DOI https://doi.org/10.51647/kelm.2022.4.58

FUNKCJE BEZPIECZEŃSTWA CYBERNETYCZNEGO I PRZECIWDZIAŁANIA CYBERPRZESTĘPCZOŚCI W WARUNKACH STANU WOJENNEGO W UKRAINIE

Oleksandr Kolosov
aspirant Katedry Wymiaru Sprawiedliwości w Sprawach Karnych
Dydaktyczno-Naukowego Instytutu Prawa Państwowego Uniwersytetu Podatkowego (Irpień, Ukraina)
ORCID ID: 0000-0003-0128-5565
kolosov2424@gmail.com

Lyubov Omelchuk
kandydat nauk prawnych, docent,
docent Katedry Wymiaru Sprawiedliwości w Sprawach Karnych
Dydaktyczno-Naukowego Instytutu Prawa Państwowego Uniwersytetu Podatkowego (Irpień, Ukraina)
ORCID ID: 0000-0002-2457-0118
o.l.v.0328@gmail.com

Adnotacja. Artykuł bada cechy bezpieczeństwa cybernetycznego i przeciwdziałania cyberprzestępczości w warunkach stanu wojennego w Ukrainie. W artykule podkreślono przypadki cyberzagrożeń w Ukrainie w czasie stanu wojennego, przeanalizowano zmiany w przepisach prawa w zakresie zapewnienia cyberbezpieczeństwa i przeciwdziałania cyberprzestępczości w warunkach stanu wojennego w Ukrainie, sformułowano propozycje na podstawie wykorzystanych źródeł w celu poprawy bezpieczeństwa cybernetycznego w Ukrainie. Przeanalizowano zmiany w Kodeksie Karnym Ukrainy dotyczące poprawy skuteczności zwalczania cyberprzestępczości w warunkach stanu wojennego, w szczególności ustawy nr 2149-IX. Uzasadnione jest również stworzenie w Ukrainie możliwości legislacyjnych i organizacyjnych dla trójstronnej współpracy w kierunku zapewnienia cyberbezpieczeństwa między sektorem publicznym i prywatnym a instytucjami naukowo-edukacyjnymi.

Słowa kluczowe: cyberbezpieczeństwo, stan wojenny, cyberprzestępstwo, cyberzagrożenie, przeciwdziałanie, cyberbezpieczeństwo, technologie informacyjne.

FEATURES OF ENSURING CYBERSECURITY AND COUNTERACTING CYBERCRIMES IN THE CONDITIONS OF MARTIAL LAW IN UKRAINE

Oleksandr Kolosov
Postgraduate Student at the Department of Criminal Justice
Educational and Scientific Institute of Law of the State Tax University
(Irpin, Ukraine)
ORCID ID: 0000-0003-0128-5565
kolosov2424@gmail.com

Lyubov Omelchuk
PhD in law, Associate Professor,
Associate Professor at the Department of Criminal Justice
Educational and Scientific Institute of Law of the State Tax University
(Irpin, Ukraine)
ORCID ID: 0000-0002-2457-0118
o.l.v.0328@gmail.com

Abstract. The article examines the features of ensuring cybersecurity and counteracting cybercrimes in the conditions of martial law in Ukraine. The article reflects cases of cyber threats in Ukraine during martial law, the changes to Ukrainian legislation in terms of ensuring cyber security and counteracting cyber crimes in the conditions of martial law in Ukraine are analyzed, proposals based on the sources used to improve cyber security in Ukraine are formulated. The changes to Criminal Code of Ukraine to improve the effectiveness of the fight against cybercrime in the conditions of martial law, in particular, Law No. 2149-IX are analyzed. It also substantiates the creation in Ukraine of legislative and organizational opportunities for trilateral cooperation to ensure cybersecurity between the public and private sectors and scientific and educational institutions.

