Черниш Р. Ф.,
кандидат юридичних наук, доцент,
Національна академія Служби безпеки України
ORCID ID: *0000–0003–4176–7569*

DOI: *https://doi.org/10.17721/2413-5372.2021.3-4/112-121*

УДК 342.951

МІЖНАРОДНИЙ ОРГАНІЗАЦІЙНИЙ ДОСВІД У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

«Хто володіє інформацією – той володіє світом!»
Натан Ротшильд

Анотація. *У статті констатовано, що протягом останніх років глобальний кіберпростір більш предметно оцінюється світовою спільнотою як один із найважливіших безпекових пріоритетів, оскільки його функціонування є суттєвим чинником розвитку економіки, військового, соціального, безпекового та інших секторів. Загроза злому інтернет-систем із злочинним умислом або в інтересах спеціальних служб іноземних держав знаходиться на одному рівні з тероризмом, шпигунством і застосуванням зброї масового ураження. Враховуючи недостатній досвід протидії вказаним негативним явищам спеціальними суб'єктами, допомога іноземних партнерів та використання їх різнопланових напрацювань за цим напрямом вбачається актуальним.*

Зважаючи на викладене, ***метою статті*** *є аналіз організаційної діяльності окремих спеціальних суб'єктів іноземних держав у сфері забезпечення кібербезпеки.*

Стверджується, що спеціальними службами РФ цілеспрямовано здійснюються кампанії з кібератак в США та країнах ЄС. Вказані виклики обумовили формування т.зв. кібервійськ. Аналізуючи відкриті джерела інформації, можна дійти висновку, що на офіційному рівні їх існування визнано лише частиною країн у світі (США, Ірак, Великобританія, РФ тощо), однак реально вони функціонують майже в кожній розвиненій державі.

Зазначається, що наразі Україна на системній основі організовує співпрацю з міжнародними партнерами, а одним із першочергових кроків повинна стати розробка національного законодавства з урахуванням положень оновленої стратегії Європейського союзу у сфері кібербезпеки за умов цифрової модернізації.

Одним із першочергових завдань у вказаній сфері також є формування дієвого механізму забезпечення безпеки інформаційного простору з урахуванням відповідного передового міжнародного досвіду. У значній мірі це стосується нашої держави з огляду на євроінтеграційні сподівання, необхідність впровадження ефективних механізмів розвитку економіки, сучасних інформаційних технологій тощо та перебування держави у стані «неоголошеної війни» з боку РФ.

Ключові слова: *кібербезпека, забезпечення кібербезпеки, кібервійська, кіберпростір, мережа Інтернет.*

Постановка проблеми. Розгляд результатів діяльності та статистичних даних що стосуються функціонування спеціальних служб і правоохоронних органів низки країн світу дозволяє дійти висновку, що в умовах сьогодення жодна держава не здатна самостійно ефективно протидіяти кібератакам, організувати ефективне забезпечення кібезбезпеки.

Протягом останніх років проблематика забезпечення безпеки глобального

кіберпростору більш предметно оцінюється світовою спільнотою як один із найбільш важливих безпекових пріоритетів, адже його функціонування є суттєвим чинником розвитку економіки, військового, соціального, безпекового[1] та інших секторів. Загроза злому інтернет-систем із злочинним умислом або в інтересах спеціальних служб іноземних держав знаходиться на одному рівні з тероризмом, шпигунством і застосуванням зброї масового ураження. Враховуючи недостатній досвід протидії вказаним негативним явищам спеціальними суб'єктами, допомога іноземних партнерів та використання їх різнопланових напрацювань за цим напрямом вбачається актуальним.

Аналіз останніх досліджень і публікацій. Проблематика функціонування т.зв. кібервійськ та міжнародної співпраці у сфері забезпечення кібербезпеки досліджувалася такими науковцями і практиками як: В. Горбулін, О. Довгань, І. Доронін, Я. Жарков, Т. Жовтенко, Л. Компанцева, В. Ліпкан, А. Марущак, В. Остоухов, В. Пилипчук, М. Погорецький, В. Полевий, Т. Ткачук, В. Цимбалюк та інші. Проте, зважаючи на актуальність окресленого питання, потребує подальшого вивчення й узагальнення. Тому, **метою статті є** аналіз організаційної діяльності окремих спеціальних суб'єктів іноземних держав у сфері забезпечення кібербезпеки.

