***Ободяк Віктор Корнелійович,***
*к.т.н., доц.,*
*доцент кафедри комп'ютерних наук,*
*Сумський державний університет,*
*м. Суми*
*ORCID 0000-0002-8539-1252;*

***Котух Євген Володимирович,***
*к.т.н,*
*доцент кафедри комп'ютерних наук,*
*Сумський державний університет,*
*м. Суми*
*ORCID 0000-0003-4997-620X*

**УДК 351.865** **doi: 10.34213/tp.20.04.05**

# ОСНОВНІ ВИКЛИКИ УРЯДУВАННЯ У СФЕРІ КІБЕРБЕЗПЕКИ

Проаналізовано характеристики урядування у сфері кібербезпеки, виявлено низку проблем, які суттєво ускладнюють урядування ("безкоштовне використання", відносні вигоди, шахрайство).

**Ключові слова:** кібербезпека, кіберпростір, урядування, міжнародна співпраця.

**Постановка проблеми.** Інформаційні та комунікаційні технології стрімко розвиваються, посилюючи свій вплив на всі ключові сфери суспільного життя. Інтернет та інші елементи кіберпростору утвердилися як невід'ємна частина економічного, політичного, соціального, безпекового секторів переважної більшості країн світу. У той же час транскордонний характер кіберпростору, його залежність від складних інформаційних технологій, активне використання майданчиків і сервісів кіберпростору всіма країнами глобалізованого світу не тільки надають нові можливості, але і продукують нові загрози для національної безпеки країни.

**Аналіз останніх досліджень і публікацій.** Проблемам влади та протистоянь у кіберпросторі присвятили свої роботи С. Гейкен, Р. Кларк, Р. Кнейк, Ш. Харріс. На питання кібербезпеки звертають увагу Ч. Білло, А. Клаймбург, К. Лорд, Т. Томас, В. Чанг, Т. Шарп. Різними аспектами врядування опікувались такі вчені, як Р. Аксельрод, Л. Бигрейв, Дж. Біг, Дж. Матисон, М. Ослон, К. Оффе, П. Самуельсон. Проте як саме співвідносяться врядування, влада та безпека у кіберпросторі, які існують проблеми в реалізації врядування у сфері кібербезпеки поки що залишається поза увагою науковців.

**Метою статті** є виокремлення та аналіз проблем, які суттєво ускладнюють врядування у сфері кібербезпеки.

**Виклад основного матеріалу.** Міжнародна співпраця конче необхідна для забезпечення кібербезпеки, оскільки навіть найбільш дієздатна держава не може сподіватися самостійно передбачити та відбити всі кібератаки. Співпраця може здійснюватися на разовій або системній основі. Останнє, на наш погляд, найкраще здатне забезпечити врядування. К. Оффе пропонує відрізняти врядування від управління ієрархічними та ринковими структурами [21]. Цей термін також застосовується до діяльності так званих багатосторонніх структур, які забезпечують механізми співпраці різних публічних і приватних акторів [3; 19]. Відповідно до такого розуміння врядування у сфері кібербезпеки включає в себе добровільні спільні зусилля публічних і приватних акторів із забезпечення доступності, автентичності, цілісності та конфі-

денційності цифрових даних, що зберігаються в кіберпросторі або переданих через нього.

Існують деякі характеристики врядування у сфері кібербезпеки, які можуть як посилювати зазначене вище співробітництво, так і загрожувати йому. Серед цих характеристик найбільш важливими є такі:

1. Практично всі можливості для атаки або захисту в кіберпросторі залежать від знання про уразливість [8, p. 54; 17, p. 16]. Як правило, ці вразливості складаються з невідомих властивостей комп'ютерного коду. Але з тим же успіхом вони можуть стосуватися і людей або організацій, схильних до атак соціальної інженерії. В обох випадках саме знання, а не матеріальні можливості, дають здатність протистояти загрозам у кіберпросторі. Однак поширення та використання знань набагато важче виявити і, отже, регулювати, ніж поширення або використання матеріальних можливостей.

