УДК 351.865

[https://doi.org/10.52058/2708-7530-2021-6\(12\)-39-52](https://doi.org/10.52058/2708-7530-2021-6(12)-39-52)

Котух Євген Володимирович кандидат технічних наук, доцент кафедри комп'ютерних наук, Сумський Державний Університет, просп. Московський, 75, кім. 4, м. Харків, 61001, тел.: (050) 338-26-93, yevgenkotukh@gmail.com, <https://orcid.org/0000-0003-4997-620X>

ТЕОРЕТИКО-МЕТОДОЛОГІЧНА МОДЕЛЬ РОЗРОБКИ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

Анотація. Концепція розділеного, визначеного, організованого та контрольованого кіберпростору суперечить тому, як більшість людей сприймає Інтернет. Це не далекий, малонаселений регіон країни, а також не ізольована нічия земля. Кордон кіберпростору – це мережа мільярдів систем практично в усіх частинах світу, в якій є рівна кількість різноманітних учасників. Експоненціальне прискорення технологічної еволюції та інновації в ній сформували середовище, в якому агресорам вдається випередити оборонні стратегії та системи.

У статті розглянуто теорії, які лежать в основі побудови національної стратегії кібербезпеки – неореалізм, теорії соціального конструктивізму та інтерсекційності, а також кібервестфаліанство. Доведено, що теоретико-методологічна основа розробки національних стратегій кібербезпеки має ґрунтуватись на інтегративному підході, що містить елементи всіх зазначених вище теорій.

Те, як громадяни сприймають роль свого уряду в кіберпросторі, суттєво відрізняється від держави до держави. Ці елементи національного менталітету можуть також перешкоджати переходу до вестфальського Інтернету. Тому хоча кібервестфальська теорія дійсно підходить до загроз кібербезпеки з технічної точки зору, вона не враховує міжнародну кібердинаміку, а також соціальні та політичні норми людей. І тому ми знов повертаємось до необхідності використання інтегрованого підходу до забезпечення кібербезпеки, який би об'єднав кращі аспекти всіх розглянутих вище теоретичних підходів. Інтегровану теоретико-методологічну модель розробки національної стратегії кібербезпеки, що пропонується.

Запропонована автором модель створює теоретико-методологічну основу для розробки національної стратегії кібербезпеки, що враховує різні її аспекти. Проте для забезпечення дієвості та ефективності даної стратегії необхідно розглянути кіберпростір не лише з точки зору наявних у ньому акторів, як це зроблено у запропонованій моделі, а ще і як своєрідний домен влади, здатний впливати на різні сфери суспільної життєдіяльності.

Ключові слова: кібербезпека, кіберпростір, модель, національна стратегія кібербезпеки.

Kotukh Yevhen Volodymyrovych Candidate of Technical Sciences, Associate Professor of Computer Sciences Department, Sumy State University, Moscow Ave., 75, room 4, Kharkiv, 61001, tel.: (050) 338-26-93, yevgenkotukh@gmail.com, <https://orcid.org/0000-0003-4997-620X>

THEORETICAL AND METHODOLOGICAL MODEL OF NATIONAL CYBERSECURITY STRATEGY DEVELOPING

Abstract. The concept of divided, defined, organized and controlled cyberspace contradicts how most people perceive the Internet. This is not a remote, sparsely populated region of the country, nor isolated land. The border of cyberspace is a network of billions of systems in almost all parts of the world, in which there is an equal number of different participants. The exponential acceleration of technological evolution and innovation in it has created an environment in which aggressors manage to stay ahead of defense strategies and systems.

The article considers the theories that underlie the construction of a national strategy for cybersecurity – neorealism, theories of social constructivism and intersectionality, as well as cyber westphalian theory. It is proved that the theoretical and methodological basis for the national cybersecurity strategies development should be based on an integrative approach that contains elements of all above theories.

How citizens perceive the role of their government in cyberspace differs significantly from state to state. These national mentality elements can also hinder the transition to the Westphalian Internet. Therefore, although cyberwestphal theory does approach cybersecurity threats from a technical point of view, it does not take into account international cyberdynamics as well as social and political norms. Therefore, we return to the need to use an integrated approach to cybersecurity, which would combine the best aspects of all the theoretical approaches discussed above – an integrated theoretical and methodological model for developing a national cybersecurity strategy.

The model proposed by the author creates a theoretical and methodological basis for the development of a national cybersecurity strategy that takes into account its various aspects. However, to ensure the effectiveness and efficiency of this strategy, it is necessary to consider cyberspace not only in terms of its actors, as done in the proposed model, but also as a kind of domain of power that can influence various spheres of public life.

Keywords: cybersecurity, cyberspace, model, national cybersecurity strategy.