Виклад матеріалу дослідження та його основні результати. Починаючи з 2000-х років, спеціальними службами РФ цілеспрямовано здійснюються кампанії з кібератак в США та країнах ЄС. Під час виступу в Сент-Ендрюському університеті Шотландії екс-міністр оборони Великобританії М. Феллон звинуватив Російську Федерацію у кібератаках, перетворенні «дезінформації у зброю», «регулярній брехні» та втручанні у перебіг вільного волевиявлення громадян (парламентські вибори у Чорногорії в жовтні 2016р., референдум в Нідерландах про асоціацію з ЄС і Україні в квітні 2016 р. тощо). Зокрема, політик відзначив: «росія явно випробовує НАТО і Захід. Вона прагне розширити сферу свого впливу, дестабілізувати країни і послабити Північноатлантичний Альянс. Це підриває національну безпеку цілого ряду союзників і міжнародну систему, засновану на правилах. У зв'язку з цим, у наших інтересах і в інтересах Європи зберегти сильні позиції НАТО, стримати Росію і відрадити її від прямування цих курсом»[2].

К. Мартін (голова Національного центру кібербезпеки Великої Британії, NCSC), заявив, що російські хакери, скоріш за все, причетні до частини атак на заклади урядового рівня. Крім цього, керівник центру кібербезпеки Англії вважає, що хакери з РФ можуть викрасти нові дослідження англійських вчених та їх персональні дані, закриту інформацію про зовнішню політику і оборону країни[3]. На думку Генерального директора британської розвідслужби MI5 Е. Паркера, Росія є зростаючою загрозою для стабільності Великобританії і використовує всі сучасні засоби, наявні в її розпорядженні, для досягнення своїх цілей, в тому числі і кібератаки[4].

Вказані виклики обумовили формування та функціонування т.зв. кібервійськ. Аналізуючи відкриті джерела інформації, можна дійти висновку, що на офіційному рівні їх існування визнано лише частиною країн у світі (США, Ірак, Великобританія, РФ тощо), однак реаль-

[1] М Погорецький, В Шеломенцев, Поняття кіберпростору як середовища вчинення злочинів (2009) 2 *Інформаційна безпека людини, суспільства, держави* 77–81.

[2] Міноборони Британії звинуватило РФ у кібератаках <http://ua.korrespondent.net/world/3809809-minoborony-brytanii-zvynuvatylo-rf-u-kiberatakakhc> дата звернення 21.09.2021.

[3] Британия предупредила об ответных мерах в случае хакерских атак <https://www.rbc.ua/rus/news/britaniya-predupredila-otvetnyh-merah-sluchae-1478018271.html> дата звернення 21.09.2021.

[4] Великобритания потратит 1,9 млрд фунтов стерлингов (2,1 млрд евро) на усиление кибербезопасности в стране в течение ближайших пяти лет <https://www.ukrinform.ru/rubric-world/2112238-britania-gotovit-na-kiberbezopasnost-21-milliarda.html> дата звернення 21.09.2021.

но вони функціонують майже в кожній розвиненій державі.

Відповідно до рейтингу Global Cybersecurity Index найпотужніші кібервійська функціонують у США, Британії, Китаю, Кореї, Естонії та низці інших потужних держав світу[1].

У США основним органом, який централізовано здійснює операції в рамках кібернетичної війни, управління та захист військових комп'ютерних мереж є Кібернетичне командування (United States Cyber Command, USCYBERCOM). Його підрозділи володіють силами та засобами для проведення кібератак, вони «застосовуються на практиці протидії будь-якій IT-інфраструктурі, з якої, на їх думку, виходять загрози». З 2018 року USCYBERCOM надали право проводити проактивні хакерські атаки з метою запобігання кібернападам, що готуються. До того часу відомство дотримувалося, в основному, оборонної позиції, стримуючи кібератаки на американські мережі. Загальна кількість кіберсолдатів у США налічує шість тисяч, за іншими даними вона досягає 9 тисяч.

Окрім USCYBERCOM, потужні кібернетичні підрозділи є в ФБР та АНБ (Агенція національної безпеки). Наприклад, після однієї з атак на нафтопровід Colonial Pipeline, ФБР змогла знищити кілька хакерських груп і відкликати більшу частину сплаченої за здирництво суми. Кілька людей при цьому було заарештовано.