Key words: cybersecurity, martial law, cybercrime, cyberthreat, counteraction, provision of cybersecurity, information technology.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ КІБЕРЗЛОЧИНАМ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Олександр Колосов
аспірант кафедри кримінальної юстиції
Навчально-наукового інституту права Державного податкового університету (Ірпінь, Україна)
ORCID ID: 0000-0003-0128-5565
kolosov2424@gmail.com

Любов Омельчук
кандидат юридичних наук, доцент,
доцент кафедри кримінальної юстиції
Навчально-наукового інституту права Державного податкового університету (Ірпінь, Україна)
ORCID ID: 0000-0002-2457-0118
o.l.v.0328@gmail.com

Анотація. У статті досліджуються особливості забезпечення кібербезпеки та протидії кіберзлочинам в умовах воєнного стану в Україні. У статті висвітлено випадки кіберзагроз в Україні під час воєнного стану, проаналізовано зміни до українського законодавства у частині забезпечення кібербезпеки та протидії кіберзлочинам в умовах воєнного стану в Україні, сформульовано пропозицій на основі використаних джерел щодо покращення забезпечення кібербезпеки в Україні. Проаналізовано зміни до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану, зокрема Закон № 2149-IX. Також обґрунтовано створення в Україні законодавчих та організаційних можливостей для трьохсторонньої співпраці у напрямку забезпечення кібербезпеки між публічним та приватним секторами та науково-освітіми навчальними закладами.

Ключові слова: кібербезпека, воєнний стан, кібезлочин, кіберзагроза, протидія, забезпечення кібербезпеки, інформаційні технології.

Вступ. На сьогоднішній день в умовах військової агресії Російської Федерації проти України захист українського кіберпростору є одним з ключових завдань в умовах воєнного стану. Таким чином, враховуючи теперішні безпекові виклики Україна потребує пошуку ефективних способів їх подолання.

Проблематкою дослідження забезпечення інформаційної безпеки займалися такі українські вчені як Арістова І. В., Березовська І. Р., Дзьобаня О. П., Калюжний Р. А., Кормич Б. А., Ліпкан В. А., Марущак А. І., Цимбалюк В. С., Юдін О. К. та інші.

Мета статті полягає у дослідженні особливостей забезпечення кібербезпеки та протидії кіберзлочинам в умовах воєнного стану в Україні.

Нормативною базою дослідження є Кримінальний кодекс України, Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII, Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 р. № 2149-IX, Указ Президента України від 26 серпня 2021 року № 447/2021 про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», Постанова Кабінету Міністрів України від 1 липня 2022 р. № 751 «Порядок використання коштів з рахунка Міністерства цифрової трансформації для забезпечення протидії інформаційним загрозам з боку держави-агресора, кіберзахисту, відновлення та розвитку цифрової інфраструктури держави», Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні». Також використовувалась аналітика з публікацій Світового банку та Оранізації об'єднаних націй та інших відкритих інформаційних джерел.

Основна частина. У досліджені використано методи аналізу та синтезу. Проаналізовано нормативно-правовий базис України у частині забезпечення кібербезпеки в Україні в умовах воєнного стану. Завданнями дослідження є:

– висвітлення випадків кіберзагроз в Україні під час воєнного стану;

– аналіз змін до українського законодавства у частині забезпечення кібербезпеки та протидії кіберзлочинам в умовах воєнного стану в Україні;

– формування пропозицій на основі використаних джерел щодо покращення забезпечення кібербезпеки в Україні.

Використання інформаційних технологій є невід'ємною частиною кожної соціально активної людини в Україні. Державний та приватний сектори економіки поступово переходять на електронний документообіг, що значно полегшує роботу як органів державної влади, так і бізнесу. Стабільність функціонування банківського сектору, критичної інфраструктури, підприємств, установ, організацій безпосередньо залежить від стабільності та безпеки кіберпростору з яким вони працюють.

