в реальному режимі, так і в записі, тому дозволяє оперативно відстежувати дії правопорушників, фіксувати обставини злочинів, збирати доказову базу, а також швидко реагувати на ситуації на вулицях міста.

Ці ЕС та інші сприяють підвищеній ефективності роботи правоохоронних органів шляхом автоматизації процесів пошуку доказової бази, фіксації правопорушень і прийняття рішень щодо них.

Найбільшою перевагою подібних систем у кожній області є те, що це, фактично, усі знання з певної галузі, акумульовані в одній системі. Варто зазначити, що ЕС не може приймати рішення за співробітника, її функція – якісне, об'ємне консультування.

Експертні системи в галузі права будуються на загальних та спеціальних знаннях в праві: існуючих правових концепціях, структурі правил, особистісному сприйнятті права, правової системи та підсистем, юридичної аргументації, логіці, семантиці, соціології та психології права, а також філософських теоріях, що носять загальний характер.

Список використаних джерел:

1. Експертні системи: особливості застосування. URL: https://osvita.ua/vnz/reports/management/13574
2. Мазниченко Н. Місце і значення експертних систем в області права. 2020. URL: http://ir.librarynmu.com/bitstream/123456789/2120/1/2020.10.6-8.pdf#page=193.

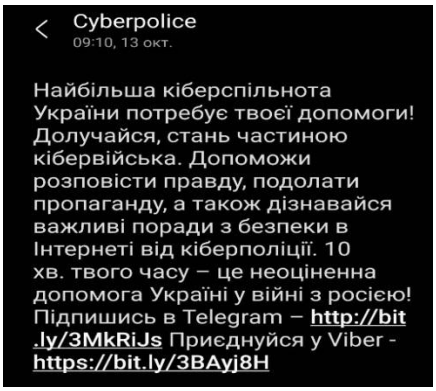
Рижков Е. В.,
професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ПРОБЛЕМНІ ПИТАННЯ ФОРМУВАННЯ КІБЕРВІЙСЬК В ПЕРІОД ВОЄННОГО СТАНУ В УКРАЇНІ

Повномасштабному вторгненню росії в Україну передувала серія глобальних кібератак на об'єкти нашої кібернетичної інфраструктури. Було атаковано понад 70 урядових та державних інформаційних ресурсів та систем. Фактично, ми отримали повномаштабну кібервійну, яка в попередні 8 років мала підготовчий період з боку агресора та безліч кібератак по відношенню до нашої країни.

Готуючись до цього, в Україні було вжито певних заходів. Так протягом 2021 року видана низка нормативних актів. Серед них Указ Президента Укріни 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].

Фактично, вказаними документами було запроваджено створення в Україні кібервійськ. Рекрутування фахівців у сфері ІТ було розпочато у різних формах: від ананімного через спеціалізовані чат-боти:



Хоча кібервійська і будуть частиною Міноборони після прийняття відповідного закону, майбутніх кібербійців планувалось розподілити між різними структурами, що відповідають за кібербезпеку: СБУ, Держспецзв'язку, кіберполіцією, РНБО, НБУ, Мінцифри, Міноборони, ЗСУ та розвідкою.

На прикладі США структура кіберкомандування кібервійськ виглядає наступним чином:

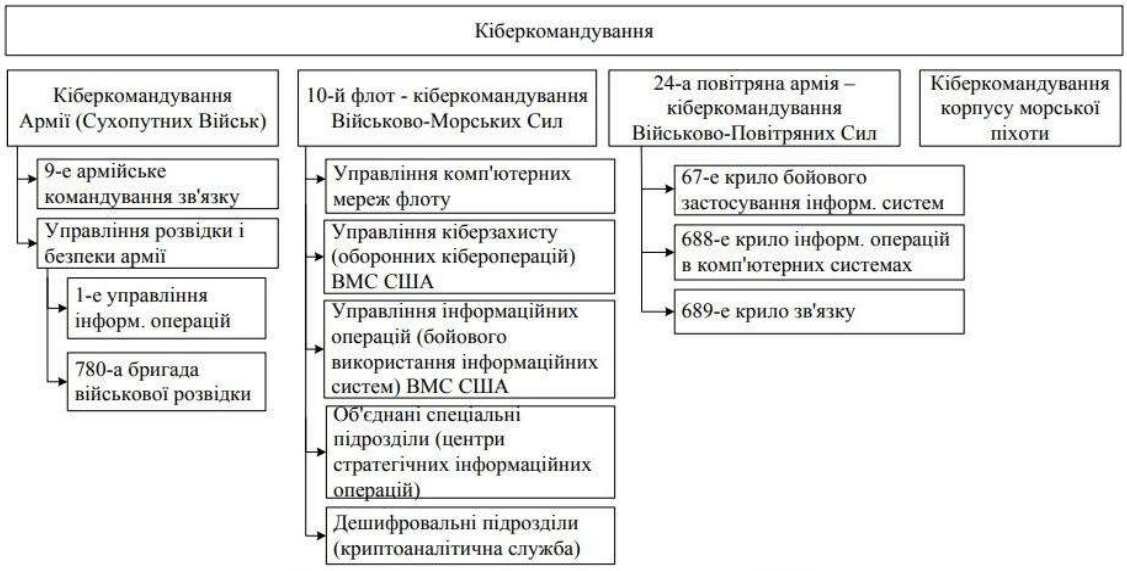


Рис. 1. Структура Кіберкомандування США

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 [3].

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 вкрай актуальною.