Постановка проблеми. Поки національні уряди борються із зростаючою кількістю широкомасштабних прихованих та публічних актів кібервійни, кіберзлочинності та кібершпигунства, науковці також не стоять осторонь цієї проблеми, адже стратегії національної безпеки, спрямовані на припинення хвилі цих атак, стають дедалі менш ефективними. Однією з

можливих причин цього може бути розрив зв'язку між традиційними теоріями безпеки, які базуються на реальних реакціях на кінетичні загрози, та набагато іншим та складним середовищем кіберпростору. Але дотримання принципів традиційних теорій безпеки, застосовування їх до кіберпростору, часто важке або навіть неможливе.

Уряди, схоже, мають більшу стурбованість цілісністю своєї інформації ніж приватні компанії, головним чином через залежність сучасного суспільства від неї. Однак уряди також регулярно винні у короткозорості, коли справа стосується кіберстратегій, їх реалізації та адміністрування. Національна кібербезпека часто непропорційно будується на макрорівні. Це, як правило, спрощує захист лише для стратегічних дій, які можуть бути реалізовані в широкому, послідовному спектрі. Саме цей широкий спектр обмежує органам влади сферу цих загроз лише охопленням конкуруючих держав або великих ворожих груп. Відповідно, держави спрямовують свої ресурси майже виключно на те, що цілком може бути для них великою загрозою, але, звичайно, не єдиною. При цьому держави часто нехтують альтернативними рішеннями.

Аналіз останніх досліджень і публікацій. Проблемі кібербезпеки в міжнародному правовому полі присвятили свої роботи Т. Девенпорт, П. Домбровський та К. Демчак вивчали кібервествальство та безпеку, Л. МакКолл та Б. Фітцджеральд розглядали кібербезпеку крізь призму інтерсекціонізму, К. Вальц, М. Вільямс, Й. Еріксон, Дж. Мешеймер, Н. Онуф присвятили свої роботи міжнародній політиці та безпеці в цифрову епоху, Р. Кларк та Р. Кнейк аналізували проблеми гарантування національної безпеки та ведення кібервійни, О. Вендт розглядав соціальну теорію міжнародної політики.

Мета статті – вироблення теоретико-методологічної основи для розробки національної стратегії кібербезпеки, базуючись на наявних теоріях.

Виклад основного матеріалу. Поступова, але послідовна мілітаризація та централізація управління у сфері національної кібербезпеки часто надає пріоритет безпеці над логістикою, а також тому, як ці дії уряду можуть впливати на поведінку та безпеку своїх громадян. Можливо, чистий негативний ефект ігнорування цих вужчих аспектів кіберстратегій є більшим, ніж загрози, які представляють державні актори або великі міжнародні групи.

Цей шлях до централізації та мілітаризації кібербезпеки посилюється в країнах, які є головними об'єктами кібератак, таких як США чи країни ЄС. Тому не дивно, що в цих країнах перспективи кібербезпеки та результуючі стратегії найбільше нагадують перспективи неореалізму. З точки зору неореалізму, рівень аналізу зосереджений на державах, а влада та безпека розглядаються як функції відносної вигоди від конкуруючих суперників. Це видається найбільш логічним, оскільки напади державних утворень є реальними, найбільш очевидними та представляють серйозну небезпеку для національної безпеки. Однак, як загальна кіберстратегія, неореалізм не розпізнає загрози та можливості для більшої цілісності систем, які представляють недержавні актори та технології.

Теорії безпеки, які зосереджені виключно на недержавних суб'єктах, таких як окремі люди та групи, та динаміці влади, якою вони діляться з державами, також недостатньо, щоб охопити всю загрозу кібербезпеці. Групи із спільною ідентичністю та цілями часто розглядають кіберпростір та баланс сил лише в контексті цих спільних норм. Ця ідея має тенденцію до зіткнення з цілями національної безпеки, що забезпечує верховенство держави над побудованими ідентичностями індивідів та колективів. Тим не менше, теорії соціальної конструктивістської безпеки вміють аналізувати спільне сприйняття як всередині, так і поза суспільством, і вміють розпізнавати як функцію ідентичності в динаміці національної безпеки, так і те, як ці сприйняття впливають на безпеку. Однак реалізувати цілком соціальну конструктивістську стратегію національної безпеки в середині зони кібервійни не є ані практичним, ані здійсненним. За таких умов існує необхідність координації кібербезпеки та звичайних стратегій та планів безпеки.