2. Оскільки знання є основним ресурсом у сфері кібербезпеки, у цій сфері спостерігається тенденція до зменшення асиметрії влади. Існує безліч суб'єктів, здатних здобувати знання і, відповідно, завдавати серйозної шкоди в кіберпросторі. Крім того, географічне розміщення цих суб'єктів не має значення для більшості операцій. З цих двох причин співпраця з цими суб'єктами або проти них повинна бути всеосяжною. Отже, досягнення домовленостей утруднено. Це також більш ризиковано, ураховуючи той факт, що обмін інформацією може здійснюватися нескінченно. У цьому відношенні управління кібербезпекою структурно дуже схоже на співпрацю в галузі розвідки [6].

3. Наявні та чинні кодекси в кіберпросторі явно не сприяють відповідальності за інциденти. Так заохочується порушення правил і, відповідно, не заохочується дотримання їх. Можлива також і неправильна атрибуція, за якої треті сторони будуть проводити операції "під фальшивим прапором" і, таким чином, спричиняти взаємні звинувачення "всіх проти всіх". Отже, quid pro quo як основний принцип встановлення та стабілізації співробітництва [1] не працює добре в кіберпросторі.

4. Феномени, що відрізняються у фізичному світі, такі як злочинність, війна та інтелект, як правило, досить схожі в кіберпросторі. Отже, існує більший ризик неправильної класифікації поведінки і серйозного неправильного сприйняття намірів [10]. Крім того, важко точно визначити межі співпраці та забезпечити, щоб актори не використали свої законні права в одній сфері як прикриття для негативних дій в інших сферах.

Зрозуміло, що ці характеристики не впливають однозначно негативно на співробітництво різних акторів у сфері кібербезпеки, але ускладнюють його, спричиняючи певні проблеми, до основних з яких можна віднести: 1) проблему "безкоштовного використання"; 2) проблему відносних вигід; 3) проблему шахрайства. Розгляньмо перші дві з них більш докладно.

Деякі суб'єкти отримують вигоду від суспільних благ, не роблячи свого внеску в їхнє виробництво та підтримку (*проблема безкоштовного використання*). Вони можуть використовувати зусилля інших, оскільки суспільні блага не мають ціни для споживачів, неконкурентні та не можуть бути виключеними. Неконкурентність означає, що споживання блага одним суб'єктом не призводить до зниження доступності блага для споживання іншими. Невиключність означає практичну неможливість виключення будь-якого суб'єкта зі споживання блага [25]. Але проблеми виникають, коли занадто багато людей піддаються спокусі безкоштовного використання [22]. У цих умовах виробництво блага може припинитися, а може і не відбутися зовсім. До речі, недостатнє

виробництво суспільних благ досить часто зустрічається в міжнародних відносинах. Цього можна уникнути двома способами. Перший полягає в тому, що повинна бути або одна держава, або група держав, які брати на себе додаткові витрати, докладаючи додаткових зусиль [9, p. 138–139, 144–145; 15; 22, p. 49–50]. Другий полягає в тому, що державам удається встановити спільний міжнародний режим як стримувальний чинник для безкоштовного використання певних суспільних благ [14].

Слабко захищені комп'ютерні мережі певних юрисдикцій, які можуть бути використані зловмисниками, створюють ризик не тільки для їхніх власників, а й для інших мереж. Слабка кібербезпека, з цієї точки зору, є такою ж суспільною вадою, як і викиди вуглекислого газу або знеліснення. Слід додати, що слабка кібербезпека зумовлена не тільки технічними і організаційними, а й законодавчими недоліками. Добрим прикладом є так званий I-love-you virus 2000 р., комп'ютерний вірус, який призвів до фінансових втрат в розмірі декількох мільярдів доларів США по всьому світу. Після того як правоохоронні органи остаточно визначили творця вірусу, молодого студента з Філіппін, вони не змогли заарештувати і притягнути його до відповідальності, оскільки філіппінське законодавство у той час не забороняло створення й використання комп'ютерних шкідливих програм [28, p. 80–81].