Управління повітряної розвідки США розробило концепцію «інформаційного панування». Ідея завоювання інформаційної переваги над супротивником шляхом здійснення деструктивних інформаційних впливів послідовно втілювалася в документах Міністерства оборони США «Чотирирічний огляд оборонної політики», а також «Єдині перспективи 2010» і «Єдині перспективи 2020»[2]. Вказані документи визначають мету, завдання й основні принципи інформаційного протиборства, обов'язки керівних органів і посадових осіб щодо організації та планування здійснення деструктивних інформаційних впливів у мирний час і в кризовій обстановці. В рамках цієї концепції, що передбачає широке використання наявного перспективного технологічного заділу й методів моделювання, під «інформаційним пануванням» розуміється можливість «випереджального» одержання необхідних відомостей і даних про тактичну або стратегічну ситуацію, що дозволяє ухвалювати своєчасні рішення з нейтралізації й стримування дій супротивника відповідно до стратегії «кризового реагування». Провідне місце, яке інформаційні системи займають в обґрунтуванні й вирішення завдань зазначеної стратегії, на сучасному етапі визначається такими особливостями:

– розвиток інформаційних систем (на відміну від подальшого нарощування озброєнь) не викликає гострої негативної реакції в широких колах американської громадськості;

– розвиток таких систем є певною мірою «безпрограшним», оскільки інформаційні військові системи можуть використовуватися й у мирних цілях. Зокрема, у США засоби космічного спостереження передбачається використовувати в комерційних цілях, для екологічного моніторингу, при боротьбі з міжнародним тероризмом і наркобізнесом;

– домінуючий статус США в розвитку засобів розвідки, зв'язку й управління закріплює їх монополію на володіння військовою, економічною, політичною інформацією, необхідною для досягнення стратегічної раптовості у випадку наростання міжнародної напруженості [175, с. 81–88].

У цілому, події кінця XX–початку XXI століття засвідчили актуальність і нагальну необхідність врахування ін-

[1] Global Cybersecurity Index <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> дата звернення 21.09.2021.

[2] Чотирирічний огляд оборони <https://history.defense.gov/Historical-Sources/Quadrennial-Defense-Review/> дата звернення 21.09.2021.

формаційного аспекту політики національної безпеки. Зокрема, після подій вересня 2001 року, Сполучені Штати Америки, розпочали активну міжнародну військово-політичну кампанію з протидії міжнародному тероризму. З перших днів її провадження виникла необхідність її ефективного інформаційного забезпечення. Однак розуміння такої необхідності сформувалося в практиці державної політики США задовго до цього – ще під час В'єтнамської війни. Явні прорахунки американського командування у роботі з журналістами довели, як зазначає у своїй книзі «Війна у В'єтнамі» екс-начальник розвідувального відділу штабу американського командування у В'єтнамі Ф. Девідсон, що «війну в Індокитаї можна було виграти на території Сполучених Штатів»[1].

У Великобританії кібервійська почали формуватися ще під час Другої світової війни. Зокрема, відомий розвідувальний центр в Блечлі-Парк у 1941–1945 роках регулярно декодував секретні повідомлення Німеччини та Італії (німецькі шифри «Енігми» та машини Лоренца).

Перші сучасні кіберпідрозділи у вказаній країні було сформовано на початку 2000-х, а в 2010-х британці провели декілька успішних кібероперацій з протидії ісламістським терористам у Сирії та Іраку, завдавши потужного удару їх пропагандистській мережі та неофіційним каналам фінансування.

У цілому, Уряд Британії системно виділяє значні суми коштів на реалізацію стратегії кібербезпеки. Зокрема, на розвиток системи автоматичного захисту сайтів від хакерських атак і спроб несанкціонованого доступу до ресурсів офіційних доменів, посилення заходів по перехопленню електронних листів-пасток, а також на закриття сайтів, за допомогою яких хакери отримують доступ до банківських рахунків інтернет-користувачів тощо.

У Великій Британії проблемами інформаційної боротьби займається департамент урядових комунікацій (The Government Communications Headquarters). Під інформаційною боротьбою у цій країні розуміється цілеспрямована реалізація комплексу заходів щодо дезорганізації і встановлення контролю над системою державного та воєнного управління противника шляхом інформаційнотехнічного й інформаційно-психологічного впливу на його інформаційні ресурси, на суспільну та індивідуальну свідомість. Питаннями проведення інформаційних операцій у військовому відомстві займається група з координації військових інформаційних операцій, яка підпорядкована міністрові оборони.