Однак неореалістичний та соціально-конструктивістський підходи до кібербезпеки поділяють подібну проблему. Вони обидва розроблені як інтерпретації традиційної міжнародної безпеки, і по суті, жоден з них не включає інформаційні технології значною мірою, що є самою суттю кібербезпеки. Однак існує дедалі більша спільнота дослідників питань безпеки, які намагаються встановити кібербезпеку в основному в цифровому, а не кінетичному вимірах. Серед цих теорій найбільш помітною є теорія «кібервестфальської» системи. Ця теорія базується на розвитку можливих або ймовірних майбутніх технологій, і стверджує, що державна централізація Інтернету в багатьох країнах, спільно з розвитком цих майбутніх технологій, приведе до появи національних «кібермеж». Дана теорія розглядає такі важливі аспекти кібербезпеки, як технології, міжнародні аспекти кіберсередовища, а також як державних, так і недержавних акторів. Однак ця теорія не приділяє уваги ролі, яку відіграють чи можуть відігравати окремі громадяни та їх поведінці у кіберпросторі. Нехтування включенням цих суб'єктів у розгляд не дає можливості визначити переваги, які вони можуть принести національній кібербезпеці, й ігнорує нездійснення секвестру в Інтернеті активності людей у демократичному суспільстві. Кібервестфаліанство також дещо обмежене за своїм обсягом (кіберпростір) та підходом до рішень (технологія). Воно також не враховує економічну, політичну та військову динаміку між великими, середніми та регіональними державами. З цих причин ця теорія також є недостатньою перспективою, з якої можна сформувати методологічну основу для національної стратегії кібербезпеки.

Усунути ці проблеми може певним чином теорія інтерсекційності, якщо її застосувати до кібербезпеки. Тому, на наш погляд, теоретико-методологічна основа розробки національних стратегій кібербезпеки має ґрунтуватись на інтегративному підході, що містить елементи інтерсекційності, неореалізму, соціального конструктивізму та кібервестфаліанства. Розглянемо докладніше унікальні та застосовні аспекти

цих теорій.

Інтерсекційність. Вперше визначена К. Креншоу в 1989 році для пояснення расових відхилень у фемінізмі, теорія інтерсекційності пояснює проблеми з точки зору перетину окремих факторів [1]. Згодом ідеї цієї теорії були розширені для вирішення інших питань соціальних наук [2, с. 1790].

Ця теорія стверджує, що такі проблеми, як соціальна несправедливість, породжуються не лише одним аспектом, подією чи системою, скоріше вони є результатом зближення чи перетину численних факторів на різних рівнях та з різних середовищ, що вимагають проведення різних типів аналізу. Нещодавно цю теорію застосували до галузі кібербезпеки такі вчені, як Бен Фіцджеральд та Тара Девенпорт [3, 4]. З цієї точки зору проблеми в кібербезпеці не розглядаються як виключно політичні, соціальні чи технічні, а є перетином усіх трьох факторів.

Саме ці «правильні набори перехресть», можливо, мали місце протягом останніх п'ятнадцяти років під час великих кібератак. У політичному плані багато державних керівників обирали внутрішню політику шифрування, яка здавалася обґрунтованою та сприяла національній безпеці. Така політика може бути розглянута в контексті політичної науки, де досліджуються політична мотивація, політика влади та законодавчі фактори. Як варіант, аналіз згаданої політики можна розглядати через приціл неореалізму. Такий підхід розглядав би втрату або виграш відносної сили певної держави через її національну політику щодо публічних ключів. Кібервестфальці також можуть розглядати це як захисний механізм, який служить типом кіберкордону.

Цілком на іншому рівні проблему можна вивчати як функцію групової чи культурної ідентичності кінцевих користувачів або кіберзлочинців або обох цих груп. Багато хто вирішив розглядати будь-яку проблему, пов'язану з кібербезпекою, як технічну проблему, і вважають, що відповідь знаходиться в технологіях. Усі ці підходи, події та актори перетинаються між собою в різних точках на часовій шкалі, що, на наш погляд, сприяє проясненню проблем кібербезпеки та їх вирішенню.

К. Креншоу визначає проблему особливого аналізу, який розділяє соціальну несправедливість на різні виклики, що стоять перед певними групами (раса, стать, сексуальна орієнтація або соціально-економічний статус) [1, с. 158]. Окремо ці аналізи пропускають загальну картину, створюючи конкуренцію та розподіл між проблемами та розриви у перспективах, які затуманюють важливі проблеми. Аналогічно аналіз кібератак може припустити, що вони були просто проблемою поганої безпеки мережі або неминучим результатом цілеспрямованого хакерського злому. І хоча кібербезпека та соціальна справедливість є помітно різними сферами, але основне розуміння інтерсекційності справедливо для обох.

Сфера кібербезпеки, на наш погляд, має вийти за межі дискусій щодо того, чи основне питання стосується проблеми А чи проблеми Б, теорії А чи теорії Б. Натомість кібербезпека повинна розуміти взаємозв'язок між усіма

проблемами та використовувати всі відповідні теорії для підходу до цих проблем.