В цілому можна зауважити, що в Україні розвиток електронної економіки зростає значними темпами. У Стратегії розвитку інформаційного суспільства в Україні схваленої розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р визначено термін електронна економіка як форма економічних

відносин у сфері виробництва, розподілу, обміну та споживання товарів, робіт і послуг, наданих в електронному вигляді за допомогою інформаційно-комунікаційних технологій (далі – е-економіка) (Розпорядження Кабінету Міністрів України, 2013).

Зворотньою стороною інформаційно-технологічного розвитку є збільшення кількості кіберзлочинів. Особливо проблема кіберзлочинності залишається актуальною під час дії воєнного стану в Україні.

Відповідно до Стратегії кібербезпеки України «Безпечний кіберпростір – Запорука успішного розвитку країни», затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021, кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами. Зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Посилюється тенденція щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, впливу на виборчі процеси (Указ Президента України, 2021).

Кіберзлочинці прагнуть використовувати вразливість людини чи безпеки, з метою безпосереднього вкрадення паролів, даних чи грошей. До найпоширеніших кіберзагроз відносяться:

– Злом (англ. "Hacking") – у тому числі соціальних мереж та паролів електронної пошти;

– Фішинг (англ. "Phishing") – підроблені електронні листи із запитом інформації про безпеку та особисті дані;

– Шкідливе програмне забезпечення (англ. "Malicious software") -, включаючи вимагачі (англ. "ransomware"), за допомогою яких злочинці захоплюють файли та утримують їх з метою отримання викупу.

– Розподілені атаки типу «відмова в обслуговуванні» (DDOS) проти веб-сайтів, які часто супроводжуються вимаганням (National Crime Agency).

Таким чином, з часу запровадження воєнного стану в Україні введеного Указом Президента України № 64/2022 у зв'язку з військовою агресією Російської Федерації проти України, були випадки невдалої спроби атаки хакерського угруповання Strontium, які намагалися отримати доступ до комп'ютерних мереж в Україні, США та ЄС, щоб забезпечити тактичну підтримку фізичного вторгнення росії в Україну та викрасти конфіденційну інформацію (Єрема, 2022).

Були повідомлення від Держспецзв'язку про отримання українськими користувачами нових небезпечних електронних листів з темою «№ 1275 від 07.04.2022». Листи містили HTML-файл, відкриття якого призводило до створення на комп'ютері архіву з файлом під назвою «Щодо фактів переслідування та вбивства працівників Прокуратури з боку російських військових на тимчасово окупованих територіях.lnk». Його відкриття, у свою чергу, призведило до можливості хакерів отримати повний контроль над комп'ютером користувача і загрожувало крадіжкою конфіденційної інформації, пошкодженням даних та комп'ютерних систем. Таку активність було асоційовано з діяльністю групи UAC-0010 (Armageddon), яка вже неодноразово здійснювала кібертаратаки як державні органи України, так і на країни ЄС (Державна служба спеціального зв'язку та захисту інформації України, 2022).

Держспецзв'язку попереджувало про розповсюдження електронних листів, що містять HTML-файл «Військові злочинці РФ.htm», відкриття якого призведить до створення на комп'ютері RAR-архіву "Viyskovi_zlochinci_RU.rar". Згаданий архів містить файл-ярлик «Військові-злочинці що знищують Україну (домашні адреси, фото, номера телефонів, сторінки у соціальних сетях).lnk». Його відкриття призведить до того, що зловмисники отримують віддалений доступ до комп'ютера жертви. Активність асоційовано з діяльністю групи UAC-0010 (Armageddon) (Державна служба спеціального зв'язку та захисту інформації України, 2022).

Під прицілом знаходяться також об'єкти критичної інфраструктури. Український провайдер Укртелеком зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагались проаналізувати, як влаштована IT-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії (Єрема, 2022).

