DOI: **: 10.33099/2311-7249/2024-49-1-93-104**

УДК: 004.03+004.9+004.62+004.049

Машталір Вадим Віталійович *(доктор історичних наук, професор)*
Гук Олександр Миколайович *(доктор філософії)*
Мурасов Рустам Камілович *(кандидат технічних наук)*
Фараон Сергій Іванович *(доктор філософії)*
Лоза Володимир Вікторович *(доктор філософії)*

Національний університет оборони України, Київ, Україна

КІБЕРБОРОТЬБА В УМОВАХ ЗБРОЙНОГО ПРОТИСТОЯННЯ: АНАЛІЗ, СТРАТЕГІЇ ТА ВИКЛИКИ

Протидія кіберзагрозам в умовах сьогодення розглядається як один із найважливіших пріоритетів безпеки і вагомий чинник у розвитку військового, соціального, економічного та інших секторів. Перебіг російсько-української війни демонструє розуміння цінності інноваційних технологій у збройному протистоянні, збільшення цифровізації військових дій з метою збереження людського ресурсу, та збільшення кібератак на сторону противника з метою суспільно-політичного залякування і нанесення шкоди національним інтересам держави. З'являється тенденція використання стратегій асиметричних непрямих дій в кіберпросторі або через кіберпростір, заснованих на комбінації військових зусиль з політичними, економічними та інформаційно-психологічними методами впливу на супротивника для вирішення завдань, які раніше вирішувалися лише з використанням військової сили. Метою статті є аналіз існуючих кіберзагроз, сучасних форм і способів ведення кіберборотьби, а також обґрунтування необхідності розроблення нових підходів у тактиці та стратегії кіберборотьби для своєчасного реагування на загрози та виклики, що виникають в умовах збройного протистояння. У статті застосовано порівняльний метод для аналізу останніх досліджень і публікацій та наукових джерел праць стосовно існуючих кіберзагроз, нормативно-правової бази у сфері кібероборони. Крім того, використано метод системного аналізу сучасних форм та способів ведення кіберборотьби, а також синтез, абстрагування, узагальнення при обґрунтуванні нових підходів у тактиці й стратегії кіберборотьби. Зазначена класифікація кібервразливостей, що можуть бути використані кіберзлочинцями під час здійснення атак на кіберінфраструктуру, як державного, так і приватного секторів. Акцентована увага на важливості кіберборотьби в умовах збройного протистояння та її впливу на сучасні воєнні стратегії. Запропоновано нові підходи та стратегії ведення кіберборотьби з метою своєчасного реагування на загрози та виклики, що виникають в умовах збройного протистояння. Розглянуто наявні інноваційні технології, що застосовуються у кіберборотьбі. Зазначена необхідність координації та консолідації зусиль державного та приватного секторів у протистоянні сучасним викликам і загрозам в кіберпросторі. Теоретична значущість дослідження полягає у тому, що на основі аналізу існуючих загроз та викликів запропоновано нові підходи та стратегії ведення кіберборотьби. Елементом наукової новизни є те, що запропоновані зміни до стратегії і тактики ведення кіберборотьби зможуть підвищити ефективність захисту власної кіберінфраструктури, а також здійснювати асиметричний вплив на супротивника при збройному протистоянні. Практична цінність полягає у тому, що систематизовані знання у сфері кіберборотьби можуть бути використані під час її ведення в умовах збройного протистояння, що дозволить визначити можливі кібервразливості, а також своєчасно реагувати на загрози та виклики, що виникають.

Ключові слова: *кіберборотьба, збройне протистояння, стратегія кіберборотьби, кібербезпека, кіберінфраструктура, інформаційно-комунікаційні системи, інформаційні технології, кіберзагрози, кіберпростір, кібервплив, кібератаки.*

Вступ

Постановка проблеми. Аналіз останніх локальних війн і збройних конфліктів показав докорінні зміни у тактиці й стратегії збройного протистояння. Супротивник, який має технологічну перевагу, замість зіткнення з противником по фронту, більш ефективніше застосовує військові сили та засоби. Кількість військ, що розгорнуті на певному напрямі, вже не відіграють вирішальної ролі в досягненні мети

операції. Для забезпечення переваги над противником, вже недостатньо мати в своєму розпорядженні певний бойовий потенціал. Важливим є застосування його в потрібних місці та часі, і, водночас, необхідними є асиметричні дії.

Зміни в сучасному цифровому світі обумовлюють застосування нових підходів до ведення кіберборотьби. Кібератаки на критично важливі сектори: енергетика, зв'язок, охорона здоров'я, логістика, банківська справа тощо, завдають значної шкоди цивільному населенню, збільшують напругу в суспільстві та можуть призвести до руйнації економічного потенціалу держави, а також завдають шкоди національним інтересам держави. Саме за таких умов, спостерігається поява нових зразків кіберзброї, атаки зловмисників стають дедалі комплексними. Існує тенденція до збільшення випадків використання великих мовних моделей (LLM, large language model, далі – ВММ) для підтримки розроблення шкідливих програм. Хоча ВММ мають певні недоліки у створенні шкідливого програмного забезпечення, для виправлення яких може знадобитися втручання людини, все одно зберігається здатність цих інструментів суттєво допомагати у створенні шкідливого програмного забезпечення, особливо для кіберзлочинців. Вони регулярно вдосконалюють свою тактику, використовуючи нові технології. Суб'єкти загроз різного походження все частіше будуть використовувати генеративний штучний інтелект, одночасно зі збільшенням обізнаності та можливостей, пов'язаних із подібними технологіями [2]. Зазначимо, що постійна зміна природи кіберзагроз є одним з основних викликів. Кібератаки на критичну інфраструктуру можуть мати різноманітні форми, включно із кібершпигунством, кібертероризмом, кіберсаботажем тощо. Варто констатувати, що розроблення адаптивних і гнучких стратегій кіберборотьби є надзвичайно важливим напрямом роботи кіберфахівців.

Існування паралелей між кібертехнологіями та іншими галузями з подвійним призначенням, такими як ядерні, біологічні, космічні та інші, що мають як корисний, так і руйнівний потенціал зумовлює необхідність створення нових підходів до захисту об'єктів критичної інфраструктури з метою своєчасного реагування на загрози та виклики, що виникають [3]. Необхідною є чітка координація та консолідація зусиль, як в середині держави на всіх рівнях, так і у міжнародному середовищі для врегулювання правових норм та створення нових підходів щодо захисту критичної інфраструктури від кіберзлочинців та кібертероризму [4].

Застосування інформаційних технологій об'єднує всіх користувачів інформаційної та кіберінфраструктури, що використовують їх сервіси для забезпечення військ (сил) в умовах збройного протистояння. Дуже важливо підтримувати цілісність мереж і стежити за їх безпекою. Всі ці зміни передбачають створення принципово нових механізмів забезпечення функціонування сучасних інформаційно-комунікаційних систем військового призначення та кіберінфраструктури держави в цілому, а також розвиток форм і способів кіберборотьби [5].