Неореалізм. Неореалістичний погляд на політичні та міжнародні відносини, викладений Кеннетом Вальцом наприкінці 1970-х років, окреслює дії націй як реакцію на структурні обмеження відносної влади [5, с. 218]. Теорія Вальца про відносний баланс сил є досить всебічною для визначення того, як держави взаємодіють одна з одною в міжнародній системі, яка є децентралізованою та анархічною. Тому цілком зрозуміло, чому багато нинішніх науковців з питань кібербезпеки та політиків вважають неореалізм корисним у формуванні стратегії кібербезпеки. Керуючись власним виживанням у міжнародній структурі, держави розвивають свої кібернетичні можливості для того, щоб або збільшити, або захистити свій відносний баланс сил [5, с. 102; 6, с. 13].

Кібербезпека добре вписується в неореалістичну модель з кількох причин. Інтернет за своєю природою є анархічним. Ця децентралізація віртуального простору ускладнює координацію зусиль на міжнародному рівні або повсюдне запровадження міжнародного законодавства. Це дозволяє застосовувати стратегії кібербезпеки, які є менш загальними, відтак, краще пристосованими до особливостей окремих держав.

Однак існують потенційні підводні камені в тому, щоб розглядати кібербезпеку суворо з неореалістичної точки зору. По-перше, єдиним рівнем аналізу тут є держави та національні інтереси. Проте багато кібератак часто ініціюються особами з мотивами, що не відповідають національним інтересам та фінансовій вигоді. Хактивістські групи, такі як «Анонім», часто мають політичні програми, не пов'язані з жодним урядом чи державою, і зазвичай проводяться без державної підтримки. Хакери часто координують транскордонну діяльність та соціальні групи для досягнення цілей, які мають мало спільного із співвідношенням сил у міжнародній системі. На відміну від національних військових та інших урядових структур, що використовуються для захисту або збільшення відносного співвідношення сил, доступ до Інтернету не обмежується лише державою. Крім того, суб'єкти, що користуються Інтернетом, які не включені в неореалістичні спостереження (тобто особи, політичні групи та корпорації), також не обов'язково мотивовані інтересами національної безпеки.

По-друге, неореалізм припускає, що держави з найбільшими ресурсами мають найбільшу владу, а отже, вони більш безпечні, ніж держави з меншими ресурсами та меншою відотною владою. Однак великі армії, передові технології та великий ВВП не потрібні для ведення кібервійни. Будь-яка країна може завдати серйозної шкоди, все що для цього потрібно – це комп'ютери з доступом до Інтернет та спеціалізовані особи, які мають досвід для здійснення нападів. І навпаки, висока залежність від Інтернет та складна, комп'ютерно-інтегрована інфраструктура в таких країнах, як США, роблять їх більш вразливими до електронних атак [7, р. 218]. Отже, асиметричний та децентралізований характер кібернетичних можливостей у країнах, що розвиваються, ускладнює адаптацію цілком неореалістичної

філософії до кіберзахисту.

Соціальний конструктивізм. Накопичення особистих даних як кіберзлочинців, так і кінцевих користувачів відіграють важливу роль у забезпеченні кібербезпеки багатьох країн. Однак, вибір такої теоретичної бази, на якій можна інтерпретувати дані кібератак з точки зору окремих суб'єктів був предметом наукових дискусій. Однією з таких теоретичних баз все більше фахівцями з кібербезпеки розглядається зараз соціальний конструктивізм. Конструктивісти, як правило, розглядають Інтернет як провідник для груп людей із спільною регіональною, культурною або нормативною ідентичністю для пропаганди ідеації [8, с. 23]. Зокрема, Ерікссон, Джакомелло та Ранспорт вже писали про те, як на кібератаки впливають побудовані ідентичності [9, с. 181].

Хоча в ній нічого не згадується про кібербезпеку, теорія «сек'юритизації», розроблена «Копенгагенською школою» в рамках конструктивістського підходу, пропонує аналіз політики загроз на основі сприйняття та побудованих ідентичностей. Питання безпеки формуються політичними суб'єктами на основі їх сприйняття загроз. Ці спільні уявлення формуються навколо того, як і коли виникають загрози та з якими наслідками [10, с. 523-526]. На думку «Копенгагенської школи», сприйняття формується за допомогою «мовленнєвих актів», тому її дослідження частково спрямовані на вивчення мови, що використовується для формування загроз. Таким чином, повідомлення, що передують кібератаці якоїсь держави на іншу, можна розглядати як явні урядові «мовленнєві акти», покликані сформулювати уявлення про певну агресивну поведінку. Це дуже корисно при вивченні політичної риторики, яка супроводжує напади. Однак при вивченні кіберзагроз, представлених окремими державними акторами, також потрібна система, більш відповідна колективним діям та поведінці людей у кіберпросторі.