Також урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, було виявлено RAR-архів «Диверсанти.rar», що містив RAR-архів «Диверсанти 21.03.rar». Він, у свою чергу, містив SFX-архів «Диверсанти filercs.rar» (для маскування розширення ім'я файлу містить right-to-left override (RTLO) символ). Згаданий архів містив документи та зображення приманки, а також VBScript-код (Thumbs.db), який забезпечував створення та запуск .NET-програми "dhdhk0k34.com". В результаті комп'ютер буде уражено шкідливою програмою Cobalt Strike Beacon (Державна служба спеціального зв'язку та захисту інформації України, 2022).

Відповідно до п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 р. № 2163-VIII кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України (Закон України, 2017). Варто зауважити, що чинне кримінальне законодавство України не містить поняття кіберзлочину. У Кримінальному кодексі України наявний розділ, який визначає відповідальність за кіберзлочини – Розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (Закон України, 2001), який

містить у собі шість статтей: 1) ст. 361 – несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 2) ст. 361-1 – створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; 3) ст. 361-2 – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; 4) ст. 362 – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; 5) ст. 363 – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; 6) ст. 363-1 – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Врахувуючи вищевикладене, підвищення ефективності боротьби з кіберзлочинністю є нагальною проблемою. Окрему увагу варто приділити прийнятому Закону України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24 березня 2022 р. (далі – «Закон № 2149-IX») (Закон України, 2022). Як зазначається у пояснювальній записці до проєкту документа, закон спрямований на посилення захисту критичної інфраструктури України від кібератак (Бізнес Цензор, 2022).

Мета нового Закону 2149-IX полягає у:

– посиленні спроможностей та оптимізації національної системи кібербезпеки для протидії кіберзагрозам;
– впровадженні дієвих кримінально-правових механізмів протидії кіберзлочинності;
– забезпеченні надійності та безпеки використання цифрових послуг (Єрема, 2022).

Відповідно до Закону України «Про електронні комунікації» й вимог іншого законодавства України у сфері кібербезпеки, термін «електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку» замінено на «інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі». Відповідні зміни також формалізовано у ст. 361 Кримінального кодексу України (Єрема, 2022).

Таким чином, стаття 361 ККУ зазнала змін серед яких можна виділити наступні:

1) термінологічних;

2) конструктивних – матеріальний склад змінено на формальний;

3) додано нові кваліфіковані юридичні склади:

– дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації (ч. 3 ст. 361 ККУ, новий кваліфікований склад, проте в попередній редакції диспозиція належала до опису основного складу).

– дії, передбачені частиною першою або другою цієї статті, якщо вони (…) створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків (ч. 4 ст. 361 ККУ).

– дії, передбачені частиною третьою або четвертою цієї статті, вчинені під час дії воєнного стану (ч. 5 ст. 361 ККУ).

Цікаво, що така ознака як вчинення злочину в умовах воєнного стану є кваліфікуючою лише щодо кваліфікованих складів (ч.ч. 3, 4 ст. 361 ККУ). Отже, вчинення діянь, передбачених ч. 1 або ч. 2 ст. 361 ККУ під час дії воєнного стану кваліфікації за ч. 5 цієї статті не підлягає, хоча це й буде розцінюватися як обставина, що обтяжує покарання відповідно до ст. 67 ККУ (Єрема, 2022).

Також внесеними до Кримінального кодексу України змінами було посилено відповідальність за несанкціоноване втручання у роботу електронних систем залежно від їхніх наслідків. Зокрема Законом № 2149-IX передбачено покарання за кіберзлочини вчинені саме під час воєнного стану – позбавлення волі на строк від десяти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років (Громадський простір, 2022).

Також Закон 2149-IX передбачає, що втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж не вважатиметься несанкціонованим, якщо таке втручання вчинено відповідно до Порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж, текст якого Держспецзв'язку зараз активно напрацьовує (Єрема, 2022).

Таким чином, в Україні відбулося узаконення процедури Bug Bounty. Дана процедура передбачає залучення за винагороду зовнішніх фахівців до пошуку помилок і вразливостей програмних продуктів, інформаційно-комунікаційних систем тощо, що дає можливість оперативно усувати всі недоліки та прогалини у безпеці (Юридична Газета online, 2022).