Аналіз останніх досліджень і публікацій. Питання протистояння у кіберпросторі досліджувались Д. В. Дубовим, В. Л. Бурячком, С. В. Толюпою [6; 7], Ю. В. Завгороднєю [8], О. Ю. Пермяковим [25; 26], С. П. Євсеєвим [18; 19]. Проблеми ведення кіберборотьби розглядалися у роботах O. Buxton [10], D. Sutton [14], Dr. Ch. Cunningham [15], M. Smeets [24]. У роботах авторів, які досліджували раніше та продовжують опрацьовувати означені питання, розглядається певна множина понять, що стосуються кіберпростору, аспектів ведення кібердій під час збройного протистояння, кіберборотьби, забезпечення кібербезпеки держави. Також висвітлено питання кіберпростору як складової частини класичної й некласичної геополітики. Розглянуто геополітичне та геостратегічне значення кіберпростору і проблемні питання щодо забезпечення національних інтересів України в умовах зростання геополітичної ролі кіберпростору та протистоянь у ньому. Запропоновано головні принципи забезпечення інформаційної та кібербезпеки, розкрито їхню сутність, основний зміст та складові. Значну увагу надано типовим інцидентам у сфері кібербезпеки, а також методам і засобам соціального інжинірингу. Докладно розглянуто систему заходів із захисту від соціотехнічних та кібератак.

Проте розгляд питань кіберборотьби в умовах сучасної російсько-української війни потребує постійного оновлення з метою фіксації та наукового аналізу кібердій, що застосовуються противником, а також для формування нового наукового напряму. Тому, розвиток системи знань про основи ведення кіберборотьби, відповідно до вимог сьогодення, зокрема, у кіберпросторі є актуальним науковим завданням.

Метою статті є аналіз існуючих кіберзагроз, сучасних форм і способів ведення кіберборотьби, а також обґрунтування необхідності розроблення нових підходів у тактиці та стратегії кіберборотьби для своєчасного реагування на загрози і виклики, що виникають в умовах збройного протистояння.

Виклад основного матеріалу дослідження

Військові та політичні процеси, що відбуваються в Україні, та кібератаки, які

проходять у світі, можуть бути взаємопов'язані та бути залежними від політичних рішень регіонального значення, а в окремих випадках і глобального значення. Виникає необхідність деталізації розуміння кіберборотьби, як складової політичних процесів на регіональному та глобальному рівні, та як інструменту для досягнення військових цілей [8].

У Стратегічному оборонному бюлетені України [9] надано такі визначення:

воєнна агресія в кіберпросторі – здійснення системних та масштабних дій проти України в кіберпросторі іноземними державами (групами держав), зокрема, із залученням кіберпідрозділів військових формувань, розвідувальних та спеціальних служб, включно із використанням кіберозброєння та інших спеціальних засобів впливу в кіберпросторі (зокрема, опосередковано, шляхом приховування джерел їх походження);

кібероборотьба – сукупність взаємоузгоджених за метою, завданнями, місцем та часом заходів визначених військ (сил), спрямованих на здобуття інформації про кіберінфраструктуру противника, її знищення всіма видами зброї або захоплення (виведення з ладу, отримання контролю), заподіяння їй шкоди шляхом здійснення кібердій, проведення кібероперацій та радіоелектронного подавлення, захист своєї кіберінфраструктури від кіберрозвідки та кібердій противника.

Зазначенні терміни цілком повно формулюють роль та місце кібербортьби, а також визначають характер дій в кіберпросторі держави та форми і способи ведення кіберборотьби. В інших джерелах подається інше, дещо спрощене, визначення терміну «кіберборотьба». Зокрема, у [10] зазначено, що *кібероборотьба* – це кібератака або серія кібератак, спрямованих на країну чи державу з метою отримання стратегічної чи військової переваги. Акти кіберборотьби передбачають проникнення в мережі або їх пошкодження, саботаж інфраструктури і порушення діяльності організацій та установ, життєво важливих для інтересів країни противника.

Як і у конвенціальній боротьбі, головною метою кіберборотьби є послаблення країни супротивника шляхом підриву соціальної єдності, політичної стабільності та військово-промислового потенціалу. Межі між кіберборотьбою, кіберзлочинністю та кібертероризмом можуть бути нечіткими. Кіберборотьба, в першу чергу, не мотивується фінансовою вигодою, а здійснюється суб'єктами, пов'язаними з державою.

Протягом січня-лютого 2024 року, за фактами деструктивних кібератак, Державною службою спеціального зв'язку та захисту інформації України були проведені комп'ютерно-технічні дослідження в інформаційно-комунікаційних системах трьох організацій, зокрема, фінансової галузі, сфери охорони здоров'я та інформаційних технологій [11]. В більшості випадків первинний несанкціонований доступ до інформаційно-комунікаційних систем об'єкту атаки був отриманий заздалегідь. Крім того, з метою доступу до мережі кіберзлочинці використовували скомпрометовані облікові записи віртуальної приватної мережі (VPN), а також недоліки налаштувань і/або вразливості програмного забезпечення публічно доступних інформаційних систем. Також мали місце інциденти, пов'язані з кібершпигунством відносно складових сектору безпеки і оборони України, які були здійсненні угрупуваннями UAC-0028 (APT28) та UAC-0003 (Turla), зокрема, із застосуванням модифікованого флагманського шкідливого програмного забезпечення KAZUAR.

Як зазначено в [11], у першому кварталі 2024 року найбільш активною загрозою було угрупування найманців UAC-0050, що пов'язане з правоохоронними структурами російської федерації. Зафіксовано та досліджено не менше 15 кампаній, під час яких кіберзлочинцями застосовано, щонайменше, п'ять різновидів шкідливих програм: Remcos Rat, Quasar Rat, Venom Rat, Remote Utilities Та Lummastealer. Ураховуючи масовість атак і застосування програм, функціонал яких передбачає викрадення автентифікаційних даних, скомпрометовані логіни, паролі та сертифікати можуть сприяти створенню технічних передумов для отримання несанкціонованого доступу до інформаційно-комунікаційних систем організацій з метою подальшого розвитку атаки на їх «внутрішні» ресурси. Крім того, масштабні ураження кіберінфраструктури спричинила діяльність угруповання UAC-0010. Усунення наслідків від діяльності UAC-0010 та застосованого шкідливого програмного забезпечення може потребувати об'єднання зусиль не лише на рівні основних суб'єктів забезпечення кібербезпеки України, а й залучення світових технологічних стейкхолдерів.

У Звіті про глобальні ризики Всесвітнього економічного форуму 2023 року спрогнозовано, що у 2024 році загроза «кібернебезпеки» оцінюється, як найсерйозніший глобальний ризик, який очікується протягом наступних двох років. Озброєні дедалі складнішими методами, зокрема, використанням штучного інтелекту, кібератаки й надалі залишатимуться надзвичайно руйнівними та все частіше націленими на критичну інфраструктуру. Також у Звіті констатується, що об'єкти критичної інфраструктури зазнали численних атак протягом кінця 2023 року. Їхній повтор із застосуванням удосконалених шкідливих програм оснащених штучним інтелектом, здатний повністю зупинити роботу тих об'єктів критичної інфраструктури, що підлягають атаці. За таких умов, економічно розвинуті країни здійснили

низку превентивних заходів, спрямованих на підвищення кіберстійкості критичної інфраструктури, з особливим ухилом на захисті від ризиків, пов'язаних зі зловмисним використанням штучного інтелекту.