Йохан Ерікссон розвиває концепцію «Копенгагенської школи» на крок далі і пов'язує її з кібербезпекою у своєму дослідженні сек'юритизації ІТ у шведській політиці. Однак замість того, щоб виявити слабкі місця у поведінці шведських ІТ чи шведській політиці щодо ІТ, його аналіз зосереджується на тому, хто винен чи що винно у кіберзагрозах, і як розподіляється відповідальність за боротьбу із ними [11, с. 211-212]. Знову ж таки, мова стає важливою, оскільки відповідальність за «кіберзлочинність» та «кібервійну» підпадає під різні сфери діяльності. Кіберзлочинністю повинна займатися поліція, роблячи злочинців учасниками аналізу.

Аналіз кібератак та того, як їх можна запобігти, спершу слід розпочати з дій людини щодо колективного розуміння Інтернету. Важко було б виправити системні проблеми, переслідуючи окремі події та різні мотивації окремих акторів. Однак вже існують конструктивістські теорії, які зосереджуються на колективізмі з огляду на конкретні кіберподії. Так, Джакомелло описує конструктивістський підхід до міжнародної кібербезпеки, який включає метод нападів [9, с. 18-19]. У своєму аналізі Джакомелло зосереджує увагу на індивідуальному та колективному

сприйнятті всього, що стосується ІТ. Однак він все ще орієнтований на мову і розглядає, як використовуються такі терміни, як «вірус», «шкідливе програмне забезпечення», «помилки», «брандмауери» тощо:

«Використання таких термінів, як «інформаційна війна» та «електронний Перл-Харбор», надає особливого значення: те, що є цифровим за своєю природою, має, однак, фізичні наслідки, порівнянні з наслідками звичайної війни. Конструктивістський аналіз може сприяти виявленню та розумінню значення такої риторики та символічних дій». [9, с. 21].

Хоча, можливо, і дещо заглиблений у терміни та символіку, Джакомелло робить вагомому аргументацію щодо використання конструктивістської системи для вивчення кібератак та їх впливу на міжнародну безпеку. Його аналіз можна винести за межі символізму, включаючи інші види дій, а саме соціальні норми та поведінку в Інтернеті. Наприклад, в Україні індивідуальне та колективне сприйняття кібербезпеки сягає своїм корінням не лише з українського «онлайн-світу», а й із культури та дій «поза Інтернетом».

«Соціальну теорію міжнародної політики» Олександра Вендта, ще одного представника конструктивізму, також можна адаптувати для інкапсуляції кіберзагроз та їх запобігання. Хоча теорія конкретно не стосується кібербезпеки, вона включає як культурні, так і міжнародні аспекти, що переважають під час кібератак останнього десятиріччя. З точки зору Вендта, колективна ідентичність і соціальні норми та практики пов'язані з міжнародною структурою через сприйняття суспільством елементів цієї структури [12, с. 313-336]. Його теорія також добре поєднується з динамікою української культури та суспільства. Спостережувана колективна поведінка може бути використана для пояснення не лише сприйняття Україною безпосередньо зовнішніх кіберзагроз, а й сприйняття їх зв'язку з міжнародною системою безпеки.

О. Вендт визначає колективну ідентичність як колективну ідентифікацію спільних характеристик Я (у нашому випадку українців) від інших (неукраїнців). Вендт стверджує, що помітність колективної ідентичності для окремих людей визначає силу прихильності суспільства до неї [12, с. 230]. Колективна ідентичність створює структури у формі органів влади та корпорацій, які підсилюють ідентичність та поведінку шляхом централізації та інтерналізації [12, с. 219]. Ці самоукріплюючі структури колективної ідентичності проявляються у централізації та інтерналізації норм та поведінки в Інтернет українськими приватними організаціями та органами влади. Вендт також вважає, що участь у громадській діяльності пов'язує людей з подіями та практиками. Ці практики посилюються шляхом інтерналізації. Отже, поведінка, як ідентичність, може бути спільною [12, с. 178].

Зв'язок колективної ідентичності з міжнародною системою безпекою залежить не тільки від структури міжнародної безпеки, але й від того, як ви розглядаєте цілі окремих суб'єктів системи. Для неореалізму це означає анархічну систему з державними суб'єктами, кінцева мета яких є матеріальною (наприклад, економічною, владною, гегемоністською,

військовою тощо). Для неолібералів і конструктивістів це означає структуровану міжнародну систему безпеки також із державними суб'єктами, але метою якої є співпраця задля більшої, стабільнішої колективної винагороди. Вендт стверджує, що науковці повинні думати про зв'язок з міжнародною системою безпеки в соціальному, а не матеріалістичному плані. Навіть анархію можна розбити на певні елементи, які сприймаються як актори (тобто нації, індивіди, суспільство) [12, с. 246-248].