Вважаємо такі зміни позитивними. Зміни до Кримінального кодексу України є своєчасною відповіддю на безпекові виклики сучасності. Узаконення процедури Big Bounty спрятиме підвищенню ефективності кіберзахисту державних інформаційних систем, зокрема шляхом перевірки на наявність вразливостей.

Також не менш важливим є питання фінансової складової у боротьбі з кіберзлочинністю в Україні. Так, Постановою Кабінету Міністрів України від 1 липня 2022 р. № 751 було затверджено Порядок використання

коштів з рахунка Міністерства цифрової трансформації для забезпечення протидії інформаційним загрозам з боку держави-агресора, кіберзахисту, відновлення та розвитку цифрової інфраструктури держави (надалі – Порядок), що визначає механізм використання коштів для забезпечення протидії інформаційним загрозам з боку держави-агресора, кіберзахисту, відновлення та розвитку цифрової інфраструктури держави, що надійшли в національній та іноземній валюті від фізичних та юридичних осіб, резидентів і нерезидентів як благодійна пожертва, гуманітарна допомога, гранти та дарунки (надалі – кошти) на поточний рахунок Мінцифри, відкритий у Національному банку. Відповідно до Порядку кошти спрямовуються на посилення кіберзахисту держави, зокрема придбання та впровадження (розроблення, модернізацію) відповідних технічних та програмних засобів, організацію спеціальних навчань та міжнародної співпраці, придбання послуг у сфері захисту інформації (Постанова Кабінету Міністрів України, 2022).

Відкритим залишається питання щодо убезпечення від кіберзагроз не тільки публічного, але і приватного сектору. Варто зауважити, що враховуючи важливу роль приватного сектору в економічному розвитку країни, зокрема електронної економіки, вважаємо, що співробітництво публічного та приватного секторів у сфері протидії кіберзлочинності є основоположним фактором забезпечення кібербезпеки держави. Тому питання публічно-приватного партнерства у сфері протидії кіберзлочинності та забезпечення кібербезпеки є як ніколи нагальним.

Згідно спільної публікації публікацією Світового банку та ООН "Combating Cybercrime: Tools and Capacity Building for Emerging Economies" від 2017 р. (надалі – «Публікація») публічно-приватне партнерство створюються або неформально, через казуальні угоди або домовленості, або формально, шляхом встановлення юридичних угод. Співпраця спрямована на полегшення обміну інформацією про загрози та тенденції, а також на запобігання конкретній діяльності та діям. Такі дії доповнюють дії правоохоронних органів та можуть допомогти зменшити збитки, завдані жертвам (The World Bank, 2017: 251).

Академічні установи відіграють різні ролі у запобіганні кіберзлочинності, у тому числі шляхом надання освіти та навчання фахівців, розробки законодавства та політики, а також роботи над технічними стандартами та розробкою рішень. Університети розміщують та допомагають експертам з кіберзлочинності, навіть розміщуючи групи CIRT (групи реагування на комп'ютерні інциденти) та інші спеціалізовані дослідницькі центри (The World Bank, 2017: 251).

Групи CIRT відіграють важливу роль у нарощуванні потенціалу за допомогою проведення заходів та обміну інформацією, дуже часто технічно. Вони також полегшують взаємодію з місцевою поліцією для виявлення кіберзлочинців, пропонують важливу підтримку приватному сектору для підтримки та координації з іншими групами CIRT для обміну технічними даними та технічними знаннями в режимі реального часу для відстеження кіберзлочинів (The World Bank, 2017: 251–252).