На посилення цього, у [12] були розроблені рекомендації, що заохочують «безпечний» підхід до розробки та використання потужних систем штучного інтелекту. Канада, Франція, Німеччина, Італія, Японія, США, Велика Британія та інші країни Європейського союзу також долучилися до умов цього документу і сформували настанови щодо відповідального розвитку та використання передових систем штучного інтелекту. Згадані вище спільні рекомендації, схвалені більш ніж 20 національними агентствами з кібербезпеки. У документі, розробникам систем штучного інтелекту наголошено на необхідності приймати обґрунтовані рішення щодо проєктування, розробки, розгортання та експлуатації таких систем таким чином, щоб їхня безпека була в пріоритеті протягом усього життєвого циклу.

У вересні 2023 року стало відомо, що китайські кіберзлочинці порушили цілісність платформи електронної пошти Microsoft, викравши десятки тисяч електронних листів з облікових записів Державного департаменту США. Це сталося після попередніх повідомлень про подібні атаки на інші державні органи уряду США, включно із Міністерством торгівлі. Протягом 2024 року очікують посилення таких загроз більш комплексними кібератаками. Особливе занепокоєння чиновників демократичних країн світу викликає те, наскільки кіберзлочинці використовуватимуть цифрову сферу для зриву демократичних процесів. Оскільки у 2024 році близько 49 відсотків населення світу в 64 країнах планують взяти участь у місцевих виборах і використати своє виборче право, деякі експерти висловлюють значне занепокоєння стосовно можливості використання виборчих процесів та інфраструктури як головної мішені. За повідомленнями CISA (Cybersecurity and Infrastructure Security Agency) генеративний штучний інтелект посилить ризики кібербезпеці та надасть змогу зловмисникам, швидше і дешевше створювати фейковий контент [12].

Ландшафт кіберзагроз продовжує розвиватися в напрямі все ефективніших і шкідливіших атак, які часто відбуваються в масштабі. Організації всіх форм власності стикнулися із загальним зростанням атак програм-вимагачів порівняно з попереднім роком, тоді як кількість атак таких програм, здійснених людиною, зросла майже втричі. Це супроводжувалося різким зростанням використання дистанційного шифрування під час атак. Використовуючи цей метод, зловмисник шифрує файл на іншому комп'ютері, а потім надсилає зашифрований файл на вихідний комп'ютер. Це може статися, якщо один комп'ютер у мережі зламано, проте є доступ до іншого комп'ютера зі зламаними обліковими записами користувача. На оригінальному комп'ютері не потрібне додаткове програмне забезпечення і шкідливі файли не залишаються.

Розглянемо деякі приклади роботи програм-вимагачів. Так, з листопада 2022 року спостерігалось подвоєння випадків *потенційного викрадення даних*, тобто крадіжки або несанкціоноване видалення чи переміщення даних із пристрою. Зазначимо, що тринадцять відсотків атак програм-вимагачів, здійснених людьми, які перейшли до фази викупу, мали певну форму викрадання даних. Частота атак компрометації електронної пошти різко зросла до понад 156 000 щоденних спроб. Аналіз подібних випадків, узагальнених компанією Microsoft Entra свідчать, що спроби атак з метою заволодіння паролями зросли більш ніж у десять разів у 2023 році, з приблизно 3 мільярдів випадків на місяць до понад 30 мільярдів [13].

Служби керованого розширеного виявлення та реагування, такі як Microsoft Defender Experts, є ефективним ресурсом для операційних центрів безпеки, що покликані виявляти критичні інциденти та вчасно реагувати на них. З їх допомогою відбувається моніторинг і спостереження за новими тактиками, методами та процедурами здійснення атак, або прогресування атак. Відповідні сповіщення надсилаються клієнтам, щоб надати конкретну інформацію стосовно обсягу, методу вторгнення та інструкцій з усунення проблеми. Зокрема, на основі сповіщень, надісланих клієнтами, експерти Microsoft Defender у 2023 році визначили дві основні загрози (рис. 1):

успішні атаки на ідентифікацію: що включали традиційні спроби викрадення паролю, складні спроби розпилення пароля в кількох країнах та IP-адресах, а також атаки «людина посередині» (Man in the middle (MITM));

використання програм-вимагачів: визначається, як будь-який випадок активності таких програм або спроб атак, що були виявлені та унеможливлені на різних етапах атаки.

На додаток до кількох варіантів програм-вимагачів, у 2023 році спостерігалася масштабна кампанія програм-вимагачів, спрямованих як на кінцеві точки, так і на хмарну архітектуру організації. Ці атаки були реалізовані угрупованням Mango Sandstorm. Ця кампанія містила як локальне, так і хмарне середовище, а також –дії з підвищення та знищення привілеїв у цифровому середовищі, та видалення ресурсів користувачів-жертв. Ще однією поширеною загрозою були цілеспрямовані спроби фішингу, що призводять до компрометації пристрою чи користувача: фітинг із застосуванням шкідливого

програмного забезпечення з наміром скомпрометувати пристрої, та фішинг з використанням атаки «людина посередині» з метою викрадення особистих даних [13].

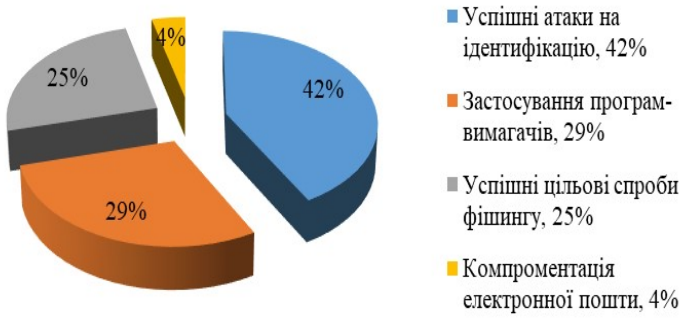

Рисунок 1 – Діаграма розподілу сповіщень про розвиток атаки за видами

Для фінансового шахрайства кіберзлочинці використовували різні методи, включно із викраденням електронної пошти та масовим розсиланням спаму за допомогою шкідливих програм. Вони також надсилали фішингові електронні листи зі шкідливими посиланнями та вкладеннями з електронної адреси жертви іншим користувачам в організації. Оскільки ці фішингові листи надсилалися внутрішньо, кілька користувачів стали жертвами атаки, натиснувши посилання протягом короткого періоду часу [13]. Зазвичай, причинами успіху кібератак є вдале використання кіберзлочинцями наявних кібервразливостей. До них належать: вразливості політики, процесів і процедур; технічні вразливості; вразливості кінцевих пристроїв; вразливості, що пов'язані з людським фактором; фізичні та екологічні вразливості (рис. 2).

Вразливості політики, процесів і процедур:
відсутність загальної політики інформаційної безпеки;
відсутність або некоректність політики контролю доступу;
неадекватне керування паролями користувачів;
використання системних облікових записів і паролів за замовчуванням;
постійне використання вбудованих системних облікових записів і паролів;
відсутність безпеки мобільних пристроїв;
відсутність поділу мережі;
нехтування політикою чистого столу та чистого екрану;
використання неперевіреного програмного забезпечення;
відсутність розподілу обов'язків;
неадекватний моніторинг та керування мережею;
використання незахищених публічних мереж;
неконтрольоване використання бездротових точок доступу;
неналежний захист від зловмисного програмного забезпечення;
несвоєчасне виправлення помилок та оновлення системи;
відсутність належних процедур резервного копіювання та відновлення;
відсутність надійної політики «принеси свій пристрій»;
неналежне керування доступом віддалених користувачів.