Тут слід підкреслити, що в той час як філіппінське законодавство послабило національну кібербезпеку, самі Філіппіни не стали жертвою цих недоліків. Швидше, провідні економіки Америки, Західної Європи та Східної Азії постраждали від шкоди, завданої найважливішим ІТ-системам. Тому випадок вірусу I-love-you virus є прикладом загальної закономірності: бідні держави мають менше стимулів інвестувати в кібербезпеку, ніж багаті. Як уникнути глобального недозабезпечення кібербезпеки? Одна з можливостей полягає у створенні та забезпеченні дотримання міжнародного режиму, який ефективно карає тих, хто не відповідає певному стандарту кібербезпеки. Інша можливість – група сильніших держав добровільно надає допомогу в забезпеченні кібербезпеки слабшим державам.

Що стосується першої стратегії, то ще приблизно десять років тому – в "Огляді політики у сфері кіберпростору" 2009 р. і в "Міжнародній стратегії США у сфері кіберпростору" 2011 р. – було наведено аргументи на користь встановлення нової міжнародної норми, яка покладе на держави відповідальність за будь-які кібератаки, що здійснюються з інфраструктур, які перебувають під їх юрисдикцією [29; 30]. Такі норми мають зобов'язати кожну державу не допустити, щоб її національні мережі стали притулком для кіберзлочинців та інших зловмисників, а також не дозволять державам приховувати свої власні кампанії за нібито приватними хакерами.

Деякі американські чиновники та коментатори навіть наполягають на більш радикальній ідеї, виступаючи за введення санкцій або легітимацію тактики "зворотного зламу" в разі порушення норм. За словами Майкла Хейдена, колишнього директора Агентства національної безпеки (АНБ) США, інтернет-трафік у штатах із відхиленнями від норми може бути сповільнено або навіть перервано [33]. Міжнародне право вже дає достатньо підстав для таких заходів "активної оборони", стверджує співробітник Міністерства оборони США Дж. Метью. Доти, доки держава, з юрисдикції якої виходять атаки, або не бажає, або не в змозі зупинити такі атаки, жертва може законно "відповісти" на ці загрози, причому вона не зобов'язана доводити усвідомлення або співучасть держави, суверенітету якої вона збирається нашкодити. Саме за такою

логікою Рада безпеки ООН санкціонувала військові дії США проти уряду талібів в Афганістані [26, p. 53–57, 64–65]. Однак той же Склеров зазначає, що нинішня державна практика, а також більшість експертів у галузі міжнародного права поки не підтримують аналогічні підходи в кіберпросторі [26, p. 62].

Другий підхід до вирішення проблеми безкоштовного використання полягає в тому, що одна держава або групи держав надають допомогу в забезпеченні кібербезпеки державам зі слабкими стратегіями та можливостями у сфері кібербезпеки. Але при цьому слід мати на увазі, що той, хто захищає іноземні мережі, може й використовувати їх у власних інтересах, у т. ч. для шпигунської діяльності, тому що одні й ті самі знання дають можливість як оборонного, так і наступального характеру. Імовірно, далеко не всі держави готові скомпрометувати свою національну безпеку в такий спосіб.

На відміну від цього, підтримка кібербезпеки через технічну та правову допомогу є моделлю низького ризику з точки зору тих, хто отримує допомогу. Вона вже досить активно практикується на двосторонній та багатосторонній основі. До найбільш активних постачальників допомоги у забезпеченні кібербезпеки належать США.

Значна кількість публічних організацій США співпрацює з міжнародними партнерами. Управління з питань державної підзвітності (УПДЗ) перераховує кілька з цих ініціатив: організаційні підрозділи міністерств торгівлі національної безпеки допомагають державам Латинської Америки та Карибського басейну підвищувати технічний, регуляторний та адміністративний потенціал у рамках Організації американських держав (ОАД). Міністерство юстиції США бере участь у навчальних програмах для членів Азійсько-Тихоокеанського економічного співробітництва та Асоціації держав Південно-Східної Азії, а також для держав – членів Африканського союзу та Економічного співтовариства країн Західної Африки. Незважаючи на ці та інші види діяльності, американські експерти та політики регулярно закликають до розроблення більш комплексної програми кібердопомоги іншим державам [18, p. 41; 30, p. 21].

