УДК 351.865

Є. В. Котух,
к. т. н., доцент кафедри комп'ютерних наук, Сумський державний університет, м. Суми
ORCID ID: 0000-0003-4997-620X

DOI: 10.32702/2306-6814.2021.11.98

ТИПИ ВЛАДНИХ ВІДНОСИН У СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

Ye. Kotukh,
PhD in Technical Sciences, Associate Professor of the Department of Computer Science, Sumy State University, Sumy

TYPES OF POWER RELATIONS IN CYBERSECURITY STRATEGY

Стратегія кібербезпеки охоплює як захист державних інтересів у кіберпросторі, так і проведення більш широкої безпекової політики шляхом використання багатьох можливостей, які пропонує кіберпростір. У статті досліджено типологію владних відносин у стратегії кібербезпеки. Розглядаючи кібербезпеку в кожній з чотирьох категорій влади (примусовій, інституційній, структурній та продуктивній), встановлено, що вони не обов'язково взаємовиключні. Доведено, що примусова влада стосовно кібербезпеки надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кібербезпекою.

The cybersecurity strategy covers both the protection of public interests in cyberspace and the implementation of a broader security policy by using lots of opportunities offered by cyberspace. Cyberspace can be considered as the sum of two components. First is the physical substrate of cyberspace: the computers and networks in which they are assembled and through which they "communicate." Second is the communication facilitated by this physical layer: networking, digital activities that include content and actions performed through digital networks. As a strategic area, cyberspace must also be a domain of power. "Domain" should be understood as in the spatial sense — cyberspace is as physical as it is virtual, but also in a narrower sense — as a collective of social actors which are influenced by a certain form of governance.

There is no single comprehensive definition of power. For the purposes of our study, we used the four-sided typology proposed by Barnett and Duvall. Examining cybersecurity in each of the four governmental categories (coercive, institutional, structural and productive) found that they are not necessarily mutually exclusive. Coercive power over cybersecurity has been shown to provide opportunities for direct control of one actor by another; institutional power provides the possibility of indirect control over actors through institutions; structural power determines social opportunities and interests through the implementation of public-private partnerships; productive power makes it possible to find out how knowledge systems and discursive practices work in cybersecurity-generated social networks.

External actors to cyber threats are divided into governmental and non— governmental, with states posing the most complex threat. Authirities and proxies can cooperate, and there can be a significant intersection between terrorists and proxies. It is possible to oppose the activities of these actors only through the cooperation of actors from all three sectors, which has been repeatedly emphasized

and on which productive power is based. The crucial point of this form of governance is that control over information is deliberately limited to members of elite knowledge communities. Discourse is controlled by these communities for their own purposes and serves their own interests, effectively closing the discursive space to those who are external to these communities. Documents such as cybersecurity strategies can openly declare their control over information, citing operational and national security reasons.

Ключові слова: кібербезпека, кіберпростір, держава, влада, владні відносини, стратегія.
Key words: cybersecurity, cyberspace, state, power, power relations, strategy.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Можливості, які надає кіберпростір, такі, що навіть найбільш медіа-репресивні режими розглядають його використання як вигідне для їхнього політичного режиму. Водночас демократичні держави хочуть за допомогою кіберпростору забезпечувати участь громадян і соціально-економічне зростання, водночас покращуючи власне стратегічне становище.

Це завдання реалізується через відповідні стратегії, у тому числі стратегію кібербезпеки, яка охоплює як захист державних інтересів у кіберпросторі, так і проведення більш широкої безпекової політики шляхом використання багатьох можливостей, які пропонує кіберпростір. Отже, зі стратегічної точки зору кібербезпека реагує на захист національних інтересів та активно реалізує ці інтереси, а кіберпростір сприймається як середовище загроз та можливостей, в якому держава повинна діяти задля власного збереження та досягнення власних цілей. Крім того, кіберпростір проблематизується як місце і як джерело небезпеки. У цьому сенсі логічно з точки зору держави, що кіберпростір вимагає регулювання та втручання, також за допомоги відповідної стратегії.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Кібербезпеці у публічному просторі, визначенню її стратегічних цілей присвятили свої дослідження М. Барнет, Дж. Гілі, Р. Дювал А. Клімбург, Дж. Мелісен, Д. Сміт. Проте відсутність дефініційного консенсусу, практична невирішеність низки питань актуалізує доцільність проведення подальших досліджень у цьому напрямі.