Технічні вразливості:
незрозумілий код;
неналежна специфікація вимог;
неналежні якість і тестування;
єдині точки відмови.

Вразливості кінцевих пристроїв:
IP камери;
фітнес-бігові доріжки та фітнес-трекери;
термостати та датчики диму.

Вразливості, що пов'язані з людським фактором:
соціальна інженерія;
відсутність поінформованості;
недотримання політики компанії та належної практики;
прості паролі;
неналежна підготовка та обізнаність.

Фізичні та екологічні вразливості:
доступ до будівлі та обладнання;
фізичний доступ до окремих елементів обладнання;
опалення, вентиляція та кондиціонування;
електроживлення.

Рисунок 2 – Класифікація кібервразливостей

Кібервразливість – будь-яке слабке місце, яке можна використати для здійснення атаки на мережу, систему чи службу [14]. Не завжди є можливість вжити превентивних дій для запобігання загрозам і безпосередньо атакам. Проте, вразливості – це ті речі до яких ми часто можемо вжити заходів для зменшення або навіть усунення, наприклад, помилки програмного забезпечення.

Деякі вразливості відображають природу активу, зокрема, здатність даних на магнітних носіях бути перезаписаними або видаленими. Їх іноді називають внутрішніми вразливостями, оскільки вони є частиною основної природи або складу предмета. Інші є результатом випадкової або навмисної дії чи бездіяльності, наприклад, нехтування створенням регулярних резервних копій. Це зовнішні вразливості, оскільки вони не є частиною основної природи чи складу предмета, а виникають за його межами.

Самі вразливості та методи (або засоби керування), які ми можемо використовувати для їх усунення, бувають різних форм. Більшість із них виникають через недотримання правил, процесів і процедур. Технічні вразливості виникають значно рідше, ніж вразливості, пов'язані з людським фактором чи навколишнім середовищем.

Нова ера усвідомлення того, що державна та приватна кіберінфраструктура, побудована на невдалій моделі безпеки на основі периметра, породжує нові загрози і спонукає галузь рухатися до нової кіберстратегії. Необхідно застосовувати нові удосконалені підходи, які дадуть змогу ефективніше реагувати на нові загрози, зменшувати вразливості та захищати кіберінфраструктуру, акцентуючи увагу на тому, що є найбільш практично досяжним. Щоб мати надійний кіберзахист, необхідно усвідомити такий фундаментальний аспект: частина нової стратегії вимагатиме технічного прогресу, управлінських та адміністративних змін в державному та приватному секторах. Фактом є те, що жодна окрема система не може бути абсолютно захищеною, якщо будь-які взаємозв'язані системи, які дотичні або мають доступ до цієї інфраструктури, також не будуть захищені. Тому для ефективності, організація має використовувати кілька пересічних рішень захисту, які працюють у тандемі. Водночас збій або обхід будь-якого індивідуального захисту не ставить під загрозу всю інфраструктуру.

Правильним стратегічним підходом у кіберпросторі є той, що визнає необхідність зосередження зусиль організацій та узгодження їхніх технологій для ефективної протидії загрозам на правильних перетинах у технологічній екосистемі. Такий стратегічний підхід зосереджується на отриманні контролю над користувацькими пристроями та системами, захищає дані, де це можливо, і якомога частіше використовує потужність хмари. Крім того, ключовим аспектом цієї стратегії є розгляд кожної мережі, пристрою, користувача, облікового запису, доступу чи іншого пов'язаного елемента, скомпрометованим, доки не буде доведено протилежне. Все це є постійною загрозою. Нікому і нічому не можна дозволяти працювати за замовчуванням, і будь-який доступ має бути чітко підтверджений, перш ніж він може мати місце.

Для того, щоб ця стратегія була ефективною, керівники мають усвідомлювати, що мережа – це завжди суперечливий простір. Мережа – це місце, де ведеться боротьба, а також динамічне середовище для реалізації загроз і не має значення є мережа хмарною чи локальною. Щоб цей підхід був ефективним, необхідно зосередитися на використанні засобів управління, які можуть бути запропоновані в ключових контрольних точках у межах цієї мережі, щоб отримати уявлення про оперативну ситуацію в системі; але ця точка контролю завжди буде слабким місцем.

У той час як концепція периметра стверджує, що далеко на кордонах мережі є оборонна «стіна», яка межує з інфраструктурою та утримує ворога на відстані, концепція «краю» стверджує, що краї інфраструктури рухаються разом з об'єктами, і, отже, також мають мати елементи керування, прив'язані до структури середовища, яке суб'єкт використовуватиме для отримання доступу до критичних даних. Важливо визнати, що з ускладненням типової кіберінфраструктури, ефективність механізмів захисту не завжди відповідає рівню цієї складності, відповідно, наявні стратегії безпеки захищають лише периметр мереж.

Будь-яка система, що використовується сьогодні, ймовірно, керуватиме кількома, якщо не сотнями, мереж та підмереж, кожна зі своєю локальною інфраструктурою, базою користувачів, сховищами даних і хмарними службами. Складність, яка настільки поширена в сучасній кіберінфраструктурі, означає, що для підприємства не існує єдиного периметра. Сама природа того, як сьогодні функціонують системи і засоби, за допомогою яких ці системи та користувачі «виконують свою роботу», передбачає те, що різні підходи до забезпечення безпеки найважливішого активу стануть частиною загальної стратегії. Цей актив, елемент, база даних чи щось інше, слід розглянути в першу чергу. Як і в реальній війні, ключовим компонентом виграшної стратегії кіберборотьби, є отримання видимості в просторі бою.

Якість розвідки залежить від можливості збору та аналізу даних про активи противника, які потребують використання даних телеметрії для цілей розвідки. Під час звичайних бойових дій найкраща видимість забезпечується під час

перебування на висоті, на пагорбі або за наявності супутникових зображень зони конфлікту. У кіберборотьбі «висота» вважається зайнятою, коли одна зі сторін, що бере участь у збройному протистоянні може «бачити» все, що відбувається всередині кіберінфраструктури супротивника. Це означає, що всі сутності та їх взаємодія з компонентами та інфраструктурою доступні для спостереження та надають корисні точки даних, які покращують здатність однієї сторони протистояння реагувати. Ключовим моментом є переконання у тому, що аналітичні дані, які надаються, дають змогу в подальшому проводити кібердії для досягнення певного результату.

Аналітичні дані, якими б інноваційними вони не були, фактично марні, якщо їх не можна використовувати для вирішення поточної проблеми. Якщо аналітичні дані, надані підрозділами збору розвідданих, не використовуються для фактичного вирішення наявних проблем, то вони буквально посилюють проблему, збільшуючи навантаження на аналітиків і тих хто забезпечує захист власної кіберінфраструктури.