У свій час, екс-прем'єр-міністр Д. Кемерон зазначив, що за останні два роки Великобританія перетворилася в найбільш швидко зростаючу сучасну економіку світу, що дозволило, з урахуванням зростаючих загроз з боку ІГІЛ, нестабільності на Близькому Сході, кризи на Україні, збільшення кількості кібератак і ризиків пандемій, здійснити додаткові інвестиції у власну національну безпеку»[2].

На особливу увагу, на нашу думку, заслуговують думки політиків про те, що «підвищенні вартості здійснення атаки проти будь-якого громадянина Великобританії буде досягатися, в тому числі, й за рахунок підвищення рівня кібернавиків. Кібербезпека – це вже не просто проблема ІТ-відділу, а й всієї робочої сили. Кібернавики повинні стати частиною кожної професії»»[3].

З цією метою у Великій Британії реалізується ряд програм із залучення громадськості до забезпечення безпе-

[1] Т Жовтенко Інформаційна війна: сучасний вимір <http://ua.112.ua/analityka/informaciyna-viyna-suchasniy-vimir-52988.html> дата звернення 21.09.2021.

[2] Р Черниш, Залучення громадськості до забезпечення кібербезпеки держави (за прикладом Великобританії) (2017) *Наукові читання* 198–202.

[3] Правительство Великобритании потратит $2,3 млрд на укрепление кибербезопасности. <http://www.securitylab.ru/blog/personal/tsarev/321169.php> дата звернення 21.09.2021.

ки інформаційного простору держави (насамперед учнівської та студентської молоді). Зокрема, Центром урядового зв'язку (GCHQ, веде радіоелектронну розвідку і забезпечує захист інформації органів уряду і армії) ініційовано програму із залучення тінейджерів у сферу кібербезпеки. Зокрема, дівчатка у віці від 13 до 15 років, які проводять багато часу в інтернеті, беруть участь у тестах на логіку і кодування, створення мереж і криптографію. Це пов'язане з тим, що на сьогодні жінки, як відзначають представники спецслужби, складають лише 10% від загального числа співробітників служб кібербезпеки по всьому світу. Змагання є частиною національної стратегії кібербезпеки. Їх організацією займається Національний центр з кібербезпеки (NCSC). Об'єднавшись у команди по 4 особи, юні учасниці змагання виконуватимуть завдання в дистанційному режимі на своїх шкільних комп'ютерах. З кожним новим етапом труднощі завдань зростатимуть. За словами представника NCSC: «жінки можуть і вже вносять величезний вклад у справу кібербезпеки, це змагання може надихнути багатьох зробити перші кроки в цій динамічній і гідної кар'єрі. Я працюю разом з деякими воістину талановитими жінками, які допомагають захищати Велику Британію від різноманітних онлайн-загроз»[1].

З метою пошуку потенційних експертів для захисту держави від хакерських атак, у школах Англії дітям пропонують відвідувати заняття з кібербезпеки. Уряд країни заявив, що таким чином має намір уже нині працювати над проблемами кібербезпеки в майбутньому.

На проект, розрахований на п'ять років, буде витрачено близько 25 мільйонів доларів. Надалі планується найперспективнішим студентам виділяти університетські гранти і забезпечувати їх роботою в цій галузі[2].

Іншим кроком у сфері формування інформаційної безпеки Великобританії є залучення для забезпечення кібербезпеки держави молоді з великим досвідом відеоігор.

Учасники програми, які успішно пройдуть відбір в урядові розвідувальні агентства, прослуховують основний дворічний курс з комунікацій, безпеки і проектування в університеті De Montfort. Вони стануть фахівцями в IT, програмному забезпеченні і телекомунікації. Закінчивши навчання, отримають професійні навички, необхідні для роботи в Центрі урядового зв'язку (GCHQ), а також у розвідувальних і оборонних службах MI5 і MI6 [258].

Значна увага також приділяється проведенню активної роз'яснювальної роботи серед населення щодо небезпек кіберзагроз. Зокрема, у Великій Британії спільно з Європейськими, американськими і канадськими партнерами було проведено захід під назвою GetSafeOnlineWeek для підвищення розуміння загроз кібербезпеки серед населення[3].

Офіційно армія кіберсолдатів в Китаї була створена 1 січня 2016 року. Вона оцінюється як найчисленніша в світі і налічує до 20 тисяч осіб. Фінансування вказаного роду військ досягає 1,5 млрд дол. на рік.