МЕТА СТАТТІ

У статті за мету обрано дослідження типології владних відносин у стратегії кібербезпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ З ПОВНИМ ОБГРУНТУВАННЯМ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

Кіберпростір можна розглядати як суму двох компонентів. Перший — це фізичний субстрат кіберпростору: комп'ютери та мережі, в які вони зібрані та через які вони "спілкуються". Другий — це комунікації, яким сприяє цей фізичний рівень: мережева, цифрова діяльність, що включає вміст і дії, які здійснюються через цифрові мережі. Обмін інформацією залежить від існування фізичного рівня, який апріорі необхідний для існування кіберпростору. Кіберпростір є як фактичним, так і віртуальним, у тому сенсі, що кіберпростір є частково віртуальним середовищем, що грунтується на суттєвості фізичних систем.

Що важливо для публічної політики, кіберпростір часто розглядається не лише як сукупність людської та машинної діяльності. Наприклад, NSS 2009 говорить про "низку фізичних та технологічних середовищ, таких як суша, море та космос, які ми можемо охарактеризувати як домени.... Кіберпростір є одним із таких доменів" [2, с. 103—104]. Це, зокрема, передбачає розширення традиційної концепції військового домену від геопросторового до когнітивного та технологічного. Крім того, NSS 2009 називає кіберпростір "найважливішим новим доменом національної безпеки останніх років". Він тісно пов'язаний з іншим із нових визнаних у NSS 2009 доменів — "громадською думкою, культурою та інформацією", що становить інформаційний вимір інших сфер діяльності національної безпеки. Подібна позиція визначена у військовій доктрині США, яка описує кіберпростір як "глобальний домен в інформаційному середовищі" [2, с. 103—104].

Таким чином, як стратегічна сфера, кіберпростір також повинен бути доменом влади. "Домен" слід розуміти як у просторовому розумінні — кіберпростір настільки фізичний, скільки і віртуальний, але також і у вужчому розумінні — як колективність соціальних суб'єктів, які зазнають впливу певної форми влади. У міжнародних відносинах відповідними суб'єктами є держави, і деякі консервативні автори з ентузіазмом розглядають можливості, що надаються державам, здійснювати владу в кіберпросторі, як правило, за допомогою застосування військової сили. Подібним чином ліберальні інституціоналісти відзначають, що кіберпростір (і інформація в цілому) пропонує значні можливості для реалізації національних інтересів через багатосторонні інституції в глобалізованому світі.

Не існує єдиного всеохоплюючого визначення влади, але ми впевнені, що недостатньо обмежитися переважаючим трактуванням влади як сили примусу, якою володіє один суб'єкт над іншим. Тому для цілей нашого дослідження ми будемо використовувати чотиристоронню типологію, запропоновану Барнеттом і Дюваллом [1].

Барнетт і Дювал визначають владу як "виробництво, в соціальних відносинах та через них, наслідків, що

формують можливості суб'єктів визначати їх обставини та долю" [1, с. 42]. Вони стверджують, що в основі концепції влади є два "виміри". Перший вимір — це види соціальних відносин, за допомогою яких впливає (та реалізується) спроможність суб'єктів, а другий вимір — специфіка цих соціальних відносин. Перший вимір відрізняється тим, як виражається влада: або через взаємодію між соціальними суб'єктами, або через регуляторні соціальні відносини. Коли влада діє через дії попередньо створених соціальних суб'єктів щодо інших, це приблизно можна порівняти з "владою над" цими іншими соціальними суб'єктами. Як зазначають автори, влада майже стає атрибутом, яким володіє актор, і який може свідомо використовуватися як ресурс для формування дій інших акторів. У другому випадку влада функціонує через соціальні відносини, які передують соціальним або суб'єктним позиціям суб'єктів і які створюють їх як соціальних суб'єктів зі своїми можливостями та інтересами. Іншими словами, актори не володіють внутрішньою владою в силу своїх властивостей, а лише відчувають владу завдяки соціальним відносинам у соціальних структурах. Соціальні відносини визначають, хто є актором і які можливості вони мають для здійснення соціальних практик, аналогічно акторові, який має "силу" формувати умови свого власного існування.