Інструменти, що застосовуються в кіберпросторі, найчастіше мають подвійне призначення. З одного боку їх можна використовувати для захисту систем і покращення якості інфраструктури, а з іншого – завжди можна обернути проти тих, хто захищається, і використати для завдання шкоди тим самим системам та їхнім користувачам. Безумовно, існує спеціально розроблена кіберзброя, що застосовується кіберзлочинцями (кіберзлочинними угрупованнями) та групами, що спонсоруються державами, проте більшість того, що використовується, як інструменти кіберборотьби, насправді є функціональними частинами інфраструктури або інструментами, що можна використовувати для інновацій.

В умовах збройного протистояння застосовуються певні кіберпідрозділи або кіберсили (якщо вони передбачені структурою) збройних сил сторін, що беруть участь у цьому протистоянні. З метою ефективного застосування сил і засобів у кібердіях та/або кібероперація в армії США застосовується оперативний підхід, що являє собою опис командиром (командувачем) послідовності дій і переліку сил та засобів, що можуть бути застосовані для досягнення мети операції, забезпечення національних інтересів й воєнної переваги в цілому [15]. Це надає основу для вказівок та інструкцій командувача стосовно виконання процедур планування штабом і взаємодіючими партнерами, що забезпечує командиру візуалізацію того, як операції різнорідних (об'єднаних) сил трансформують поточні умови на бажані– те, як командир передбачає оперативне середовище після завершення операції для досягнення мети та забезпечення національних інтересів. Оперативний підхід в основному базується на розумінні оперативного середовища та проблем, викликів з якими може стикнутися командир. Під час розробки оперативного підходу, командири мають синхронізувати дії в кіберпросторі та через кіберпростір з іншими видами діяльності для досягнення визначених цілей. Дії в кіберпросторі зазвичай є наступальними та оборонними операціями, які перешкоджають супротивнику використовувати ресурси або маніпулюють інформацією, інформаційними системами чи мережами супротивника.

З іншого боку, військові діють через кіберпростір на регулярній основі, оскільки виконують спільні функції: командування та контроль, розвідка, здійснення ударів, пересування та маневрування, захист, інформаційне забезпечення. Ці спільні функції містять пов'язані можливості та дії, згруповані разом, щоб допомогти командирам інтегрувати, синхронізувати та керувати операціями (Рис. 3) [15].

У процесі побудови кіберзахисту, потрібно спочатку визначити, які типи атак мають найбільшу ймовірність успіху. Установа або організація може краще розрізняти, які пріоритети мають бути встановлені для вирішення проблем, та які мають найбільший вплив. Так само як у бою у фізичному просторі, захист є найкращим, коли він базується на реальності та коли захисник застосовує свою стратегію і технології, щоб захищатися там, де напад найімовірніший. Під час ведення кіберборотьби атаки досягають успіху, оскільки вони виявляють і використовують слабкі місця в системах і мережах. Кіберзлочинці здійснюють пошук технічних вразливостей та тих, що пов'язані з людським фактором, а потім ретельно зосереджуються на виявлених точках збою. Щоб захиститися від такого циклу атак, необхідно постійно перевіряти систему на наявність ймовірних слабких місць. Але це може бути складно, особливо коли мова йде про великі інфраструктури, які об'єднані між хмарними, нехмарними, локальними, зовнішніми та багатьма іншими потенційними конфігураціями.

Деякі з найцікавіших і найновіших інноваційних технологій, які є у вільному доступі, надають усвідомлення того, як ці активи можна використовувати для ведення кіберборотьби. Оскільки кіберзлочинці спрямовують свої атаки до легших і вразливіших цілей, власникам систем та об'єктів, що використовують останні інноваційні технології, також доведеться адаптувати методи експлуатації.

Однією з найновіших інновацій, що набула поширення в усьому світі, є автономний автомобіль. За останні кілька років автономні

транспортні засоби стали набагато ширшим глобальним явищем, ніж просто безпілотні автомобілі. Зараз існують автономні трактори, гелікоптери, таксі та човни – майже в кожному життєздатному варіанті використовуються різноманітні транспортні засоби з автономним керуванням або навігацією. Оскільки все більше транспортних засобів створюються з використанням штучного інтелекту і вдосконалюються для подальшого усунення людських помилок і прискорення руху, існує певна ймовірність збою. Наприклад, Військово-морські сили США та Сухопутні війська США, випробовують і впроваджують системи автономного транспорту. Якщо в автономній системі озброєння відбудеться спрацювання на невірно функціонуючий датчик, це спричинить реальну фізичну шкоду в межах циклу атаки, та ставить під загрозу виконання бойового завдання. Збільшення ступеню подальшого об'єднання цих систем та підвищення взаємозв'язку елементів, обумовлює можливість несанкціонованого доступу та/або маніпулювання логікою, завдяки якій ці системи функціонують, що може бути використано зловмисником.

Рисунок 3 – Дії в кіберпросторі, через кіберпростір, поза межами кіберпростору

Оскільки транспортні засоби вийшли за межі свого традиційного призначення, вимоги до бортового програмного забезпечення зросли в геометричній прогресії. Сучасний автономний транспортний засіб може мати приблизно сотню мільйонів рядків коду, що керує ефективною роботою до 70 електронних блоків керування. Для порівняння операційна система Windows Vista має близько 40 мільйонів рядків коду. Ця операційна система також має 905 відомих уразливостей, відповідно Національній базі даних уразливостей США (National Vulnerability Database), і використовувалася під час широкомасштабних кібератак програм-вимагачів Wanna Cry та Not Peyta у 2017 році. Тому логічним є те, що подібні, якщо не більш масштабні, типи атак можуть бути використані проти автономних транспортних засобів, а через складніші вимоги в операційній системі, ймовірніше, буде ще більше експлойтів.

Автономні транспортні засоби – це не більше, ніж кілька тисяч фунтів металу з сотнями датчиків, вбудованих у цей апарат. Ці транспортні засоби використовують дані від лідарів, лазерів, радарів, камер і ультразвукових датчиків. У бортових або водних автономних транспортних засобах часто присутні інші датчики, такі як датчики висоти та глибини, а також багато інших. Датчики надсилають інформацію на комп'ютер, який координує величезні обсяги даних, летячи дорогою, або водою, або повітрям, на значній швидкості. Безперечно, автономні транспортні засоби є благом для людства, проте існують загрози помилкової або несанкціонованої експлуатації.

Іншою інноваційною технологією, яка може бути використана з метою завдання шкоди супротивнику, під час ведення кіберборотьби, є застосування безпілотних літальних апаратів (далі – БпЛА). Вони доставляють пакунки, поповнюють запаси підводних човнів і навіть можуть використовувати медичне обладнання в екстрених випадках. Сфера застосування БпЛА

безмежна, але їх використання як у військових, так і у цивільних цілях створює водночас й потенційні загрози. Вони складаються із систем, які забезпечують політ автономно або за допомогою оператора, і мають складне програмне забезпечення та можливості керування. БпЛА військового класу – це інша історія, оскільки вони мають власні внутрішні енергетичні установки та часто створені для більшої стійкості до типових векторів атак (протидія РЕБ, захоплення управління). Однак навіть БпЛА, що розроблені та виготовлені для військового застосування, можуть бути скомпрометовані та використані супротивником у власних цілях. Досвід російсько-української війни засвідчив, що такі випадки відбуваються з обох боків.

