DOI 10.31558/2519-2949.2024.2.25
УДК 339.137.22:355.402

ORCID ID: https://orcid.org/0000-0002-7362-2666
Гунін В. Є., Воєнна академія імені Євгенія Березняка

ORCID ID: https://orcid.org/0000-0002-4222-813X
Смолянюк В. Ф., Воєнна академія імені Євгенія Березняка

КОНКУРЕНТНА РОЗВІДКА В УМОВАХ ЕСКАЛАЦІЇ СУЧАСНИХ КІБЕРЗАГРОЗ

Проаналізовано тенденції поширення кібернетичної злочинності у світі, що є загрозою інформаційній безпеці нашої держави та безпеці діяльності конкурентної розвідки зокрема.

З'ясовано, що завдяки кібератакам з боку окремих держав на інформаційний простір інших атакуючи намагаються досягнути на свою користь певних політичних цілей: змінити легітимні уряди в інших країнах; деструктивно вплинути на економічний, енергетичний, військовий потенціали цих країн, а також на їх духовній стан; взяти під диктаторський контроль цілі народи і країни, а можливо й поневолити їх без застосування військової сили в класичному її розумінні. Яскравим прикладом такої цільової кібератаки можна виділити напад російських хакерів на супутниковий інтернет-сервіс Viasat, який відбувся 24 лютого 2022 року за годину до повномасштабного вторгнення російських військ на територію України. Ця атака привела до знищення більшості супутникових терміналів, що негативно вплинуло на зв'язок між військовим керівництвом держави і підрозділами Сил оборони України.

Виділено місце та роль кібернетичної безпеки в системі національної безпеки України та її державних структур. Розглянуто стан систем забезпечення безпеки від кібернетичних атак в провідних країнах світу, зокрема Сполучених Штатах Америки, Великої Британії та Австралії. Визначено реакцію керівництва зазначених країн на сучасні кіберзагрози. З огляду на поширення кіберзлочинності у світі одним з пріоритетних напрямів удосконалення діючої системи кібербезпеки в цих країнах стає реформування національних контррозвідувальних органів. Встановлено, що основна мета цього реформування полягає у реорганізації діючих інформаційно-аналітичних підрозділів і створення нових, що здатні адекватно протидіяти зазначеним загрозам.

Підготовлено окремі пропозиції суб'єктам конкурентної розвідки щодо можливих варіантів організації протидії сучасним кіберзагрозам з огляду на особливості реформування іноземних спецслужб.

***Ключові слова**: національна безпека, кібернетичний простір, кібернетична безпека, кіберзагрози, кібератаки, інформаційно-комунікаційні технології та системи, контррозвідка*

Постановка проблеми в загальному вигляді. Сьогодні узаконеного поняття «конкурентна розвідка» в Україні не існує, хоча діяльність зі збирання, зберігання, обробки та розповсюдження інформації регулюється цілою низкою законодавчих і нормативних актів. Наприклад, відповідно до положень Закону України «Про розвідку» одним з основних завдань розвідки є своєчасне забезпечення споживачів розвідувальною інформацією, зокрема добування, аналітичне опрацювання, оброблення і надання розвідувальної інформації її споживачам у встановленому цим Законом порядку. Основним завданням конкурентної розвідки з огляду на чинне законодавство України є постійний збір, нагромадження, аналіз даних про внутрішнє й зовнішнє середовище компанії з відкритих джерел та надання вищому менеджменту комерційної структури інформації, що дозволяє її керівництву передбачити зміни в навколишній обстановці і приймати своєчасні оптимальні рішення щодо управління сучасними ризиками. Конкурентна розвідка насамперед має виявляти та визначати ступінь небезпеки від зовнішніх загроз, що деструктивно впливатимуть на функціонування компанії, впроваджувати нові форми та методи з організації протидії цим загрозам, зокрема в кіберпросторі [1, 2].