Другий вимір влади стосується специфіки соціальних відносин влади, будь то прямі та безпосередні, або опосередковані та дифузні. Прямі соціальні відносини виникають між суб'єктами, які перебувають у фізичній, історичній чи соціальній позиційній близькості. Прямі відносини між суб'єктами є помітними, і що відносини є "механістичними, контактними, прямими, або логічно необхідними" [1, с. 46]. Прямі відносини не виключаються труднощами емпіричного встановлення відносин між суб'єктами, і принцип логічної необхідності є кращою умовою для їх встановлення. На відміну від цього, коли соціальні відносини є непрямими або дифузними, влада діє через опосередковані зв'язки і активна навіть тоді, коли діючі особи соціально, тимчасово або фізично віддалені.

Перехресним зіставленням цих чотирьох категорій влади Барнет і Дювал створюють просту таксономію. Примусова влада діє через безпосередній контроль одного суб'єкта над умовами існування та поведінкою іншого. Інституційна влада виявляється у непрямому контролі актора над умовами існування соціально віддалених інших суб'єктів. Структурна влада діє через прямі регуляторні соціальні відносини. Продуктивна влада виявляється через дифузні регуляторні соціальні відносини.

Хоча така типологія представлена в контексті теорії міжнародних відносин, однак її цілком можна використовувати і стосовно кібербезпеки, яка стосується національної безпеки та відносин між державами та відносин цілого ряду соціальних суб'єктів. Тому нижче розглянемо кібербезпеку в кожній з чотирьох категорій влади.

Примусова влада визначається як "діапазон відносин між суб'єктами, що дозволяють одному безпосередньо формувати обставини чи дії іншого" [1, с. 49]. Здійснення примусової влади безпосередньо впливає як на екзистенційні умови інших суб'єктів, так і на їх можливості для самостійних дій. У різноманітних течіях реалістичної теорії держава є головним референтом для політичних дій, і вона діє у власних інтересах, виключаючи всі інші інтереси. Хоча подібна точка зору апріорі не є неправильною, вона зайнята визначенням безпеки з точки зору національних інтересів і грунтується на логіці збройних загроз та військових реакцій. А у подібних дослідженнях політики та безпеки аналіз влади найчастіше перекошений у бік наймогутніших держав та здійснення військової сили для досягнення їх національних інтересів. Наприклад, важко обговорювати проблеми безпеки будь-якої країни без посилання на якийсь момент на Сполучені Штати, гегемонічний статус яких забезпечує центральне місце в західному (та і глобальному) дискурсі безпеки.

Звичайно, держава не повинна бути єдиним референтним об'єктом безпеки. Є багато інших суб'єктів, починаючи від окремих людей, соціальних груп та рухів, закінчуючи суспільствами і цивілізаціями, або навіть людством чи біосферою. Можливо, через труднощі приписування фіксованості сутностей на мікро- та макрокінцях цього спектра, "обмежені колективні угруповання" середнього рівня, як-от: держава та нація, зберігаються як домінуючі референтні об'єкти в дослідженнях безпеки. Хоча у багатьох стратегіях кібербезпеки приділяється багато уваги безпеці людей, але зазвичай держава залишається головним референтом для всіх форм безпеки в урядовому дискурсі. Наприклад, у кібербезпеці Великобританії безпека держави нерозривно пов'язана зі здоров'ям національної економіки, і вони пов'язані між собою як ті, що мають бути забезпечені за допомогою заходів кібербезпеки [2]. Це слідує переважаючому реалістичному погляду, що економічне процвітання є як передумовою національної безпеки, так і засобом здійснення впливу на неї. Також часто приділяється увага забезпеченню належного управління та державних послуг, хоча вони в значній мірі залежать від національної безпеки та економічного добробуту.

Стратегія кібербезпеки є частиною національної стратегії безпеки, і тому слід очікувати, що за необхідності держава використає свої безпекові можливості для захисту держави від супротивників у кіберпросторі. Ці дії повинні включати можливість "втручатися проти супротивників", і саме цей компонент кібербезпеки ми розглянемо як форму примусової влади.