Китайські хакери займаються в основному кібершпіонажем, перехопленням дипломатичної пошти, промисловим шпигунством тощо. При цьому китайські кібератенти атакують мало не всі країни світу.

У 2016 році китайська група кібершпигунів зламала значну кількість індійських веб-ресурсів. До них потрапили матеріали систем центрального уряду

[1] Британская разведка ищет кибер-агентов среди девочек-подростков <http://ru.delfi.lt/abroad/global/britanskaya-razvedka-ischet-kiber-agentov-sredi-devochek-podrostkov.d?id=73490964> дата звернення 21.09.2021.

[2] У школах Англії введуть заняття з кібербезпеки <https://bdzhola.com/news/u-shkolah-angliji-vvedut-zanjattja-z-kiberbezpeki> дата звернення 21.09.2021.

[3] Get Safe Online week <http://www.cabinetoffice.gov.uk/news/get-safe-online-week> дата звернення 21.09.2021.

та провідних фінансових інституцій. Для своїх атак вони використовували понад 50 різновидів шкідливого програмного забезпечення. В більшості випадків їм вдалося викрасти конфіденційну інформацію.

Для китайських хакерів характерні так звані килимові атаки: вони атакують усе підряд, викачують усю наявну інформацію, а потім аналізують, чи є там щось цінне для них. Для виконання такої роботи задіяні величезні ресурси – сотні чи навіть тисячі людей.

Водночас, згідно з багатьма рейтингами, в топ-5 країн за чисельністю кіберагентів входить Південна Корея – кількість хакерів досягає 700, а річний бюджет становить 400 млн дол. Але в цій країні кібервійська виконують лише оборонну функцію.

У Німеччині створений і активно функціонує Центр безпеки інформаційної техніки (штат 500 співробітників, річний бюджет 50 млн євро). За результатами його діяльності передбачається ведення наступальних і оборонних операцій інформаційної війни для досягнення національних цілей. Німецькі аналітики розглядають управління засобами масової інформації як дієвий елемент інформаційної війни. Крім того, вони окремо розглядають економічну інформаційну війну[1].

У 2007 році Естонія, що є однією з найбільш розвинутих кібердержав у світі, зазнала масованої атаки з боку російських хакерів. Більшість цифрових сервісів, сайти парламенту, банків та ЗМІ були на деякий час недоступні. Після того влада Естонія зробила кілька потужних кроків для посилення своєї кібербезпеки. У 2008 році тут відкрили Об'єднаний центр передових технологій з кібероборони НАТО.

Крім того, в 2018 році в армії Естонії створили новий підрозділ, який має опікуватися кібербезпекою країни. Уряд також анонсував ініціативу створення волонтерського підрозділу з кібербезпеки. Планується, що волонтери з хорошим рівнем знань в галузі ІТ будуть захищати естонський кіберпростір у час, вільний від роботи.

За останні роки ізраїльська армія зробила чимало для «диджиталізації» своїх сухопутних військ. Але це підвищило загрозу того, що під час війни противник спробує порушити роботу військової мережі. Основну загрозу Ізраїль вбачає з боку Ірану. Саме тому країна створила елітний підрозділ кіберагентів для ведення національної кібервійни.

У 2018 році армія прийняла на службу близько 300 молодих комп'ютерних фахівців. Ці солдати будуть служити у підрозділі військової розвідки, а також в Управлінні командування, підрозділах зв'язку та розвідки.

Водночас Ізраїль вперше в історії показав, що на атаки у віртуальному світі можна відбити реальним бомбардуванням. Зокрема, в травні 2019 року авіація Ізраїлю завдала швидкого авіаудару по будівлі в секторі Газа. За даними розвідки саме звідти проводилася кібератака.

5 березня 2020 року Литва очолила формування в Євросоюзі сил швидкого реагування на кібератаки. До того часу Литва лише координувала ці сили. Представники відповідних держорганів Литви, Нідерландів, Польщі, Румунії, Хорватії та Естонії підписали про це меморандум.

Міжнародна команда з реагування на кібератаки складається з військових і цивільних осіб, які будуть чергувати у своїх країнах і підключатися до протидії інцидентам у віртуальному просторі.

«Створені цивільними та військовими експертами, ці групи реагування дозволять нейтралізувати та розслідувати небезпечні кіберінциденти. Зміцнивши національний кіберпотенціал, Литва створює основу для міжнародного співробітництва, яке допоможе протистояти

[1] Історія інформаційно-психологічного протиборства: підручник (Київ, Наук. – вид. відділ НА СБ України, 2012) 212.