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-

© Гунін В. Є., Смолянюк В. Ф., 2024

комунікаційних технологій (ІКТ) з надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу. Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу. У зв'язку з цим цілком природно постала необхідність контролю та подальшого врегулювання відповідних відносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість брак такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони [3–5].

Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі має стати одним з пріоритетних завдань конкурентної розвідки. У зв'язку з цим виникає проблемне питання, як саме суб'єкти конкурентної розвідки мають долучитися до виконання заходів з протидії сучасній кіберзлочинності й водночас використовувати кіберпростір для розв'язання пріоритетних завдань комерційних структур з огляду на реформування контррозвідок провідних країн світу [6–13].

Зв'язок проблеми з важливими науковими і практичними завданнями. Обраний напрям дослідження тісно пов'язаний з виконанням положень Указу Президента України від 14 вересня 2020 р. № 392/2020 «Про стратегію національної безпеки України», Указу Президента України від 15 жовтня 2021 р. № 685/2021 «Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки», Указу Президента України від 26 серпня 2021 р. № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України», а також необхідністю долучити сили та засоби конкурентної розвідки до організації адекватної протидії виявленим кіберзагрозам діяльності державних структур відповідно до вимог чинного законодавства України [1, 2].

Аналіз останніх досліджень і публікацій. Перелік сучасних загроз національним інтересам України та її державним інститутам у кіберпросторі визначено в [3]. Основні положення Стратегії кібербезпеки України розглянуто в [4, 5]. Реакція контррозвідок провідних країн світу на сучасні кіберзагрози національній безпеці держави викладено в [6–9]. Перспективи реформування контррозвідок провідних іноземних країн з огляду на характер впливу сучасних кіберзагроз на національну безпеку висвітлено в [10–13]. Зважаючи на результати проведеного аналізу зазначених матеріалів, можна зробити обґрунтований висновок, що сьогодні недостатньо уваги приділяється дослідженню проблем щодо використання досвіду іноземних спецслужб, зокрема контррозвідувальних органів провідних країн світу, у регламентації діяльності суб'єктів конкурентної розвідки з огляду на визначені кіберзагрози.

Метою статті є підготовка окремих пропозицій суб'єктам конкурентної розвідки щодо можливих варіантів організації протидії сучасним кіберзагрозам з огляду на особливості реформування іноземних контррозвідок, що викликано сучасними кіберзагрозами.

Виклад основного матеріалу. Досліджуючи питання щодо забезпечення безпеки діяльності суб'єктів конкурентної розвідки в сучасному кіберпросторі насамперед потрібно визначитися, яку саме небезпеку для них можуть становити сучасні кіберзагрози.

Тенденції поширення кібернетичної злочинності у світі. У сучасних умовах глобалізації суспільства кіберзагрози все частіше стають ефективним інструментом для досягнення мети щодо несилового контролю та управління об'єктами з критичною інформаційною інфраструктурою держави. Сьогодні завдяки кібератакам окремі держави світу отримують можливість досягнути певні політичні цілі, змінювати легітимні уряди в інших країнах, а також здійснювати деструктивні зміни в усіх сферах життєдіяльності суспільства і держави (економічній, енергетичній, духовній тощо) цих країн, брати під контроль і навіть поневолювати цілі народи і країни практично без застосування військової сили в класичному її розумінні.

Згідно з останнім звітом "Verizon 2020 Data Breach Report: Money Still Makes the Cyber-Crime World Go Round" [11] з кіберзлочинності, 86% атак фінансово мотивовані: зловмисники або безпосередньо вимагають гроші в жертви, або виконують сторонні замовлення, наприклад, конкурентів чи інших недоброзичливців.

Сьогодні можна виділити п’ять основних типів кіберзагроз: програми-вимагачі; цільові кібератаки; DDoS-атаки; інсайдерські загрози і фішинг, пов’язані з діяльністю інсайдерів і людськими помилками.