Стратегія кібербезпеки, на наш погляд, обов'язково має містити елементи примусової влади для того, щоб розвинути більші можливості для здійснення безпосереднього контролю над діями суб'єктів, які є шкідливими для національних інтересів. Ця форма примусової влади включає типи активних оборонних та наступальних дій, які згадувались вище, але може також включати розгортання нематеріальних ресурсів, таких як правові та нормативні режими, з метою безпосереднього впливу на дії інших. Символічні ресурси, як-от: загроза воєнних дій, також слід розглядати як негативну санкцію, доступну державі в цій категорії, і тісно пов'язані із стримуючими та примусовими ефектами, сильно вираженими в прагненні зменшити мотивацію та спроможність противника.

Проте слід враховувати, що здійснення влади в режимі стримування, орієнтованого на актора (а не на вектор загрози), відрізнятиметься спробами стримувати державних та недержавних суб'єктів, не в останню чер-

гу через проблеми ідентифікації та атрибуції в кіберпросторі. Необхідно також, щоб потенційні та відомі супротивники знали, що проти них було створено ресурси, і вважали, що загроза проти них достовірна.

Як зазначалось, кіберпростір через свої характеристики є середовищем, яке сприяє діям агресора. У поєднанні зі значною здатністю зникати після нападу це ускладнює стримування супротивників за допомогою традиційних застосувань контролю та примусу. Тому доцільно, щоб примусова влада діяла тут також через вплив на процеси прийняття рішень ряду супротивників, навіть вилучаючи їх із мереж, якщо це можливо.

Інституційна влада. Очевидно, що державам не завжди можливо безпосередньо контролювати суб'єктів як таких — повинні бути посередники, за допомогою яких можна здійснювати владу та отримувати результати. Отже, держава повинна діяти через цих агентів, щоб контролювати дії та можливості інших. Це форма непрямої дії, роз'єднання між акторами, що створює "соціальну дистанцію", яка може діяти як у просторовому, так і в часовому аспектах. Подібне спричиняє чітку артикуляцію влади, коли держава та супротивник є соціально віддаленими, але пов'язаними через посередницьку установу, яка може або не може бути повністю під контролем держави. Тобто інституційну владу можна у цьому разі визначити як вплив на суб'єктів, які працюють за визначеними для них правилами та процедурами, що направляють, керують та обмежують дії (або бездіяльність) та умови існування соціально віддалених інших суб'єктів.

У випадку установ, над якими домінуючий суб'єкт здійснює повний контроль, ці правила та процедури можуть розглядатися як інструменти примусової влади. Там, де це не так, або коли кілька суб'єктів здійснюють контроль над даними інструментами, існує певна форма інституційної влади. Іноді, наприклад, щодо відносин між урядом та спецслужбами, може бути важко зробити висновок, чи є ці правила та процедури інструментами примусової влади чи вони обумовлюють інституційну владу. Однак ми вважаємо, що більшість із цих установ законодавчо пов'язані з державою і діють суворо за її розпорядженням, і тому їх слід розглядати в режимі примусової влади, навіть якщо їм надається оперативна широта самостійних дій.

Проте, оскільки кібербезпека — це не лише питання захисту національних активів від загроз, це також не лише відповідальність військових, розвідки чи правоохоронних органів. Уряд, організації всіх секторів, громадськість та міжнародні партнери також мають свою роль у забезпеченні кібербезпеки. Тому у контексті інституційної влади необхідно розробляти та реалізовувати програми, що спрямовані на впровадження змін у поведінці та робочій культурі, які вимагає наша залежність від кіберсередовища, насамперед у публічному секторі.

Однією із специфічних сфер, в якій зміна культури сприймається як необхідна, є захист інформації. У цьому також ми бачимо функціонування інституційної влади через посередників, завданням яких є частково змінити поведінку не лише техніків та фахівців з інформаційної безпеки, але й державних службовців та компаній щодо забезпечення безпечного проходження та зберігання економічно та політично конфіденційних дані.