кіберзагрозам, обмінюватися важливими знаннями та проводити спільні навчання», прокоментували у Міністерстві оборони Литви[1].

Німецька модель забезпечення інформаційної безпеки держави діє на підставі Конституції ФРН, федеральних законів і законів земель, рішень конституційних судів, наднаціонального законодавства та відповідних підзаконних нормативно-правових актів.

Зокрема, відповідно до параграфа 1 статті 5 Конституції ФРН, кожен має право на свободу вираження і поширювання своєї думки усно, письмово і за допомогою образотворчих засобів, безперешкодно отримувати інформацію з усіх загальнодоступних джерел. Гарантується свобода друку і свобода передавання інформації за допомогою радіо і кіно. Цензура не здійснюється.

У 2009 році Конституцію ФРН було доповнено статтею 91c, яка заклала основу для співпраці федерального уряду та урядів земель у сфері інформаційних технологій. Це положення є широким з урахуванням постійного прогресу інформаційних технологій і його зростаючого значення для державного управління. Воно включає в себе фактичні та юридичні аспекти такої співпраці, закріплює можливість узгодження стандартів для їх одноманітного застосування для забезпечення сумісності і вимог безпеки при обміні даними.

Базовим законом у сфері інформаційної безпеки Німеччини є Закон «Про посилення безпеки систем інформаційних технологій» (Закон про безпеку IT) від липня 2015 року. Закон відводить Федеральному відомству з безпеки у сфері інформаційних технологій (нім. BSI) центральну роль у захисті критично важливих інфраструктур у Німеччині. При цьому під критичними інфраструктурами розуміють об'єкти, установи або їх частини, які належать до секторів енергетики, інформаційних технологій і телекомунікацій, транспорту і дорожнього руху, охорони здоров'я, водопостачання, харчування, фінансів і страхування. Такі об'єкти мають суттєве значення для спільноти, тому що їх зупинка або погіршення роботи призведе до значного дефіциту поставок або створить загрози для громадської безпеки.

У січні 2016 року в Німеччині оголосили про створення кібервійськ. До цього часу за кібероборону у Німеччині відповідало міністерство внутрішніх справ. Новий підрозділ розмістили в місті Бонн. Вказаний рід військ забезпечить безпеку інформаційних систем збройних сил Німеччини, а також буде захищати від злому ті види озброєнь, де застосовуються цифрові технології. Бюджет підрозділу становить 250 млн дол. на рік.

За даними аналітиків, щодня на мережі ФРН відбувається від 2,5 до 6,5 тисяч кібератак. Кібероборону вважають стратегічним напрямком для забезпечення безперешкодного функціонуванні країни.

З огляду на викладене, Україна на системній основі організовує співпрацю з міжнародними партнерами щодо захисту національного суверенітету у різних сферах суспільного життя. В рамках першого раунду Кібердіалогу Україна – Європейський Союз, який відбувся у червні 2021 року, сторони дійшли згоди щодо необхідності дотримання принципів верховенства права для забезпечення глобальності, відкритості, стабільності й безпечності кіберпростору.

Учасники обмінялися інформацією про інституційну структуру та повноваження органів у сфері кіберпростору, останні напрацювання у розробці законодавчих ініціатив, які включають оновлення Директиви ЄС 2016/1148 щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі[2].

[1] У ЄС з'явиться підрозділ кібербезпеки – Cyber Rapid Response Team <https://mil.in.ua/uk/news/u-yes-z-yavytsya-pidrozdil-kiberbezpeky-cyber-rapid-response-team/> дата звернення 21.09.2021.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016) 194 *Official Journal*

Наступним кроком для України повинна стати розробка національного законодавства з урахуванням положень оновленої стратегії Європейського союзу у сфері кібербезпеки за умов цифрової модернізації модернізації на наступні роки, яку затверджено Радою Європейського Союзу у березні 2021 року.

Вказана стратегія була представлена Єврокомісією та високим представником ЄС у грудні 2020 року. Вона містить рамкові умови дій ЄС із захисту громадян та бізнесу Євросоюзу від кібернетичних загроз, з розвитку захищеної інформаційної системи та захисту глобального, відкритого, вільного й безпечного кіберпростору.

Як зазначається в документі, кібернетична безпека є ключовим фактором для розбудови стійкої, «зеленої» та цифрової Європи, а також для досягнення цілей стратегічної автономії ЄС за умови збереження відкритої економіки європейської спільноти.