Наприклад, першою такою загрозою можна назвати використання кіберзлочинцями програм-вимагачів або вірусів-вимагачів, за допомогою яких зловмисники шифрують дані на комп’ютері користувача і вимагають викуп за можливість відновити доступ до них. Найбільшого впливу від таких атак телекомунікаційні компанії, інтернет-провайдери, освітні установи, урядові й технологічні організації.

Другою не менш шкідливою кіберзагрозою для телекомунікаційних систем є цільова кібератака. Її зміст полягає в тому, що спочатку зловмисники шукають спосіб потрапити в корпоративну мережу: збирають інформацію, шукають уразливості організації (не тільки цифрові, а й фізичні), вивчають розклад, маршрути, слабкості співробітників, які їх зацікавлюють тощо. Потім відбувається власне проникнення: зловмисники можуть надіслати на електронну пошту конкретного співробітника фішинговий лист, вкрасти його телефон для вилучення будь-яких корпоративних паролів, утертися в довіру компанії під виглядом підрядника або проникнути в офіс як кур’єр. На цьому етапі кіберзлочинець приховано встановлює програмне забезпечення на корпоративній техніці. На останньому кроці, діючи вже ізсередини компанії, зловмисник підбирається до інформації, яка його цікавить, і викрадає її в обхід засобів захисту. Потім кіберзлочинець замітає сліди, щоб атаку не було виявлено.

Третьою небезпечною кіберзагрозою можна вважати так звану DDoS-атаку. Це атака на будь-яку обчислювальну систему (наприклад, сервер), щоб вичерпати її апаратний ресурс через величезну кількість одночасних звернень до неї. Коли система не справляється з обробкою великої кількості звернень, відбувається відмова в обслуговуванні (Denial of Service) звернень і система виходить з ладу.

Четвертою загрозою, що становить достатньо велику небезпеку є так звана інсайдерська загроза. Джерелом такої загрози, на жаль, є власні співробітники. Виникнення цієї загрози поширено в організаціях, де не контролюють надання прав доступу високого рівня, а також не розмежовують права доступу до інформаційних ресурсів. Проте слід відрізняти інсайдерські загрози, які можуть бути пов’язані зі злим умислом, від спричинених випадковими діями або пов’язаних з людською помилкою.

П’ятою кіберзагрозою телекомунікаційним системам з переліку основних є фішинг. Це вид шахрайства для виманювання в довірливих або неуважних користувачів комп’ютерної мережі персональних даних. Найчастіше приманкою для таких осіб може стати звичайний електронний лист, здатний зацікавити одержувача, а функції гачка для нього виконує закладений у цей лист шкідливий файл або гіперпосилання на нього [12].

Яскравим прикладом цільової атаки може бути факт нападу російських хакерів на Україну, що розпочався буквально за кілька хвилин до повноцінного вторгнення армії рф. За даними агентства Reuters, США, Великобританія та Європейський Союз тоді офіційно звинуватили рф у великомасштабному кібернападі, який 24 лютого 2022 року порушив роботу супутникового інтернет-сервісу Viasat саме за годину до початку повномасштабного вторгнення рф на територію України. Це спричинило знищення «десятків тисяч» супутникових терміналів. Великобританія зазначила, що атака деструктивно вплинула на роботу центральноєвропейських інтернет-користувачів та вітрових електростанцій, а також українських військових та деяких цивільних клієнтів [14].

Кіберзлочинність як загроза діяльності конкурентної розвідки. Сьогодні практично всі більш-менш розвинені держави зіткнулися з деструктивними наслідками впливу сучасних кіберзагроз та гострою потребою розпочати формування системи кібербезпеки та кібероборони. В ході вивчення особливостей виникнення і перебігу сучасних воєнних конфліктів було виявлено нову тенденцію їх розвитку, зокрема перенесення звичайних бойових дій до нового середовища – так званого кіберпростору, що ще більше загострило ці конфлікти. Ця проблема спонукала провідні країни світу до запровадження першочергових заходів зі створення спеціальних структур і підрозділів безпеки для організації протидії загрозам у кіберпросторі. Спираючись на світовий досвід можна стверджувати, що процес забезпечення кібербезпеки насамперед передбачає організацію адекватної протидії сучасним загрозам у світовому кіберпросторі. Для організації протидії таким загрозам провідні країни світу намагаються створити потужну підсистему так званого кіберзахисту в загальній системі забезпечення національної безпеки. Безумовно, що цю підсистему мають постійно вдосконалювати