Структурна влада. На відміну від інституційної влади, яка спирається на існуючі соціальні відносини, структурна влада стосується того, як взаємно створюються відносини між суб'єктами. Структури, в цьому сенсі, є співконститутивними, внутрішніми відносинами структурних позицій, класичним прикладом яких є, наприклад, відносини господар-раб і капітал-праця, в яких "соціальні відносини, суб'єктивність та інтереси суб'єктів безпосередньо формуються із зайнятих ними соціальних позицій" [1, с. 52—53]. Важливо, що структурна влада може замаскувати визнання акторами своїх структурних позицій по відношенню до інших, так що вони стануть готовими "прийняти свою роль у існуючому порядку речей" [1, с. 53]. Таким чином, структурна влада може формувати поведінку та можливості, навіть коли даний суб'єкт не активно прагне здійснювати контроль над іншим прямими (примусовими) або опосередкованими (інституційними) засобами.

У кібербезпеці більшості сучасних держав дифузна структурна сила пронизує соціальні відносини. Одним із прикладів є взаємозв'язок між урядом та промисловістю, який відтворюється та модифікується заборонами політики кібербезпеки та практикою, яку вона пропагує. Зараз звичним є те, що в умовах ринкової економіки переважна частка критично важливих інфраструктур, на які покладається національна безпека та економічне здоров'я, насправді належить приватному сектору та управляється ним. Історично це є результатом дерегуляції та приватизації державного сектору, які передали націоналізовані галузі в руки приватних компаній та їх акціонерів. Ситуація ускладнюється глобалізацією капіталу таким чином, що критично важлива інфраструктура в одній країні може контролюватися або належати компанії в іншій, а на неї впливають відмови в третій. Це створює численні проблеми для урядів. По-перше, уряд не може забезпечити безпеку критично важливих інфраструктур самостійно. По-друге, уряд повинен знайти способи стимулювання приватного сектору забезпечити цю безпеку. По-третє, уряд повинен збалансувати переваги можливого втручання в критично важливу інфраструктуру та її дефіцит, особливо в умовах, що не допускають регулювання. По-четверте, уряду, можливо, доведеться покладатися на галузеві навички та досвід для захисту державних мереж, оскільки надання та обслуговування інформаційно-комунікаційних технологій, як правило, передається в приватний сектор.

Найкращим рішенням у такій ситуації стає публічно-приватне партнерство (далі — ППП), у рамках якого публічний та приватний сектор працюють у партнерстві для досягнення стратегічних результатів. Результатами такого партнерства може бути обмін розвідданими, плани безперервності бізнесу, регуляторні питання, взаємні поради, навички та досвід, спільні стратегії дій, дослідження та розробки, інновації та інвестиції, управління ризиками, найкращі практики тощо. ППП можуть приймати різні форми, але ми пропонуємо використовувати типологію, розроблену Ліндером, яка передбачає, що кожне різне використання ППП як поняття "посилається на певні передумови щодо того, які відповідні проблеми слід вирішити та як само їх вирішити" [3, с. 42].

Продуктивна влада стосується "систем виявлення та визначення мереж соціальних сил, що постійно форму-

ють одна одну" [1, с. 55]. У той час як структурна влада працює через бінарні відносини, які служать для розширення можливостей тих, хто має структурні переваги, та позбавлення можливостей тих, хто таких переваг не має, продуктивна влада пов'язана з дифузними та непередбачуваними соціальними процесами, які виробляють певні види суб'єктів, фіксованими значеннями та категоріями, та створює те, що береться як само собою зрозуміле і звичайне у світовій політиці [1, с. 57]. Дискурс, а не структура, створює ідентичність та спроможність соціальних суб'єктів.

Із зростаючою залежністю від інформаційно-комунікаційних технологій також виникає більша кількість нових загроз і ризиків. Так, існують технічні проблеми, як-от: системні помилки, властиві технологічним системам, які, можливо, спричиняють каскадні збої в інших системах через їх взаємозв'язок та взаємозалежність. Існують також соціальні загрози та ризики, які походять від людських акторів, які бажають завдати шкоди як самим фізичним системам, так і тим практикам та процесам, які залежать від них. Отже, технічне та соціальне глибоко переплітаються, але у стратегії кібербезпеки, на наш погляд, слід надавати соціальним агентам пріоритет над технічними аспектами, хоча не завжди приписувати людську діяльність як причину "розладу" інфраструктури.