Проте, по факту маємо ситуацію в якій залучено до співпраці лише десятки фахівців з тисяч, що подали анкети. Виникає питання чому склалася така ситуація? Чому у глухому «резерві» вже протягом року знаходяться вкрай 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 чи мета анкетування була зовсім та, що продикларована? Картинка налагодження співпраці з представниками населення є. Результат мінімальний від можливого.

Ще одна проблема чітко позначилась напередодні повномасштабного вторгнення. Це відкриття кримінальних проваджень відносно найбільш кваліфікованих вітчизняних ІТ-фахівців, що пропонували свої послуги державі задля боротьби з рашистами. Після декількох спроб встановлення конструктивної взаємодії та обєднання зусиль з відповідними державними структурами вони були як мінімум деморалізовані, а за фактом нейтралізовані в цьому напрямі [4]. Типовим прикладом цьому є Ukrainian Cyber Alliance «Украинский кибераьянс» (УКА) [5]. «Тепер не буде жодних нічних дзвінків про допомогу, не буде публікацій, не буде консультацій удень і вночі для різних державних силових відомств. Все зупинилося», – заявив, у свою чергу, співзасновник компанії Олександр Галущенко [6].

Головна міжнародна мережа хакерів Anonymous оголосивши війну владі Росії [7]. Наразі вона також діє самостійно, демонструючи свою безумовну ефективність у кіберпросторі ворога [8].

За період війни з росією маємо безліч ганебних фактів саботажу, колобаранства та державної зради з боку представників різних ланок державницького сектору (безвійськова здача Криму, Іловайський котел для добробатів, размінування проходів до Херсонщини, знаходження джевелінів у амбарах замість передовій у лютому 2022 р. та інш.), які отримають свою правову оцінку після перемоги [9]. Що стосується захисту представників Українського кібераьянсу від кримінального переслідування, то такі спроби з боку представників законодавчого органу влади вже мали місце [10].

Чи виправиться ситуація і коли з вказаних нами вище проблем – є риторичним питанням. Причина в тому, що сфера кіберзахисту держави в Україні у силу своєї специфіки є вкрай консервативна, закрита та практично не досяжна для здійснення контролю з боку громадськості.

Безумовно, одним із можливих вариантів співпраці кібер-аматорів з правоохоронними структурами може бути реалізована в рамках конфіденційності [11]. Проте, вказані приклади поки що свідчать про протилежне.

Безумовним є той факт, що кіберзахист є однією з основних складових безпеки держави, а його ефективність – запорукою перемоги над ворогом у кіберпросторі. Сама ж ефективність повинна реалізовуватись через конструктивну співпрацю правоохоронних та військових структур із населенням – у нашому випадку фахівцями у ІТ сфері. Проте, темпи розробки вітчизняного законопроекту щодо створення кібервійськ суттєво відстають від успіхів ЗСУ на фронті, а його прийняття та вступ в дію ризикує відбутися вже після перемоги України над рашизмом.

Список використаних джерел:

1. Указ Президента України від 26.08.2021 р. № 446/2021 Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про невідкладні заходи з кібероборони держави». URL: https://www.president.gov.ua/documents/4462021-40009.
2. Указ Президента України від 26.08.2021 р. № 447/2021 Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про Стратегію кібербезпеки України». 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-ukrayinciv-zaprosyly-doluchytysya-do-kibervijsk-zastupnyk-sekretarya-rnbo/
4. РНБО видала розпорядження створити Кібервійська в Україні. Що це буде? URL: https://www.ukrinform.ua/rubric-technology/3316171-rnbo-vidala-rozporadzenna-stvoriti-kibervijska-v-ukraini-so-ce-bude.html.
5. Про українських хактивістів, кібервійну та вразливості в держсекторі. Інтерв'ю з членом Ukrainian Cyber Alliance Андрїєм Барановичем. URL: https://dou.ua/lenta/interviews/story-of-ukrainian-cyber-alliance/
6. Український кіберальянс. URL: https://ru.wikipedia.org/wiki.
7. «Український кіберальянс» припиняє діяльність в Україні. URL: https://censor.net/ua/n3178085.
8. Хакери Anonymous 3 березня обіцяють спустошити рахунки росіян і направити кошти на ЗСУ. URL: https://uagit.tv/2022/2/28/16206-hakery-anonymous-3-bereznya-obitsyayut-spustoshyty-rahunky-rosiyan-i-napravyty-koshty-na-zsu-video.
9. Хакери Anonymous збільшили атаки на офіційні сайти російських органів влади у два-три рази. URL: https://uagit.tv/2022/3/19/16641-hakery-anonymous-zbilshyly-ataky-na-ofitsiyni-sayty-rosiyskyh-orhaniv-vlady-u-dva-try-razy.
10. Рижков Е. В. Протидія корупції в ОВС. *Науковий вісник ДДУВС*. 2015. № 3. С. 19-24.
11. В «ЄС» вимагають від влади припинити переслідування «Українского кіберальянсу» URL: https://www.5.ua/ru/polytyka/v-es-trebuiut-ot-vlasty-prekratyt-presledovanye-ukraynskoho-kyberaliansa-209613.html.
12. Рижков Е. В., Маклаков Г. Ю. Особливості оперативно-розшукової діяльності при розслідуванні злочинів у сфері високих технологій. *Використання сучасних досягнень криміналістики у боротьбі зі злочинністю*: матер. міжвуз. наук.-практ. конф. студентів, курсантів і слухачів (м. Донецьк, 12 квітня 2002 р.). Донецьк: ДІВС, 2002. С. 19-29.