відповідні державні органи і структури з огляду на характер виявлених ними кіберзагроз. Зазначена підсистема обов'язково має в собі включати такі важливі елементи як кіберрозвідка та кібервплив.

З огляду на деструктивний вплив сучасних кіберзагроз на всі сфери життєдіяльності держави, суб'єкти конкурентної розвідки мають долучатися до організації адекватної протидії зазначеним вище загрозам, використовуючи всі наявні сили та засоби. Такий підхід суттєво сприятиме інтеграції України до ЄС та НАТО, а також реалізації вимог Альянсу щодо проведення процедур управління всією системою оборони країни, зокрема інформаційного забезпечення її державних структур. Проте, суб'єкти конкурентної розвідки мають усвідомлювати, що ці загрози також деструктивно впливатимуть на їх діяльність, що заважатиме ефективному виконанню професійних завдань, які ставляться вищим менеджментом комерційної структури.

Проблемним у цій сфері залишається питання щодо наукового обґрунтування пріоритетів в організації захисту держави від сучасних кіберзагроз, зокрема із залученням можливостей конкурентної розвідки, яка також має залучатися до протидії сучасним кіберзагрозам. Стає очевидним, що вирішити цю проблему неможливо без детального вивчення суб'єктами конкурентної розвідки діючих нормативно-правових актів [2] та використання досвіду провідних іноземних країн у цій сфері.

Реакція контррозвідок провідних країн світу на сучасні кіберзагрози. Сучасною організаційною формою діяльності контррозвідки в Армії США є розслідування. За результатами чергового розслідування стосовно нещодавно проведених кібератак на державні установи США іноземними спецслужбами директор Національного центру контррозвідки та безпеки Білл Іваніна зробив висновок, що сьогодні Китай у цій сфері далеко випереджає будь-які інші країни, навіть рф. Зокрема, США звинуватили китайську розвідку у спробі викрасти в західних компаній технології, що використовують у комерційній авіації. Газета Financial Times повідомила, що китайські вчені, які працюють у західних університетах, ведуть збір інформації на користь китайської армії [8]. Також контррозвідка США нещодавно попередила американську космічну галузь про небезпеку з боку іноземних розвідувальних організацій, які намагаються викрасти дослідницькі та комерційні секрети щодо національних космічних програм. Також у звіті Національного центру контррозвідки та безпеки вказувалося на те, що невизначені іноземні організації (за первинною оцінкою КНР та рф) використовували кібератаки, щоб отримати доступ до космічної галузі США [9].

У липні 2023 року Комітет з питань розвідки та безпеки британського парламенту (ISC) оприлюднив відкриту частину свого звіту про розслідування щодо характеру загрози національній безпеці з боку Китаю в широкому плані, а також про виявлену розвідувальну зацікавленість КНР до трьох конкретних сфер (академічної спільноти, промисловості й технологій, ядерної енергетики). Зокрема ISC зазначив, що використання китайськими спецслужбами сучасного кіберпростору дало можливість їм заволодіти певною інтелектуальною власністю та інформацією у цих ключових галузях промисловості Сполученого Королівства, що в подальшому сприятиме технологічному домінуванню Китаю над Заходом [10].