Також варто відмітити важливість співпраці між науково-освітніми установами та державними органами у сфері забезпечення кібербезпеки. Оскільки вважаємо, що ефективна підготовка фахівців з кібербезпеки є одним із ключових завдань держави у сфері протидії кіберзагрозам. Так, у 2012 році Національний університет Філіппін (англ. "The National University of the Philippines") та Міністерство юстиції США (англ. "U. S. Department of Justice") підписали угоду про публічно-приватне партнерство для підготовки експертів з кіберзлочинності у рамках першого у Південно-Східній Азії чотирирічного курсу цифрової криміналістики. Курс – ступінь бакалавра наук у галузі комп'ютерних досліджень зі спеціалізацією в галузі цифрової криміналістики (англ. "Bachelor of Science in Computer Studies, Major in Digital Forensics") – призначений для підготовки фахівців у спеціалізованій галузі, особливо у сфері пошуку доказів із жорстких дисків комп'ютерів, мобільних телефонів та інших пристроїв ІКТ. Довгострокове публічно-приватне партнерство призначене для забезпечення інституційного нарощування потенціалу та забезпечення спільного використання ресурсів для вирішення глобальної проблеми кіберзлочинності шляхом мобілізації наступних поколінь (The World Bank, 2017: 253).

Також у Публікації зазначено, що координація кібербезпеки дуже часто носить епізодичний чи бюрократичний характер. У всіх ініціативах необхідно впровадити дієву культуру обміну інформацією та координації. Необхідно створити відповідні інститути для реалізації цих культурних зрушень, оскільки багато приватних суб'єктів досі не знають чи, коли і як буде корисна (або шкідлива) взаємодія з урядом з цих питань (The World Bank, 2017: 254–255).

Вважаємо, що в Україні необхідно створити чіткі законодавчі та організаційні механізми для функціонування злагодженої координації зусиль відповідних державних органів, приватного сектору та науково-освітніх закладів. Зокрема, одним з таких напрямків може бути створення створення в національних вищих навчальних закладах кібер-лабораторій, де студенти мали б можливість здобувати практичні знання, переймати досвід та проводити сумісні дослідження з фахівцями як публічного, так і приватного сектору.

Висновки. Отже, вважаємо позитивними зміни у вітчизняне законодавство щодо протидії кіберзлочинам, зокрема зміни закріплені у прийнятому Закону України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24 березня 2022 р., що є об'єктивною необхідністю в умовах дії воєнного стану в Україні. Проте, вважаємо за необхідне закріпити у Кримінальному кодексі України визначення поняття «кіберзлочин». Такі зміни сприятимуть формуванню єдиних підходів до протидії кіберзлочинності.

Також, вважаємо доцільними узаконення в Україні процедури Bug Bounty. Дана процедура спрятиме підвищенню ефективності кіберзахисту державних інформаційних систем, зокрема шляхом перевірки на наявність вразливостей.

Також вважаємо, що одним із ключових питань у протидії кіберзлочинності особливо в умовах воєнного стану є консолідація зусиль публічного та приватного секторів. Вважаємо за необхідне поглиблювати співпрацю між публічним та приватним секторами у сфері кібербезпеки та створювати законодавчі та організаційні можливості для трьохсторонньої співпраці у даному напрямку між публічним та приватним секторами та науково-освітіми навчальними закладами. Одним з таких напрямків може бути створення створення в національних вищих навчальних закладах кібер-лабораторій.

Список використаних джерел:

1. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-р#Text (дата звернення: 01.07.2022).
2. Про Стратегію кібербезпеки України : Рішення Ради національної безпеки і оборони України від 14 травня 2021 року. Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 02.07.2022).
3. Cyber crime. National Criminal Agency. URL: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime (дата звернення: 03.07.2022).
4. Єрема Микола. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. ЮРЛІГА : веб-сайт. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 04.07.2022).
5. Увага! Нова кібератака групи Armageddon на державні органи України. Сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-grupi-armageddon-na-derzhavni-organi-ukrayini (дата звернення: 05.07.2022).
6. Увага! Нова кібератака на державні органи України. Сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-na-derzhavni-organi-ukrayini (дата звернення: 06.07.2022).
7. Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon. Сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/kiberataka-na-derzhavni-organizaciyi-ukrayini-z-vikoristannyam-shkidlivoyi-programi-cobalt-strike-beacon (дата звернення: 07.07.2022).
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. N 2163-VIII. База даних «Законодавство України». ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.07.2022).
9. Кримінальний кодекс України. Кодекс. Закон України № 2341-III 05 квітня 2001 р. База даних «Законодавство України». ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 15.07.2022).
10. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України № 2149-IX від 24 березня 2022 р. База даних «Законодавство України». ВР України. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 17.07.2022).
11. Рада посилила покарання за кіберзлочини в умовах воєнного стану. Бізнес Цензор : веб-сайт. URL: https://biz.censor.net/news/3328358/rada_posylyla_pokarannya_za_kiberzlochyny_v_umovah_voyennogo_stanu (дата звернення: 18.07.2022).
12. Особливості боротьби з кіберзлочинністю в умовах воєнного стану. Громадський простір : веб-сайт. URL: https://www.prostir.ua/?news=osoblyvosti-borotby-z-kiberzlochynistyu-v-umovah-vojennoho-stanu (дата звернення: 20.07.2022).
13. В Україні узаконили Bug Bounty: що це і як допоможе? Юридична газета : веб-сайт. URL: https://yur-gazeta.com/golovna/v-ukrayini-uzakonili-bug-bounty-shcho-ce-i-yak-dopomozhe.html (дата звернення: 22.07.2022).
14. Порядок використання коштів з рахунка Міністерства цифрової трансформації для забезпечення протидії інформаційним загрозам з боку держави-агресора, кіберзахисту, відновлення та розвитку цифрової інфраструктури держави : Постанова Кабінету Міністрів України від 1 липня 2022 р. № 751. URL: https://zakon.rada.gov.ua/laws/show/751-2022-п#Text (дата звернення: 22.07.2022).
15. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf (дата звернення: 22.07.2022).

References:

1. Pro skhvalennya Stratehiyi rozvytku informatsiynoho suspil'stva v Ukrayini : Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 15 travnya 2013 r. № 386-r [On the approval of the Information Society Development Strategy in Ukraine : Decree of the Cabinet of Ministers of Ukraine dated May 15, 2013 No. 386-r]. Retrieved from: https://zakon.rada.gov.ua/laws/show/386-2013-p#Text [in Ukrainian]
2. Pro Stratehiyu kiberbezpeky Ukrayiny : Rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku. Ukaz Prezydenta Ukrayiny vid 26 serpnya 2021 roku № 447/2021. [On Cyber Security Strategy of Ukraine : Decision of the National Security and Defense Council of Ukraine dated May 14, 2021. Decree of the President of Ukraine dated August 26, 2021 No. 447/2021]. Retrieved from: https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian]
3. Cyber crime. National Criminal Agency. Retrieved from: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime [in English]