Рада ЄС визначила ключові напрямки діяльності із розвитку кібернетичної безпеки на наступні роки. Серед них, зокрема, намір створити мережу оперативних центрів з безпеки по усьому ЄС, головним призначенням якої буде прогнозування, своєчасне виявлення та протидія кібернетичним атакам на комунікаційні мережі. При цьому в ЄС має бути визначена оперативна структура, яка буде опікуватися питаннями координації дій та кризового менеджменту для протидії кібернетичним атакам і загрозам.

Окреме місце у стратегії відводиться швидкому завершенню формування в ЄС комунікаційної мережі 5G, її надійному захисту та зусиллям із розвитку наступних систем зв'язку нового покоління.

Планується також підвищити стандарти безпеки в мережі Інтернет, який залишається важливим інструментом для досягнення цілей безпеки глобальних комунікацій. Для досягнення цієї мети ЄС використовуватиме конкурентні переваги власної промисловості, підвищуватиме стандарти безпеки у мережі, включаючи застосування сучасних систем захисту та шифрування інформації. Такий захист надаватиметься, в першу чергу, мережам правоохоронних органів та судової влади для забезпечення ефективного обміну оперативною інформацією.

Вдосконаленню підлягатиме також «кібернетична дипломатія», яка передбачатиме інструментарій ЄС для запобігання кібернетичним нападам та для реагування на такі атаки, якщо вони скоєні проти ЄС в таких сферах, як стійкість мереж постачання, критично важлива інфраструктура та послуги, демократичні процедури та діяльність державних інституцій, економічна безпека тощо. При розвідувально-ситуаційному центрі ЄС (INTCEN) також, заплановано створення спеціальної групи кіберрозвідки[1].

Висновки. Підсумовуючи вищевикладене та враховуючи правозастосовну практику в умовах російської агресії, доходимо висновку, що організація дієвої міжнародної співпраці в інформаційній сфері дозволить забезпечити належний рівень кібербезпеки України.

Одним із першочергових завдань у вказаній сфері є формування дієвого механізму забезпечення безпеки інформаційного простору з урахуванням відповідного передового міжнародного досвіду. У значній мірі це стосується нашої держави з огляду на євроінтеграційні сподівання, необхідність впровадження ефективних механізмів розвитку економіки, сучасних інформаційних технологій тощо та перебування держави у стані «неоголошеної війни» з боку РФ.

of the European Union 1–30.

[1] EU's CS (2021) Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy <https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy//> дата звернення 21.09.2021.

REFERENCES

LIST OF LEGAL DOCUMENTS

LEGISLATION

1. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016) 194 *Official Journal of the European Union* 1–30.

2. EU's CS (2021) Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy <https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy//> data zvernennia 21.09.2021.

BIBLIOGRAPHY

ARTICLES

3. Pohoretskyi M, Shelomentsev V, Poniattia kiberprostoru yak seredovyshcha vchynennia zlochyniv [Concept of cyberspace as an environment for committing crimes] (2009) 2 *Informatsiina bezpeka liudyny, suspilstva, derzhavy* 77–81 [in Ukrainian].

4. Chernysh R, Zaluchennia hromadskosti do zabezpechennia kiberbezpeky derzhavy (za prykladom Velykobrytanii) [Involvement of the public in ensuring the cyber security of the state (by the example of Great Britain)] (2017) *Naukovi chytannia* 198–202 [in Ukrainian].

BOOKS

5. Istoriia informatsiino-psykholohichnoho protyborstva [History of informational and psychological struggle] Pidruchnyk (K., Nauk. – vyd. viddil NA SB Ukrainy, 2012) 212 [in Ukrainian].

WEBSITES

6. Brytanyia predupredyla ob otvetnыkh merakh v sluchae khakerskykh atak [The British Ministry of Defense accused Russia of cyber attacks] <https://www.rbc.ua/rus/news/britaniya-predupredila-otvetnyh-merah-sluchae-1478018271.html> data zvernennia 21.09.2021 [in Ukrainian].

7. Brytanskaia razvedka yshchet kyber-ahentov sredy devochek-podrostkov [British intelligence is looking for cyber-agents sredi devochek-podrostkov] <http://ru.delfi.lt/abroad/global/britanskaya-razvedka-ischet-kiber-agentov-sredi-devochek-podrostkov.d?id=73490964> data zvernennia 21.09.2021. [in Ukrainian].