Незважаючи на переконливий опис конструктивістами кібердинаміки, її акторів та зв'язків із міжнародною системою безпеки, важко буде переконати тих, хто знаходиться за межами конструктивізму (особливо тих, що знаходяться в уряді), що кіберінфраструктуру можна адекватно захистити виключно шляхом визнання ідентичності як ідеї. Крім того, конструктивізм не може пояснити технологічні прогалини між кінцевими споживачами та не пояснює, як технологія може вплинути на проблему кібербезпеки та запропонувати відповідні рішення.

Кібервестфальська теорія. Кріс К. Демчак та Пітер Домбровський у своїй роботі «Підйом кібернетичної Вестфалії» [13] стверджують, що відносно некерований кордон кіберпростору, як і всі кордони, не триває вічно, коли задіяні людські суспільства. Врешті-решт національні держави поширяють свій суверенітет на Інтернет і здійснюватимуть контроль над електронною інформацією, яка надходить і виходить до/із їхніх національних доменів. По суті, нації створюватимуть електронні кордони. Демчак і Домбровський наводять останні події в політиці кібербезпеки розвинених країн як свідчення того, що держави вже рухаються до межового Інтернету [13, с. 13]. Тому ця теорія вже визначає певні умови національної кібербезпеки та процес, через який країни створюватимуть кібермежі за допомогою технологій.

Такі країни, як Китай та США, розробляють технології та оборонні стратегії, які б створили кордони в кіберпросторі та дозволили б країнам боротися із загрозами; навіть коли ці загрози надходять від власних громадян. Ці країни вже продемонстрували свою готовність піти в наступ, щоб захистити національні інтереси. Завдяки «кіберкомандуванню» кожної нації військові технологічно розвинених країн вступають у кібервійну, яка виходить за рамки простого шпигунства або вандалізму, оскільки вони прагнуть поширити свою парадигму регіональної та міжнародної безпеки на кіберпростір. Такі дії змусили менш розвинені в технологічному відношенні країни підштовхнути своїх більш розвинених союзників до захисту свого кіберпростору за допомогою традиційних механізмів безпеки та організацій, таких як НАТО та ООН, оскільки кібервестфальська карта починає формуватися [13, с. 7].

Концепція розділеного, визначеного, організованого та контрольованого кіберпростору суперечить тому, як більшість людей сприймає Інтернет. Це не далекий, малонаселений регіон країни, а також не ізольована нічия земля. Кордон кіберпростору – це мережа мільярдів систем практично в усіх

частинах світу, в якій є рівна кількість різноманітних учасників. Експоненціальне прискорення технологічної еволюції та інновації в ній сформували середовище, в якому агресорам вдається випередити оборонні стратегії та системи. Програмне та апаратне забезпечення, призначене для крадіжки інформації, підризу систем, порушення публічної політики та маскування особистості користувача, вільно ділиться між хакерами. Також користувачі комп'ютерів у ліберальних демократіях звикли до свободи, яку надає безмежний кіберпростір. Спроби урядів закрити скриньку Пандори часто зустрічають опір, який виливається на політичну арену і має значний вплив на державну політику. На відміну від фізичного кордону, стримування у віртуальному просторі здається неможливим. Однак Демчак та Домбровські стверджують, що повернення суверенітету через Інтернет є технологічно можливим, психологічно комфортним і системно та політично керованим.

Демчак і Домбровський стверджують, що нова карта кіберпростору, укомплектована межами та кордонами, які приймають усі держави, є неминучою. Початок цього з різним ступенем вже можна побачити в таких країнах, як США, Китай, Південна Корея та країни ЄС. [13, с. 22]. Однак вивчення не лише кібервійськової політики цих держав, але також їх державної та комерційної політики в Інтернеті виявляє, що ліберально-демократичним країнам буде важко здійснювати та застосовувати навіть багато основних обмежувальних кіберполітик. Крім того, створення кіберкордонів залежить від розподілу віртуального простору за допомогою технологій та національних державних стандартів.

Технології, що забезпечують кордони в кіберпросторі, повинні мати можливість сканувати всю інформацію, що надходить через його мережі, з метою виявлення шкідливих або незаконних кодів, розмежування національного та міжнародного вмісту, а також виявлення та визначення місцезнаходження їх джерел. Загальноприйнята думка полягає в тому, що такі заходи безпеки просто неможливі, і що жодна оборона не є непроникною. Незалежно від того, яку стратегію оборони або технології можуть розробити держави, надавши достатньо часу, кожна система може бути зламана [14]. Сучасна технологія не може сканувати всі вхідні дані, щоб визначити їх національне походження та потенціал загрози, а також сучасні криміналістичні методи не завжди можуть відстежувати джерело зламу та особу хакера. Утім, Демчак і Домбровський сперечаються проти цього [13, с. 2].