4. Yerema Mykola. Borot'ba z kiberzlochynnistyu v umovakh diyi voyennoho stanu : Zakon 2149-IX. [Combating cybercrime under martial law : Law 2149-IX]. YURLIHA : veb-sayt. Retrieved from: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix [in Ukrainian]
5. Uvaha! Nova kiberataka hrupy Armageddon na derzhavni orhany Ukrayiny. [Attention! Armageddon group's new cyber attack on Ukrainian state bodies]. Sayt Derzhavnoyi sluzhby spetsial'noho zv'yazku ta zakhystu informatsiyi Ukrayiny. Retrieved from: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-grupi-armageddon-na-derzhavni-organi-ukrayini [in Ukrainian]
6. Uvaha! Nova kiberataka na derzhavni orhany Ukrayiny. [Attention! New cyber attack on state bodies of Ukraine]. Sayt Derzhavnoyi sluzhby spetsial'noho zv'yazku ta zakhystu informatsiyi Ukrayiny. Retrieved from: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-na-derzhavni-organi-ukrayini [in Ukrainian]
7. Kiberataka na derzhavni orhanizatsiyi Ukrayiny z vykorystannyam shkidlyvoyi prohramy Cobalt Strike Beacon. [A cyber attack on state organizations of Ukraine using the Cobalt Strike Beacon malware]. Sayt Derzhavnoyi sluzhby spetsial'noho zv'yazku ta zakhystu informatsiyi Ukrayiny. Retrieved from: https://cip.gov.ua/ua/news/kiberataka-na-derzhavni-organizaciyi-ukrayini-z-vikoristannyam-shkidlivoyi-programi-cobalt-strike-beacon [in Ukrainian]
8. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny : Zakon Ukrayiny vid 05 zhovtnya 2017 r. N 2163-VIII. [On the main principles of ensuring cyber security of Ukraine : Law of Ukraine dated October 5, 2017 No. 2163-VIII]. Baza danykh "Zakonodavstvo Ukrayiny". VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian]
9. Kryminal'nyy kodeks Ukrayiny. Kodeks. Zakon Ukrayiny N 2341-III 05 kvitnya 2001 r. [Criminal code of Ukraine. Code. Law of Ukraine No. 2341-III April 5, 2001]. Baza danykh "Zakonodavstvo Ukrayiny". VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/2341-14#Text [in Ukrainian]
10. Pro vnesennya zmin do Kryminal'noho kodeksu Ukrayiny shchodo pidvyshchennya efektyvnosti borot'by z kiberzlochynnistyu v umovakh diyi voyennoho stanu : Zakon Ukrayiny № 2149-IX vid 24 bereznya 2022 r. [On making changes to the Criminal Code of Ukraine to improve the effectiveness of the fight against cybercrime under martial law : Law of Ukraine No. 2149-IX dated March 24, 2022]. Baza danykh "Zakonodavstvo Ukrayiny". VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/2149-20#Text [in Ukrainian]
11. Rada posylyla pokarannya za kiberzlochyny v umovakh voyennoho stanu. [The Council has increased penalties for cybercrimes under martial law]. Biznes Tsenzor : veb-sayt. Retrieved from: https://biz.censor.net/news/3328358/rada_posylyla_pokarannya_za_kiberzlochyny_v_umovah_voyennogo_stanu [in Ukrainian]
12. Osoblyvosti borot'by z kiberzlochynistyu v umovakh voyennoho stanu. [Peculiarities of combating cybercrime under martial law]. Hromads'kyy prostir : veb-sayt. Retrieved from: https://www.prostir.ua/?news=osoblyvosti-borotby-z-kiberzlochynistyu-v-umovah-vojennoho-stanu [in Ukrainian]
13. V Ukrayini uzakonyly Bug Bounty: shcho tse i yak dopomozhe? [Bug Bounty has been legalized in Ukraine: what is it and how will it help?]. Yurydychna hazeta : veb-sayt. Retrieved from: https://yur-gazeta.com/golovna/v-ukrayini-uzakonili-bug-bounty-shcho-ce-i-yak-dopomozhe.html [in Ukrainian]
14. Poryadok vykorystannya koshtiv z rakhunka Ministerstva tsyfrovoyi transformatsiyi dlya zabezpechennya protydiyi informatsiynym zahrozam z boku derzhavy-ahresora, kiberzakhystu, vidnovlennya ta rozvytku tsyfrovoyi infrastruktury derzhavy : Postanova Kabinetu Ministriv Ukrayiny vid 1 lypnya 2022 r. № 751. [The procedure for using funds from the account of the Ministry of Digital Transformation to ensure counteraction to information threats from the aggressor state, cyber protection, restoration and development of the state's digital infrastructure : Decree of the Cabinet of Ministers of Ukraine of July 1, 2022 No. 751]. Retrieved from: https://zakon.rada.gov.ua/laws/show/751-2022-п#Text [in Ukrainian]
15. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf [in English]