У Річному звіті Організації розвідки і безпеки Австралії (Australia's Security Intelligence Organization – ASIO) за 2021–2022 роки було акцентовано, що національна безпека країни останнім часом потерпає від різних кіберзагроз зовні, які мають яскраве забарвлення шпигунської діяльності з використанням кіберзасобів. Зокрема, у звіті визначено, що іноземні спецслужби постійно намагаються викрасти інформацію про політичну систему Австралії, плани й наміри щодо перспектив забезпечення національної безпеки, оборонні заходи та підготовку до проведення спеціальних операцій, технологічні можливості країни, її економічні і торгові переваги над іншими, особливості діяльності діаспор на території країни, а також намагаються отримати доступ до баз персональних даних австралійців. У зв'язку з цим найбільшою загрозою національній безпеці країни контррозвідка Австралії вважає кібершпигунство з боку іноземних держав [13].

Об'єднує за змістом ці звіти те, що вказані провідні країни світу занепокоєні проблемою щодо розвитку сучасної кіберзлочинності, тому вони насамперед ставлять за мету проведення відповідних реформ в своїх структурах, направлених на реорганізацію діючих підрозділів та створення нових, які виконуватимуть функції з організації (підготовки) та здійснення заходів з адекватної протидії сучасним кіберзагрозам.

Пропозиції суб'єктам конкурентної розвідки щодо можливих варіантів організації протидії сучасним кіберзагрозам з огляду на особливості реформування іноземних спецслужб. На жаль не існує готових рецептів на всі випадки життя та підходів, однаково придатних для всіх організацій,

щоб убезпечити себе хоча б від найбільш вірогідних ризиків. З огляду на це суб'єкти конкурентної розвідки мають взяти до уваги, що в ході виконання професійних завдань вони можуть зазнати значної шкоди у результаті деструктивного впливу кіберзагроз різного ґатунку, що спеціально штучно створюються іноземними контррозвідувальними органами, оскільки одним із основних їх завдань є захист комерційної таємниці.

Добуваючи інформацію комерційного характеру, суб'єкти конкурентної розвідки також мають усвідомлювати, що окрім фізичного та технічного захисту своїх комерційних об'єктів іноземна контррозвідка вживатиме спроби потрапити до телекомунікаційних мереж, якими користується розвідка. Яскравим прикладом наведеного може стати хакерська атака групи «Солнцепек» з росії на ІТ-інфраструктуру української телекомунікаційної компанії «Київстар», що відбулася 13 грудня 2023 року. Отже для суб'єктів конкурентної розвідки проблемним залишається питання не тільки продовжувати ефективно виконувати свої професійні завдання в умовах можливого впливу сучасних кіберзагроз, але у той же час вони мають своєчасно організувати адекватну протидію цим кіберзагрозам. Таким чином вони протидіятимуть іноземним спецслужбам, під контролем яких зазвичай здійснюються подібні наведеним вище кібератаки на державні та приватні структури. Тому суб'єкти конкурентної розвідки, проникаючи до комерційної інформації, що зберігається на різних носіях в іноземних компаніях, мають не забувати про відповідний захист тих засобів і мереж, якими вони користуються в ході професійної діяльності.

Наприклад, для повноцінного захисту телекомунікаційних мереж, якими користуються суб'єкти конкурентної розвідки для виконання професійних завдань, від програм-вимагачів або вірусів-вимагачів вищому менеджменту кожної зацікавленої компанії потрібно зосередити увагу на якості спеціального обладнання та сучасного програмного забезпечення, яке використовують її підлеглі, а також на регулярне проведення їх системної профілактики, що включає оцінку ризиків, установку міжмережевих екранів, створення резервних копій корисної інформації, розробку сценаріїв реагування на різноманітні події та інші заходи.