Те, як громадяни сприймають роль свого уряду в кіберпросторі, суттєво відрізняється від держави до держави. Ці елементи національного менталітету можуть також перешкоджати переходу до вестфальського Інтернету.

Наприклад, у Китаї уряд відчув дуже малий опір своїй обмежувальній політиці в Інтернеті. Починаючи з середини 1990-х років, послідовні нормативні акти все більше обмежували те, що громадяни Китаю можуть говорити або отримувати доступ до Інтернету. Це призвело до створення розділу п'ятого «Положень комп'ютерної інформаційної мережі та Інтернет»,

що стосуються безпеки, захисту та управління, затвердженого Державною радою 11 грудня 1997 р. Цей закон передбачає кримінальну відповідальність за використання Інтернет для створення, тиражування, отримання чи передачі будь-чого, що підбурює не лише до злочинних та зрадницьких дій, але до всього, що завдає шкоди національному об'єднанню та пропагуванню неправди, пороків та наклепів [15]. На додаток до цензури урядової критики в Інтернеті, багато комерційних та соціальних мереж, таких як Google та Facebook, заборонені та замінені їхніми внутрішніми аналогами.

Існують і ті країни, які прагнули контролювати потік певної чутливої зовнішньої та внутрішньої інформації лише для того, щоб виявити, що їх зусилля підриваються громадянами, які не бажають відповідати державним стандартам. Найкращий приклад цього – «Арабська весна». Незважаючи на заборону соціальних мереж та зовнішніх сайтів ЗМІ, громадяни Тунісу, Єгипту, Лівії, Ємену, Сирії та Бахрейну змогли використовувати заборонені сайти для організації протестних рухів, розповсюдження цензурованої інформації та врешті-решт змінити багато з правлячих режимів у цих країнах.

З огляду на характер громадянського суспільства в ліберальних демократіях, непевно, що кіберкордони також можуть бути політично керованими. У деяких суспільствах свобода слова витісняє питання кібербезпеки всередині політики. Для цих країн кіберкордони не є політично керованими. Крім того, демократичний процес у багатьох країнах часто перешкоджає формуванню політичного консенсусу, необхідного для прискорення нової кіберполітики. Швидкість технологічного розвитку, порівняно зі швидкістю формування політики, також надзвичайно ускладнює урядам формування адекватного законодавства щодо ІТ-технологій.

Тому хоча кібервестфальська теорія дійсно підходить до загроз кібербезпеки з технічної точки зору, вона не враховує міжнародну кібердинаміку, а також соціальні та політичні норми людей. І тому ми знов повертаємось до необхідності використання інтегрованого підходу до забезпечення кібербезпеки, який би об'єднав кращі аспекти всіх розглянутих вище теоретичних підходів. Інтегровану теоретико-методологічну модель розробки національної стратегії кібербезпеки, що пропонується, наведено на рис. 1.

Рис. 1. Теоретико-методологічна модель розробки національної стратегії кібербезпеки

Відповідно до запропонованої моделі актори у кіберпросторі (державні актори, недержавні актори, кінцеві користувачі та кіберзлочинці) здійснюють дії (проводять політику, сліднують політиці, атакують, захищаються від нападів, отримують і передають інформацію, здійснюють комунікацію, використовують ІКТ для роботи й у побуті тощо), які перетинаються з різними аспектами кіберпростору та кібербезпеки (політичними, соціальними, культурними, технологічними) та породжують явища кібербезпеки, такі як вразливості, цілісність системи, шкідлива поведінка, ідентичність, мотивація тощо.

Державні та недержавні актори, конкуренція за відносні вигоди та політичні аспекти кібербезпеки вимагають неореалістичного підходу до її забезпечення і формулювання відповідних положень стратегії кібербезпеки. У той же час, інтерсекційність дозволяє врахувати у стратегії кібербезпеки соціальні аспекти, зокрема, такі як рівність і справедливість у кіберпросторі,

адже ці фактори часто становлять причини злочинної групової поведінки у кіберсередовищі. Кінцеві користувачі, кіберзлочинці та їх поведінка є продуктом їхньої ідентичності як представників певного національного культурного середовища, так і користувачів Інтернет. Врахувати культурні аспекти кібербезпеки допоможе соціальний конструктивізм. Нарешті, кібервестфалізм дозволяє врахувати у стратегії кібербезпеки сучасні технологічні аспекти та їхній вплив на інші аспекти кіберпростору та кібербезпеки.