Цього можна очікувати: в той час як захисні заходи, такі як інформаційна безпека та управлінські процеси, такі як забезпечення інформації, є давно встановленою оперативною практикою, характер та еволюція образливих загроз державним інтересам, зрозуміло, представляють більший інтерес для стратегічних планувальників, які мислять не лише у категоріях безпосередньої підтримки цілісності мереж та інформації. Адже дуже важливим є виявлення потенційних або фактичних зловмисників для розробки загальних та спеціальних контрзаходів. Їх можна розуміти як акторів, що діють на місцях, акторів, які впливають на динаміку даної сфери, як функціональних суб'єктів. Функціональний суб'єкт — це той, хто суттєво впливає на рішення у сфері безпеки, але насправді не відповідає за формулювання політики безпеки. Крім того, функціональних суб'єктів можна розрізнити на "внутрішніх", тих, хто є частиною спільнот, що формують безпекову політику, та "зовнішніх" суб'єктів, які повністю розташовані за межами цих спільнот. У цьому сенсі можна визначити чотири типи зовнішніх функціональних суб'єктів, які вже згадувались вище: держави, державні довірені особи, злочинці, терористи. П'ята категорія, інсайдери, стирає різницю між внутрішніми та зовнішніми суб'єктами.

ВИСНОВКИ З ПРОВЕДЕНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ЦЬОМУ НАПРЯМІ

Таким чином, розглядаючи кібербезпеку в кожній з чотирьох категорій влади, визнаємо, що вони не обов'язково взаємовиключні. З цієї точки зору примусова влада стосовно кібербезпеки надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кібербезпекою.

Зовнішні суб'єкти кіберзагрози поділяються на державні та недержавні, при цьому держави представляють найскладнішу загрозу. Держави та довірені особи можуть співпрацювати, і може існувати суттєве перетинання між терористами та довіреними особами. Протистояти діяльності цих суб'єктів можливо лише через співпрацю акторів всіх трьох секторів, на чому вже неодноразово наголошувалось, і на чому грунтується продуктивна влада.

Вирішальним моментом цієї форми влади є те, що контроль над інформацією свідомо обмежується членами елітних спільнот знань. Дискурс контролюється цими спільнотами для своїх цілей та слугує їхнім власним інтересам, фактично закриваючи дискурсивний простір для тих, хто є зовнішнім для цих спільнот. Такі документи, як стратегії кібербезпеки, можуть відкрито заявляти про свій контроль над інформацією, посилаючись на оперативні причини та причини національної безпеки. А там, де пропонується місце для розбіжностей та дискусій, наприклад, у парламенті, воно використовується лише для запитань механіки кібербезпеки, а не її принципів чи необхідності.

Тобто продуктивна влада працює над побудовою "іншого", тим самим виправдовуючи розширені функціональні можливості та витрати кібербезпеки. Будь-яка емпірична основа для прийняття рішень не повідомляється громадськості і, натомість, залежить від дискурсивної конструкції суб'єктів, приписування значення цим суб'єктам, а також заходів та дій, які пропонуються для боротьби з ними.

Література:

1. Barnett, Michael, and Raymond Duvall (2005). Power in International Politics, International Organization, vol. 59 (2), pp. 39—75.

2. Cabinet Office (2009a). The National Security Strategy of the United Kingdom: Update 2009: Security for the Next Generation, Cm. 7590, June 2009 (Norwich: The Stationery Office); [Електронний ресурс]. — Режим доступу: http://www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf (дата звернення 31.03.2021).

3. Linder, Stephen H. (1999), Coming to Terms with the Public-Private Partnership: A Grammar of Multiple Meanings, American Behavioural Scientist, vol. 43 (1), pp. 35—51.

References:

1. Barnett, M. and Raymond, D. (2005), "Power in International Politics", International Organization, vol. 59 (2), pp. 39—75.

2. Cabinet Office (2009), "The National Security Strategy of the United Kingdom: Update 2009: Security for the Next Generation, Cm. 7590, June 2009 (Norwich: The Stationery Office)", available at: http://www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf (Accessed 31 March 2021).

3. Linder, S. H. (1999), "Coming to Terms with the Public-Private Partnership: A Grammar of Multiple Meanings", American Behavioural Scientist, vol. 43 (1), pp. 35—51.

Стаття надійшла до редакції 26.05.2021 р.