Поряд із США та іншими великими кібернетичними державами основними акторами з надання допомоги в забезпеченні кібербезпеки є міжнародні організації. Як уже зазначалось, Глобальний порядок денний з кібербезпеки (GCA) Міжнародного союзу електрозв'язку (ITU) спрямовано на поліпшення публічних та приватних можливостей по всьому світу [13, p. 186–187; 27]. Країни, що розвиваються, можуть узяти участь у Робочій програмі МСЕ з кібербезпеки для надання допомоги країнам, що розвиваються [13]. У рамках Європейського Союзу Європейське агентство мережевої та інформаційної безпеки (ЄНІСА) надає допомогу публічним та приватним суб'єктам у створенні та функціонуванні груп із реагування на надзвичайні ситуації в комп'ютерній сфері (CERT).

Але, розглядаючи таку допомогу недемократичним режимам, слід розуміти, що вона може використовуватись для спостереження та залякування політичних дисидентів, тому має бути чіткий контроль і моніторинг використання цієї допомоги.

Кібербезпека – це вигідно чи ні? Щоб відповісти на це запитання, у першу чергу необхідно знати, як влада в кіберпросторі розподіляється між державами. Але як можна визначити ранг влади в кіберпросторі? Існують різноманітні критерії, які можуть бути використані для вимірювання кібер-потужності. Згідно з Кларком, їх можна згрупувати, принаймні, в три категорії: залежність, наступальні можливості та оборонні спроможності [13, p. 147–149]. Якщо роз-

глядати залежності, то слід відповісти на запитання: які активи держави повинні захищати в кіберпросторі? Цілком очевидно, що у країн з розвиненою економікою більше причин побоюватися відсутності кібербезпеки, ніж у більш відсталих у цьому сенсі країн.

Але залежності відносяться не тільки до економіки, але і до оборонної політики. Держави, чиї військові стратегії та сили значною мірою покладаються на ІТ-системи, стикаються з більш високим ризиком кібератак, ніж держави, чиї сили все ще характеризуються низьким рівнем мережевої взаємодії.

Тобто кіберпростір, оскільки він є повністю рукотворним середовищем, перевертає з ніг на голову асиметрію влади в одному конкретному аспекті: від нього найбільше залежать провідні економічні та військові держави. Вони мають стежити за своїми кроками в кіберпросторі. На відміну від них, низькотехнологічним країнам майже нічого втрачати, і вони можуть навіть подумати про стратегії "випаленої землі" в кіберпросторі як про крайній варіант. Коли йдеться про наступальні можливості, застосовується протилежна логіка. Великі економічні та технологічні ресурси призводять до великих атакуючих можливостей.

Кіберпростір зменшує асиметрію потужностей, але не забезпечує рівних можливостей. Звичайно, окремі особи або невеликі групи хакерів можуть породжувати хаос у переважній більшості комерційних або адміністративних мереж. Проте атаки на високосекретні та фізично ізольовані мережі практично недоступні цим приватним хакерам, швидше за все, це тільки сфера діяльності державних органів безпеки [8]. Маніпуляції з іранськими установками зі збагачення урану в 2010 р., як приклад високоскладних кібератак, імовірно, потребували кількох місяців роботи різноманітних фахівців та експертів і близько чверті мільйона доларів США, щоб купити інформацію про невідомі вразливості програмного забезпечення [7; 22, p. 3].

Тобто технічні, фінансові та організаційні ресурси все ще мають значення в кіберпросторі [11]. Відмінності з точки зору цих ресурсів також пояснюють деякі асиметрії влади між державами в кіберпросторі, через що більшість експертів виділяють групу країн із розвиненими можливостями атак. Зокрема, експерти Центру нової американської безпеки до таких країн відносять США, Великобританію, Францію, Ізраїль, Росію та Китай [18, p. 29].