Для запобігання цільовим атакам з боку іноземних спецслужб, представників інших зацікавлених компаній або анонімних хакерів, співробітники конкурентної розвідки мають враховувати те, що сучасні засоби захисту від кібератак, за умови їх правильного й комплексного використання, насамперед дають змогу користувачу своєчасно зрозуміти про початок неавторизованої активності невідомого походження. Тому, працюючи в певній телекомунікаційній мережі в інтересах комерційної структури, користувач спочатку має пройти свою ідентифікацію. Тобто довести системі, що це саме він, а потім авторизуватися – отримати суворо регламентовані права для роботи в цій системі. З метою запобігання цільових атак на телекомунікаційну мережу вищий менеджмент компанії має регламентувати суворий і чіткий розподіл прав доступу всередині цієї системи, а також дотримання принципу мінімальної достатності: тобто кожним користувачем системи виконуються лише ті дії, на які він має повноваження і які потрібні для досягнення необхідних результатів.

Для боротьби з DDoS-атаками в телекомунікаційних мережах мають застосовуватися DDoS-фільтри, що дають можливість вибірково відсікати зайві звернення до сервера, які можуть надходити від так званих ботів. Профілактика DDoS-атак включає розумну мінімізацію контактів системи з іншими пристроями: доступ до системи має бути закритий для портів, протоколів і додатків, взаємодію з якими не передбачено користувачем.

Для боротьби з інсайдерськими загрозами необхідно реалізовувати принцип мінімальної достатності: працівнику компанії мають надавати лише ті права, які йому потрібні для виконання робочих обов'язків. Крім того, для боротьби з цими загрозами також можуть допомогти системи і методи, які аналізують поведінку самого користувача. Такі системи побудовано на технологіях штучного інтелекту. Вони придатні до навчання на основі надходження певних статистичних даних. Зокрема ці системи постійно моніторять активність співробітників компанії на робочих місцях. Якщо вони відхиляються від заздалегідь заданих сценаріїв діяльності, то формуються оповіщення для служби безпеки компанії, яка може заблокувати ту чи іншу дію.

Небезпека фішингу полягає в тому, що головний елемент в цій кіберзагрозі має не технічний, а психологічний характер. Кіберзлочинці спочатку знаходять людину, яку обдурити легше ніж сам комп'ютер, а потім вона свідомо або несвідомо надає їм доступ до закритої інформації через провадження програм-шпигунів в закриті внутрішні мережі компанії.

Висновок. Аналіз сучасної кіберзлочинності вказує на те, що завжди існують загрози можливого використання іноземними спецслужбами, представниками інших зацікавлених структур або анонімними хакерами тощо так званих програм-шпигунів для отримання корисної інформації через

проникнення до закритих телекомунікаційних мереж певної компанії. Не виключено, що таке проникнення може відбуватися і через відкриті соціальні мережі. Отже, щоб організувати адекватну протидію сучасним кіберзагрозам і водночас ефективно використовувати кіберпростір для вирішення своїх професійних завдань, суб'єкти конкурентної розвідки мають суворо дотримуватися рекомендованих заходів безпеки під час роботи із сучасними ІКТ та ІТС, а також своєчасно вносити вищому менеджменту компанії, в інтересах якої вони працюють, пропозиції щодо вдосконалення кіберзахисту її телекомунікаційних мереж з огляду на характер виявлених ними кіберзагроз.

Перспективи подальших досліджень. Деталізувати особливості організації протидії сучасним кіберзагрозам з огляду на використання компанією штучного інтелекту.

Бібліографічний список:

1. Про розвідку : Закон України від 17.09.2020 р. № 912-IX. URL: https://zakon. rada.gov. ua/laws/show/912-20#Text (дата звернення: 26.11.2023).

2. Ланде Д. В. Правові питання конкурентної розвідки. *Інформація і право*. 2020. № 2(33). С. 51–68.

3. Щоденні кіберзагрози. Офіційний веб-сайт МО України. URL: https://www.mil.gov. ua/ukbs/shhodenni-kiberzagrozi/ (дата звернення: 30.11.2023).

4. Про Стратегію кібербезпеки України : Указ Президента України №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року». Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/ 4472021-40013 (дата звернення: 06.12.2023).