Комерційні дрони так само небезпечні, як і військові, а часто навіть більше. Безпека не є пріоритетним питанням у процесі розробки цих засобів. У більшості випадків це, в кращому випадку, усувається в процесі експлуатації. У комерційних дронах експлуатація найчастіше здійснюється через атаки на контролер Wi-Fi або його бездротові системи. Wi-Fi є загальним інтерфейсом для більшості комерційних дронів, які присутні на ринку. Він функціонує, як інтерфейс між контролером і середовищем, де дані та відео циркулюють між дроном і станцією (пунктом) управління. Відповідно зловмисник знайомий зі звичайними методами зламу або експлуатації бездротового зв'язку, у нього є наявна вразливість у самому дроні, тому їх так само можна використовувати, як і будь-який звичайний комп'ютер, що використовує бездротові протоколи. Незважаючи на це, БпЛА може стати фізично рухомою та, можливо, кінетично застосованою зброєю, якщо цей зв'язок буде перехоплено, а управління дроном буде змінено для цілей, що не відповідають його початковому призначенню.

Вже існує певна зацікавленість військових фахівців, як використовувати технологію малих безпілотників для проведення кінетичних ударів. Метою цього рою безпілотників є його запуск (застосування) і керованість звичайними піхотними силами, які б направляли рій на ціль у радіусі до 100 кілометрів. Ці невеликі дрони мають мінімальний радарний перетин сигнатур і, ймовірно, будуть пропущені або помилково ідентифіковані радарними засобами захисту (перехоплення) як птахи, або інший подібний об'єкт. Досягнувши потрібної зони, дрони скоординовано спускаються для знищення цілі. Кожен окремий безпілотник матиме можливість очолити рій, якщо головний дрон буде знищено або зроблено непридатним для використання. Наприклад, Збройні сили США також розвивають цей тип можливостей. Нещодавно Агентство передових оборонних дослідницьких проєктів (Defense Advanced Research Projects Agency DARPA) презентувало скоординований рій безпілотників, який проводить систематичний тактичний аналіз району бойових дій, а потім огороджує зону загрози [16].

Поодинокі атаки безпілотників або автономних транспортних засобів чи будь-яка невірна, хибна їх експлуатація не є єдиним способом досягнення цілей для зловмисника або ворога. Загрозливі кіберзлочинні угруповування та спонсоровані державами подібні особи (організації) тепер прагнуть поєднати інструменти та методи атак, щоб посилити вплив для досягнення своїх цілей. Комбінуючи наявні можливості для атак, суб'єкти загроз тепер можуть досягати більш комплексних, руйнівних, та асиметричних результатів [16].

Поряд із зазначеним вище, кіберзлочинці активізують використання ВММ для підтримки розробки шкідливих програм. ВММ можуть допомогти зловмисникам створювати нове шкідливе програмне забезпечення та покращувати наявне. Це може значно полегшити завдання тим злочинцям, які не мають належної технічної кваліфікації. Так, у період із січня до березня 2023 року Mandiant спостерігав дії суб'єктів загроз на підпільних форумах, які рекламували послуги із надання ВММ, продаж та доступ до інтерфейсу програмування додатка (API), а також створення ВММ коду [2].

Під час збройного протистояння основною функцією інформаційних систем є автоматизація процесів управління військами і зброєю, під якою розуміється процес створення і втілення в роботу органів управління систем і засобів автоматизації з потрібним математичним, програмним, інформаційним і лінгвістичним забезпеченням. Відповідно під час ведення кіберборотьби будь-яке злочинне угруповання, або спонсоровані державою кіберугруповування, будуть використовувати всі наявні можливості для здійснення атак на кіберінфраструктуру противника.

Висновки та перспективи подальших досліджень

Наведені вище результати цього дослідження, обумовлюють необхідність змін у стратегії і тактиці кіберборотьби. Побудова ефективного захисту вимагає від керівників всіх рівнів та осіб, що приймають рішення, адаптувати свій підхід до такого, який буде відповідати поточному та найближчому майбутньому стану кіберінфраструктури.

Відповідні зміни у підходах до ведення кіберборотьби на стратегічному рівні, можуть надати перевагу у формах та способах взаємодії з ворогом у кіберпросторі. Лише адаптація й модифікація державних та приватних стратегій кіберборотьби, зробить успішним протистояння

діям кіберзлочинців. Керівники установ (організацій) всіх форм власності з метою забезпечення кібербезпеки (в межах власної компетенції) зобов'язані планувати довгострокову перспективу та зосереджуватися на досягненні успіху у протистоянні в кіберпросторі, зменшенні загроз на основі аналізу реальних умов та факторів, необхідних для належного функціонування кіберінфраструктури.

У кіберпросторі час не на боці того хто захищається. Кіберзлочинці не обмежені законами чи дотриманням їх вимог; у них немає заборон у способах, якими вони можуть досягти своєї мети. Зловмисники постійно підвищують ефективність своїх атак, тому зволікання щодо оновлення засобів захисту та прийняття нових оптимальних стратегій боротьби з майбутніми загрозами може призвести до неприпустимих наслідків у функціонуванні об'єктів критичної інфраструктутри та кіберінфраструктури в цілому. Кібергрупи, які спонсоруються державою, і кіберзлочинні угруповання, також застосовують інноваційні технології, а в деяких випадках більш ефективно, ніж державні інституції та приватні організації. Кожен новий пристрій, користувач, обліковий запис або технологія, які запропоновані на ринку, стають додатковою зброєю, яку можна використовувати у злочинних цілях.

Напрямом подальших досліджень може бути розробка нових та вдосконалення існуючих форм і способів ведення кіберборотьби, відповідно до існуючих викликів та ландшафту загроз, що постійно змінюється та еволюціонує.

.