8. Chotyryrichnyi ohliad oborony [Quadrennial Defense Review] <https://history. defense.gov/Historical-Sources/Quadrennial-Defense-Review/> data zvernennia 21.09.2021 [in Ukrainian].

9. Global Cybersecurity Index URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

10. Get Safe Online week <http://www.cabinetoffice.gov.uk/news/get-safe-online-week> data zvernennia 21.09.2021 [in Ukrainian].

11. Minoborony Brytanii zvynuvatylo rf u kiberatakakh [The British Ministry of Defense accused Russia of cyber attacks] <http://ua.korrespondent.net/world/3809809-minoborony-brytanii-zvynuvatylo-rf-u-kiberatakakhs> data zvernennia 21.09.2021 [in Ukrainian]

12. Pravytelstvo Velykobrytanyy potratyt $2,3 mlrd na ukreplenye kyberbezopasnosty [The British government will spend $2.3 billion to strengthen cyber security] <http://www.securitylab.ru/blog/personal/tsarev/321169.php> data zvernennia 21.09.2021 [in Ukrainian].

13. Velykobrytanyia potratyt 1,9 mlrd funtov sterlynhov (2,1 mlrd evro) na usylenye kyberbezopasnosty v strane v techenye blyzhaishykh piaty let [Great Britain will spend 1.9 billion pounds sterling (2.1 billion euros) to strengthen cyber security in the country over the next five years] <https://www.ukrinform.ru/rubric-world/2112238-britania-gotovit-na-kiberbezopasnost-21-milliarda.html> data zvernennia 21.09.2021 [in Ukrainian].

14. U shkolakh Anhlii vvedut zaniattia z kiberbezpeky [Cyber security classes will be introduced in schools in England] <https://bdzhola.com/news/u-shkolah-angliji-vvedut-zanjattja-z-kiberbezpeki> data zvernennia 21.09.2021 [in Ukrainian].

15. U YeS z'iavytsia pidrozdil kiberbezpeky – Cyber Rapid Response Team [Cyber security unit – Cyber Rapid Response Team will appear in the EU] <https://mil.in.ua/uk/news/u-yes-z-yavytsya-pidrozdil-kiberbezpeky-cyber-rapid-response-team/> data zvernennia 21.09.2021 [in Ukrainian].

Chernysh R.,
Candidate of Law, Associate Professor,
National Academy of Security Service of Ukraine
ORCID: *0000–0003–4176–7569*

DOI: *https://doi.org/10.17721/2413-5372.2021.3-4/112-121*

INTERNATIONAL ORGANIZATIONAL EXPERIENCE IN THE SPHERE ENSURING CYBER SECURITY

«Whoever owns information owns the world!»
Nathan Rothschild

Annotation. *The article states that in recent years global cyberspace has been more objectively assessed by the world community as one of the most important security priorities, as its functioning is a significant factor in the development of the economy, military, social, security and other sectors. The threat of hacking Internet systems with criminal intent or in the interests of special services of foreign countries is on the same level as terrorism, espionage and the use of weapons of mass destruction. Taking into account the insufficient experience of counteracting the specified negative phenomena by special entities, the help of foreign partners and the use of their diverse efforts in this direction is considered relevant.*

Taking into account the above, ***the purpose of the article*** *is to analyze the organizational activities of certain special entities of foreign states in the field of cyber security.*

It is claimed that special services of the Russian Federation are purposefully carrying out cyber attack campaigns in the USA and EU countries. These challenges led to the formation of the so-called cyber troops Analyzing open sources of information, we can come to the conclusion that at the official level their existence is recognized only in a part of the countries in the world (USA, Iraq, Great Britain, Russian Federation, etc.), but in reality they function in almost every developed state.

It is noted that currently Ukraine organizes cooperation with international partners on a systematic basis, and one of the priority steps should be the development of national legislation taking into account the provisions of the updated strategy of the European Union in the field of cyber security in the conditions of digital modernization for the coming years.

One of the primary tasks in the specified area is also the formation of an effective mechanism for ensuring the security of the information space, taking into account the relevant best international experience. To a large extent, this concerns our country in view of European integration hopes, the need to implement effective mechanisms for the development of the economy, modern information technologies, etc., and the country's stay in a state of «undeclared war» on the part of the Russian Federation.

Key words: *cyber security, cyber army, cyber space, Internet network.*