Висновки. Таким чином, запропонована модель створює теоретико-методологічну основу для розробки національної стратегії кібербезпеки, що враховує різні її аспекти. Проте для забезпечення дієвості та ефективності даної стратегії необхідно розглянути кіберпростір не лише з точки зору наявних у ньому акторів, як це зроблено у запропонованій моделі, а ще і як своєрідний домен влади, здатний впливати на різні сфери суспільної життєдіяльності.

Література:

1. Crenshaw, Kimberle (1989). *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine*. Feminist Theory and Antiracist Politics. University of Chicago Legal Forum.
2. McCall, Leslie (2005). *The Complexity of Intersectionality*. Signs: Journal of Women in Culture and Society 30, No. 3. P. 1771-800. doi:10.1086/426800.
3. Davenport, Tara (2015). *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*. Catholic University Journal of Law and Technology, No 24.
4. FitzGerald, Ben (May 17, 2015). *The Theory of Intersectionality Can Make Cybersecurity Collaboration Real*. TechCrunch. Retrieved from <http://techcrunch.com/2015/02/17/the-theory-of-intersectionality-can-make-cybersecurity-collaboration-real/>
5. Waltz, Kenneth N. (1979). *Theory of International Politics*. Reading, MA: Addison-Wesley Pub.
6. Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: Norton, 2001.
7. Clarke, Richard A., and Robert K. Knake (2010). *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco.
8. Onuf, Nicholas (2012). *Worlds of Our Making: The Strange Career of Constructivism in International Relations* in Donald J. Puchala, ed., *Visions of International Relations*.
9. Eriksson, Johan, and Giampiero Giacomello (2007). *International Relations and Security in the Digital Age*. London: Routledge.
10. Williams, Michael C. (2014). *Words, Images, Enemies: Securitization and International Politics*. Int Studies Q International Studies Quarterly 47, No. 4. P. 511-531. doi:10.1046/j.0020- 8833.2003.00277.x.
11. Eriksson, Johan (2001). *Threat Politics: New Perspectives on Security, Risk, and Crisis Management*. Aldershot, Hants, England: Ashgate.
12. Wendt, Alexander (1999). *Social Theory of International Politics*. Cambridge: University Press.
13. Demchak, Chris, and Peter Dombrowski (March 2011). *Rise of a Cybered Westphalian Age*. Strategic Studies Quarterly.
14. *Defending Cyber Borders: Beyond the Virtual Maginot Line* (October 25, 2012). Cisco Systems. Retrieved from https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/campusconnection120512maginot.pdf
15. Information Audit and Control Association (ISACA): *Cybersecurity Fundamentals Glossary*. Retrieved from <https://www.isaca.org/resources/glossary>

References:

1. Crenshaw, Kimberle (1989). *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine*. Feminist Theory and Antiracist Politics. University of Chicago Legal Forum.
2. McCall, Leslie (2005). *The Complexity of Intersectionality*. Signs: Journal of Women in Culture and Society 30, No. 3. P. 1771-800. doi:10.1086/426800.
3. Davenport, Tara (2015). *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*. Catholic University Journal of Law and Technology, No 24.
4. FitzGerald, Ben (May 17, 2015). *The Theory of Intersectionality Can Make Cybersecurity Collaboration Real*. TechCrunch. Retrieved from <http://techcrunch.com/2015/02/17/the-theory-of-intersectionality-can-make-cybersecurity-collaboration-real/>
5. Waltz, Kenneth N. (1979). *Theory of International Politics*. Reading, MA: Addison-Wesley Pub.
6. Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: Norton, 2001.
7. Clarke, Richard A., and Robert K. Knake (2010). *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco.
8. Onuf, Nicholas (2012). *Worlds of Our Making: The Strange Career of Constructivism in International Relations* in Donald J. Puchala, ed., *Visions of International Relations*.
9. Eriksson, Johan, and Giampiero Giacomello (2007). *International Relations and Security in the Digital Age*. London: Routledge.
10. Williams, Michael C. (2014). *Words, Images, Enemies: Securitization and International Politics*. Int Studies Q International Studies Quarterly 47, No. 4. P. 511-531. doi:10.1046/j.0020- 8833.2003.00277.x.
11. Eriksson, Johan (2001). *Threat Politics: New Perspectives on Security, Risk, and Crisis Management*. Aldershot, Hants, England: Ashgate.
12. Wendt, Alexander (1999). *Social Theory of International Politics*. Cambridge: University Press.
13. Demchak, Chris, and Peter Dombrowski (March 2011). *Rise of a Cybered Westphalian Age*. Strategic Studies Quarterly.
14. *Defending Cyber Borders: Beyond the Virtual Maginot Line* (October 25, 2012). Cisco Systems. Retrieved from https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/campusconnection120512maginot.pdf
15. Information Audit and Control Association (ISACA): *Cybersecurity Fundamentals Glossary*. Retrieved from <https://www.isaca.org/resources/glossary>