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України: Закон України від 04.04.2024 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 05.04.2023). **2. Threat Actors are Interested in Generative AI, but Use Remains Limited**, URL: https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited (accessed: 05.04.2023). **3. Гук О. М., Мурасов Р. К., Фараон С. І., Толмачов І. В.** Стратегії кібербезпеки для захисту критичної інфраструктури: виклики та перспективи *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*: Міжнародна науково-практична інтернет-конференція, 12–13.03.2024. Вип. 86. URL: http://www.konferenciaonline.org.ua/ua/article/id-1649/ (дата доступу: 05.04.2023). **4. Гук О. М., Мурасов Р. К., Фараон С. І., Толмачов І. В.** Особливості здійснення кібервпливів, як складової кіберборотьби в умовах збройного протистояння. *Матеріали IV Всеукраїнської науково-практичної конференції* (м. Київ, 28 лютого 2024 року). Навчально-науковий інститут захисту інформації ДУІКТ. Київ, 2024. 300 с. https://duikt.edu.ua/uploads/p_2661_62255520.pdf (дата доступу: 05.04.2023). **5. Машталір В. В., Гук О. М., Толмачов І. В., Фараон С. І.** Прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення з урахуванням його еволюції. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 48(3). С. 147–156. DOI: 10.33099/2311-7249/2023-48-3-147-156. **6. Дубов Д. В.** Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ: НІСД, 2014. 328 с. **7. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В.** Інформаційна та кібербезпека: соціотехнічний аспект : підручник за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ. ДУТ, 2015. 288 с. **8. Завгородня Ю.В.** Історія становлення кібервійни як складової політичного процесу. *Збірник наукових праць Актуальні проблеми політики.* 2023. Вип. 72 DOI: https://doi.org/10.32782/app.v72.2023.6. **9. Стратегічний оборонний бюлетень України:** Указ Президента України №473/2021 від 20 серпня 2021 р. URL: https://www.president.gov.ua/documents/4732021-40121 (дата доступу: 05.04.2023). **10. Buxton Oliver Cyber Warfare**: Types, Examples, and How to Stay Safe. Academy. URL: https://www. avast.com/c-cyber-warfare (accessed: 05 April 2023). **11. Щодо обстановки в сфері кібер на 23-24 лютого 2024 року** URL: https://cert.gov.ua/article/6277822 (accessed: 05.04.2023). **12. Global Threat Intelligence Report** (September 1 – December 31, 2023). March 2024. URL: https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report (accessed: 05 April 2023). **13. Microsoft Digital Defense** Report 2023. Building and improving cyber resilience URL: https://www.microsoft.com/uk-ua/security/security-insider/microsoft-digital-defense-report-2023 (accessed: 05.04.2023). **14**. **Sutton D.** Cybersecurity. The complete guide to cyber threats and protection Second edition **15. Gregory D. Hillebrand**, **Bill Ault**, Strategic Cyberspace Operations Primer 18 December 2023, United States Army War College. **16**. **Dr. Chase Cunningham** Cyber Warfare - Truth, Tactics, and Strategies, 2020 Packt Publishing ISBN 978-1-83921-699-2 **17. Пермяков О. Ю., Королюк Н. О., Фараон С. І.** Організація інформаційних систем Збройних Сил України : навчальний посібник. Київ: НУОУ ім. Івана Черняховського, 2019. 143 с. **18. Yevseiev S., Milov O., Opirskyy I., Dunaievska O., Huk O., Pogorelov V., Bondarenko K., Zviertseva N., Melenti Y., Tomashevsky B.** Development of a concept for cybersecurity metrics. *Eastern-European Journal of Enterprise Technjlogies.* 2022. Vol. 4, No. 118. P. 6–18. **19. Yevseiev S., Ponomarenko V., Laptiev O., Milov O.** Synergy of building cybersecurity systems : monograph. Kharkiv. PC Technology Center, 2021. 188 p. **20. Військовий стандарт ВСТ 01.112.004 – 2017 (01)**. Військовий зв'язок та інформаційні системи. Словник НАТО з систем зв'язку та інформаційних систем (AAP-31 (Edition 3), IDT**).** Терміни та визначення. [Чинний від 2017-08-15]. Вид. офіц. Київ : МО України, 2017. 56 с. **21. Даник Ю. Г., Воробієнко П. П., Чернега В. М.** Основи кібербезпеки та кібероборони: підручник. Одеса: Вид-во ОНАЗ ім. О.С. Попова, 2018. 228 с. **22. Зв'язок та інформаційні системи**. Доктрина. Затв. Головнокомандувачем Збройних Сил України від 02.07.2020 р. №15841/С. **23. Гук О. М., Чередниченко О. Ю., Штонда Р. М., Диба І. О.** Дії в кіберпросторі під час підготовки та ведення мережецентричної війни. *Сучасні інформаційні технології у сфері безпеки і оборони.* 2017. Вип. 2(29). С. 107–112. **24. Max Smeets,** No Shortcuts: Why States Struggle to Develop a Military Cyber-Force (2022; online edn, Oxford Academic, 22 Sept. 2022). DOI: https://doi.org/10.1093/oso/9780197661628.001.0001.

25. Пермяков О. Ю., Сбітнєв А. І. Інформаційні технології і сучасна збройна боротьба. Луганськ: Знання, 2008. 204 с. **26. Основи моделювання бойових дій військ:** підручник/За ред. О. Ю. Пермякова. Київ : НАОУ, 2005.

CYBER WARFARE IN ARMED CONFRONTATION CONDITIONS: ANALYSIS, STRATEGIES AND CHALLENGES

Mashtalir Vadym *(Doctor of Historical Sciences, Professor)*
Huk Oleksandr *(Philosophy Doctor)*
Murasov Rustam *(Candidate of Technical Science)*
Faraon Serhii *(Philosophy Doctor)*
Loza Volodymyr *(Philosophy Doctor)*

The National Defence University of Ukraine, Kyiv, Ukraine

Formulation of the problem in general. *Countering cyber threats in today's conditions is considered one of the most important security priorities and a significant factor in the development of military, social, economic and other sectors. The course of the Russian-Ukrainian war demonstrates an understanding of the value of innovative technologies in armed conflict, an increase in the digitization of military operations in order to preserve human resources, and an increase in cyber attacks on the enemy side with the aim of social and political intimidation and harming the national interests of the state. There is a trend to use strategies of asymmetric indirect actions in cyberspace or through cyberspace, based on a combination of military efforts with political, economic and informational and psychological methods of influencing the adversary to solve tasks that were previously solved only with the use of military force. The purpose of the article is the analysis of existing cyber threats, modern forms and methods of conducting cyber warfare, as well as substantiation of the need to develop new approaches in tactics and strategy of cyber warfare for timely response to threats and challenges arising in conditions of armed confrontation.*

Analysis of recent researches and publications. *In the works of the authors who previously researched and continue to research the specified topic, a certain set of concepts related to cyberspace, aspects of conducting cyber operations during armed confrontation, cyber warfare, and ensuring the cyber security of the state are considered. The issue of cyberspace as a component of classical and non-classical geopolitics is also explored. The geopolitical and geostrategic significance of cyberspace and problematic issues related to ensuring the national interests of Ukraine in the conditions of the growing geopolitical role of cyberspace and confrontations in it are considered. The main principles of ensuring information and cyber security are highlighted, their essence, main content and components are revealed. Considerable attention is paid to typical incidents in the field of information technologies, as well as methods and means of social engineering. The system of measures to protect against sociotechnical and cyberattacks is considered in detail. Therefore, the development of a system of knowledge about the basics of conducting cyber warfare, in accordance with today's requirements and taking into account the experience of the Russian-Ukrainian war, in particular in cyberspace, is an urgent scientific task.*

Presenting the main material*. The article uses a comparative method for analysis the latest research, publications and scientific sources related to existing cyber threats, the regulatory and legal framework in the field of cyber defense, a method of systematic analysis of modern forms and methods of conducting cyber warfare, as well as synthesis, abstraction, generalization when justifying new approaches in tactics and cyber warfare strategies. The classification of cyber vulnerabilities that can be used by cyber criminals during attacks on the cyber infrastructure of both the public and private sectors is specified. Emphasis is placed on the importance of cyber warfare in armed conflict and its impact on modern military strategies. New approaches and strategies for conducting cyber warfare are proposed for the purpose of timely response to threats and challenges arising in the context of armed conflict. The available innovative technologies used in cyber warfare are considered. The need for coordination and consolidation of the efforts of the public and private sectors in confronting modern challenges and threats in cyberspace is indicated.*

An element of scientific novelty *is that the proposed changes to the strategy and tactics of conducting cyber warfare will be able to increase the effectiveness of the protection of one's own cyber infrastructure, as well as exert an asymmetric influence on the opponent during an armed confrontation.*