5. Стратегія кібербезпеки України: цілі та пріоритети. Інтернет-видавництво: *АрміяІнформ*. URL: https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili -ta-priorytety/ (дата звернення: 14.12.2023).

6. Стратегія національної контррозвідки США (2020–2022): основні загрози та пріоритети. URL: https://niss.gov.ua/news/statti/strategiya-nacionalnoi-kontrrozvidki-ssha-2020-2022-osnovni-zagrozi-ta-prioriteti (дата звернення: 20.12.2023).

7. Кравченко Р. М. Діяльність військової контррозвідки в армії США: організаційно-правовий аспект. *Інформація і право*. 2018. № 4(27). С. 112–120.

8. Китай загрожує США більше, ніж Росія – американська контррозвідка. URL: https://www.radiosvoboda.org/a/news-kytaj-zagrozhue-amerytsi-bilshe-nizh-rosiya/29671071.html (дата звернення: 24.12.2023).

9. Контррозвідка США попередила космічні компанії про іноземне шпигунство. URL: https://www.unian.ua/world/kontrrozvidka-ssha-poperedila-kosmichni-kompaniji-pro-inozemne-shpigunstvo-12364569.html (дата звернення: 27.12.2023).

10. Паливода В. О. Оцінка загрози національній безпеці Сполученого Королівства з боку Китайської Народної Республіки. *Центр зовнішніх досліджень НІСД*, 2023. С. 1–4.

11. Отчет Verizon Business 2020 о расследовании утечек данных (DBIR2020). URL: https://www.securitymagazine.com/articles/92415-verizon-2020-data-breach-report-money-still-makes-the-cyber-crime-world-goround (дата звернення: 06.01.2024).

12. Global Threat Landscape Report. URL: https://www.fortinet.com/content/dam/ maindam/ PUBLIC/02_MARKETING/08_Report/Threat-Report-H1–2020.pdf (дата звернення: 17.01.2024).

13. Організація розвідки і безпеки Австралії: річний звіт 2021–2022. Australia's Security Intelligence Organization (ASIO). Annual Report 2021–2022. Australia. GPO Box 2176, Canberra ACT. 2601. P. 1–151.

14. Війна Росії проти України почалася з кібернападу на супутники. За годину до вторгнення були знищені «десятки тисяч» терміналів Viasat. *IT community, Технології*. URL: https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/ (дата звернення: 20.01.2024).

References:

1. Pro rozvidku : Zakon Ukrainy vid 17/09/2020 r. № 912-IX. URL: https://zakon. rada.gov. ua/laws/show/912-20#Text (accessed on: 26/11/2023).

2. Lande D. V. (2020). Pravovi pytannia konkurentnoi rozvidky. *Informatsiia i pravo*. 2№ 2(33). S. 51–68.

3. Shchodenni kiberzahrozy. Ofitsiinyi veb-sait MO Ukrainy. URL: https://www.mil.gov. ua/ukbs/shhodenni-kiberzagrozi/ (accessed on: 30/11/2023).

4. Pro Stratehiiu kiberbezpeky Ukrainy : Ukaz Prezydenta Ukrainy №447/2021 «Pro rishennia Rady natsionalnoy bezpeky I oborony Ukrainy vid 14 trvnia 2021 roku». Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy. URL: https://www.president.gov.ua/documents/ 4472021-40013 (accessed on: 06/12/2023).

5. Stratehiia kiberbezpeky Ukrainy: tsili ta priorytety. Internet-vydavnytstvo: ArmiiaInform. URL: https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili -ta-priorytety/ (accessed on: 14/12/2023).

6. Stratehiia natsionalnoy kontrrozvidky SShA (2020-2022): osnovni zahrozy ta priorytety. URL: https://niss.gov.ua/news/statti/strategiya-nacionalnoi-kontrrozvidki-ssha-2020-2022-osnovni-zagrozi-ta-prioriteti (accessed on: 20/12/2023).