The theoretical significance *of the research lies in the fact that, based on the analysis of existing threats and challenges, new approaches and strategies for conducting cyber warfare are proposed.*

The practical value *is that systematized knowledge in the field of cyber warfare can be used during its conduct in the conditions of armed confrontation, which will allow to identify possible cyber vulnerabilities, as well as to respond in a timely manner to emerging threats and challenges.*

Conclusion and the perspectives of future researches. *Building an effective defense requires leaders and decision-makers at all levels to adapt their approach to one that meets the current and near-future state of cyber infrastructure. Corresponding changes in approaches to conducting cyber warfare at the strategic level can provide an advantage in the forms and methods of interaction with the enemy in cyberspace. Only the adaptation and modification of public and private strategies of cyber warfare will make the opposition to the actions of cybercriminals successful. Leaders of institutions of all forms of ownership in order to ensure cyber security are required to plan for the long term and focus on achieving success in countering cyberspace, reducing threats based on an analysis of real conditions and factors necessary for the proper functioning of cyber infrastructure. The direction of further research may be the development of new and improvement of existing forms and methods of conducting cyber warfare, in accordance with existing challenges and the constantly changing and evolving threat landscape.*

Keywords: *cyber warfare, armed confrontation, cyber warfare strategy, cyber security, cyber infrastructure, information and communication systems, information technologies, cyber threats, cyber space, cyber influence, cyber attacks.*

References

1. About the main principles of ensuring cyber security of Ukraine [online], (2024). Zakon Ukrainy № 2163-VIII, 04 April. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text [Accessed 05 April 2023]. **2. Threat Actors are Interested in Generative AI, but Use Remains Limited** [online], (2023), Available at: https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited [Accessed 05 April 2023]. **3. Huk O. M., Murasov R. K., Faraon S. I., Tolmachov I. V.,** (2024). Cybersecurity strategies for critical infrastructure protection: In: *International Scientific and Practical Internet Conference on Information Society: Technological, Economic and Technical Aspects of Formation*. 12-13 March 2024. Issue 86. [online]. Available at: http://www.konferenciaonline.org.ua/ua/article/id-1649/ [Accessed 05 April 2023]. **4. Huk O. M., Murasov R. K., Faraon S. I., Tolmachov I. V.** Peculiarities of implementing cyber influences as a component of cyber warfare in conditions of armed confrontation. In: *IV All-Ukrainian Scientific and Practical Conference* (Kyiv, February 28, 2024). Educational and Scientific Institute of Information Protection DUIKT. Kyiv. **5. Mashtalir, V. V., Huk, O. M., Murasov, R. K., Faraon, S. I., Tolmachov, I. V.,** (2023). Forecasting the degree of cyber influence on heterogeneous information systems of military purpose, taking into account its evolution. *Modern information technologies in the sphere of security and defense.* 48(3), 147-156. DOI: 10.33099/2311-7249/2023-48-3-147-156. **6. Dubov, D. V.,** (2014). *Cyberspace as a new dimension of geopolitical rivalry*: monograph. Kyiv: NISD. **7. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V.,** (2015). Information and cyber security: socio-technical aspect: Pidruchnyk za zah. red. d-ra tekhn. nauk, profesora V. B. Tolubka. Kyiv. DUT. 288. **8. Zavhorodnya, Yu. V.,** (2023). The history of the formation of cyber warfare as a component of the political process. *Collection of scientific papers Current problems of politics.* 72 DOI: https://doi.org/10.32782/app.v72.2023.6 **9. Strategic Defense Bulletin of Ukraine** [online], (2021). Ukaz Prezydenta Ukrayiny No. 473/2021, 20 August,. Available at: https://www.president.gov.ua/documents/4732021-40121 [Accessed 05 April 2023]. **10. Buxton Oliver Cyber Warfare**: Types, Examples, and How to Stay Safe. Academy [online], (2023). Available at: https://www.avast.com/c-cyber-warfare [Accessed 05 April 2023]. **11. Regarding the situation in the cyber sphere on February 23-24, 2024** [online], (2023). Available at: https://cert.gov.ua/article/6277822 [Accessed 05 April 2023]. **12. Global Threat Intelligence Report** (September 1 – December 31, 2023) [online], (March 2024). Available at: https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report [Accessed 05 April 2023]. **13. Microsoft Digital Defense Report 2023**. [online], Building and improving cyber resilience Available at: https://www.microsoft.com/uk-ua/security/security-insider/microsoft-digital-defense-report-2023 [Accessed 05 April 2023]. **14**. **Sutton, D.** Cybersecurity. The complete guide to cyber threats and protection Second edition **15. Gregory, D. Hillebrand**, **Bill Ault**, Strategic Cyberspace Operations Primer 18 December 2023, United States Army War College. **16**. **Dr. Cunningham, Chase** Cyber Warfare - Truth, Tactics, and Strategies, 2020 Packt Publishing ISBN 978-1-83921-699-2 **17. Permiakov, O. Yu., Koroliuk, N. O., Faraon, S. I.,** (2019). *Organization of information systems of the Armed Forces of Ukraine*: navchal'nyj posibnyk. Kyiv: NUOU im. Ivana Cherniakhovs'koho, 143. **18. Yevseiev, S., Milov, O., Opirskyy, I., Dunaievska, O., Huk, O., Pogorelov, V., Bondarenko, K., Zviertseva, N., Melenti, Y., Tomashevsky, B.,** (2022). Development of a concept for cybersecurity metrics. *Eastern-European Journal of Enterprise Technjlogies.* 4, 118, 6–18. **19. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O.,** (2021). Synergy of building cybersecurity systems: monograph. Kharkiv. PC Technology Center,. 188 p. **20. Military standard MST 01.112.004 – 2017 (01),** (2017). *Military communication and information systems. NATO Dictionary of Communication and Information Systems (AAP-31 (Edition 3), IDT). Terms and definitions.* [Chynnyj vid 2017-08-15]. Vyd. ofits. Kyiv: MO Ukrainy, 56. **21. Danyk, Yu. H., Vorobiienko, P. P., Cherneha, V. M.,** (2018). *Fundamentals of cyber security and cyber defense* : pidruchnyk. Odesa: Vyd-vo ONAZ im. O. S. Popova. **22. Communication and information systems.** Doktryna. Zatv. Holovnokomanduvachem Zbrojnykh Syl Ukrainy vid 02 July 2020 №15841/S. **23. Huk, O. M., Cherednychenko, O. Yu., Shtonda, R. M., Dyba, I. O.,** (2017). Actions in cyberspace during the preparation and conduct of a network-centric war. *Suchasni informatsijni tekhnolohii u sferi bezpeky i oborony.* 2 (29), 107-112. **24. Max Smeets,** No Shortcuts: Why States Struggle to Develop a Military Cyber-Force (2022; online edn, Oxford Academic, 22 Sept. 2022), https://doi.org/10.1093/oso/9780197661628.001.0001, accessed 5 Apr. 2024. **25. Permiakov, O. Yu., Sbitniev, A. I.,** (2008). Information technologies and modern armed struggle. Luhans'k: Znannia,. 204. **26. Basics** of military military action modeling: pidruchnyk / za red. O. Yu. Permiakova. Kyiv. NAOU, 2005.