7. Kkavchenko R. M. (2018). Diialnist viiskovoi kontrrozvidky v armii SShA: orhanizatsiino-pravovyi aspect. *Informatsiia i pravo*. № 4(27). S. 112–120.

8. Kytai zahrozhuie SShA bilshe, nizh Rosiia – amerykanska kontrrozvidka. URL: https://www.radiosvoboda.org/a/news-kytaj-zagrozhue-amerytsi-bilshe-nizh-rosiya/29671071.html (accessed on: 24/12/2023).

9. Kontrrozvidka SShA poperedyla kosmichni kompanii pro inozemne shpyhunstvo. URL: https://www.unian.ua/world/kontrrozvidka-ssha-poperedila-kosmichni-kompaniji-pro-inozemne-shpigunstvo-12364569.html (accessed on: 27/12/2023).

10. Palyvoda V. O. (2023). Otsinka zahrozy natsionalnii bezpetsi Spoluchenoho Korolivstva z boku Kytaiskoi Narodnoi Respubliky. *Tsentr zovnishnikh doslidzhen NISD,* S. 1–4.

11. Otchet Verizon Business 2020 o rassledovanii utechek dannyh (DBIR2020). URL: https://www.securitymagazine.com/articles/92415-verizon-2020-data-breach-report-money-still-makes-the-cyber-crime-world-goround (accessed on: 06/01/2024).

12. Global Threat Landscape Report. URL: https://www.fortinet.com/content/dam/ maindam/PUBLIC/02_ MARKETING/08_Report/Threat-Report-H1–2020.pdf (accessed on: 17/01/2024).

13. Orhanizatsiia rozvidky i bezpeky Avstralii: richnyi zvit 2021–2022. Australia's Security Intelligence Organization (ASIO). Annual Report 2021–2022. Australia. GPO Box 2176, Canberra ACT. 2601. P. 1–151.

14. Viina Rosii proty Ukrainy pochalasia z kibernapadu na suputnyky. Za hodynu do vtorhnennia buly znyshcheni «desiatky tysiach» terminaliv Viasat. *IT community*, *Tekhnolohii*. URL: https://itc.ua/ua/novini/vijna-rosiyi-proti-ukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatki-tisyach-terminaliv-viasat/ (accessed on: 20/01/2024).

Hunin V., Smolianiuk V. Competitive intelligence in the context of the escalation of modern cyber threats

The trends in the spread of cybercrime in the world, which is a threat to the information security of our state and the security of competitive intelligence in particular, have been analyzed.

It was found that thanks to cyber attacks by individual states on the information space of others, they are trying to achieve certain political goals in their favor: to change legitimate governments in other countries; to have a destructive effect on the economic, energy, and military potential of these countries, as well as on their spiritual state; to take entire peoples and countries under dictatorial control, and possibly to enslave them without the use of military force in the classical sense.

A striking example of such a targeted cyber attack is the attack by Russian hackers on the Viasat satellite Internet service, which took place on February 24, 2022, an hour before the full-scale invasion of Russian troops into the territory of Ukraine. This attack led to the destruction of most of the satellite terminals, which negatively affected the communication between the military leadership of the state and units of the Defense Forces of Ukraine. The place and role of cyber security in the national security system of Ukraine and its state structures is highlighted. The state of security systems against cybernetic attacks in the leading countries of the world, in particular the United States of America, Great Britain and Australia, is considered. The reaction of the leadership of the specified countries to modern cyber threats has been determined. Given the spread of cybercrime in the world, one of the priority directions for improving the current cyber security system in these countries is reforming national counterintelligence agencies. It was established that the main goal of this reform is to reorganize the existing information and analytical units and create new ones capable of adequately counteracting the specified threats.

Separate proposals have been prepared for the subjects of competitive intelligence regarding possible options for organizing countermeasures against modern cyber threats, taking into account the peculiarities of reforming foreign special services.

Keywords*: national security, cyber space, cyber security, cyber threats, cyber attacks, information and communication technologies and systems, counterintelligence*