Наступальна міць, проте, не повинна вимірюватися виключно здатністю держав проводити складні кібератаки проти сильно захищених інфраструктур. Велика кількість простіших кібератак може бути досить ефективною, наприклад, із метою економічного шпигунства проти іноземних компаній. Численні атаки на дисидентські вебсайти також можуть бути високоефективним проявом політичних репресій [24, p. 182–183]. Саме з цієї причини політичні відносини між державами та різними хакерськими групами також можуть слугувати додатковим індикатором здатності держави до атак у кіберпросторі. Деякі авторитарні держави явно виграють у цьому відношенні. Найбільш яскравим прикладом є Китай, у якому ідея інтеграції приватних хакерських груп у проведені державою кампанії по веденню кібератак давно вже обговорюється в неофіційних стратегічних документах [2, p. 29–38; 31; 32, p. 471]. У Китаї багато хакерів є співробітниками державних компаній або студентами технічних вузів, а отже, і частиною китайської державної системи [16, p. 45–46; 32, p. 3]. Росія – це інша авторитарна країна, яку підозрюють у створенні довгострокових альянсів із приватними хакерськими угрупованнями. На думку деяких експертів, російські силові структури та націоналіс-

тичне хакерське співтовариство пов'язані через молодіжні організації, такі як "Наші" або "Євразійський рух молоді" [4, p. 117–119]. За винятком Ізраїлю, мало які демократичні уряди, ймовірно, могли б розраховувати на допомогу приватних хакерських груп. Зовсім навпаки: більшість західних хакерів дуже критично ставляться до ролі державних органів у кіберпросторі і навряд чи підпорядкували б себе їм у період кризи.

Нарешті, що стосується оборонних можливостей, то тут знову важливі як ресурси, так і взаємини між державою та суспільством. Але ще більш важливими є політичні обмеження. Ці обмеження в першу чергу стосуються демократичних держав. У Китаї всі критичні вузли мереж прямо або побічно контролюються урядом. На відміну від цього, органи безпеки США юридично обмежені тільки захистом урядових мереж. АНБ і Міністерство національної безпеки (МНБ) не можуть протистояти атакам на приватні мережі. ФБР також може розслідувати випадки кіберзлочинів тільки після факту завдання збитку. І потрібні були роки, щоб розпочати пілотний проєкт, що дозволяє АНБ і МНБ співпрацювати з великими оборонними компаніями США. Спочатку ідея полягала в тому, що в обмін інформацію про нові вразливості і загрози від компаній потрібно було б інформувати служби безпеки про вторгнення в мережі й дозволяти урядовим групам проводити криміналістичну експертизу цих інцидентів [12]. Однак після того, як активісти руху за громадянські права і частина самої адміністрації виступили з масовими запереченнями, проєкт довелося скоротити, і на даний час відповідальність за фактичні заходи захисту, як і раніше ,лежить виключно на компаніях [20]. Це є хорошим прикладом політичних та законодавчих обмежень кібербезпеки під керівництвом держави в умовах демократичних політичних систем.

Чому авторитарні держави мають виступати проти більш узгоджених зусиль із боротьби з кіберзлочинністю, що передбачає Конвенція проти кіберзлочинності? Чому такі держави, як Росія, відмовляються приєднатися до Конвенції? Хіба російські громадяни і бізнес не стають жертвами кіберзлочинців? Насправді, це так. Але інші країни, імовірно, більше потерпають від кіберзлочинності, ніж Росія. Отже, приєднання Росії до Конвенції принесло би більше користі іншим країнам, ніж самій Росії. Тут слід повторити, що приватні хакери, відіграють певну роль у портфелі російських атак. Вони ще більш важливі в китайському стратегічному мисленні, у той час як у багатьох західних країнах безпекові структури та приватні хакерські угрупування в кращому разі терплять один одного. Тому і в Росії, і в Китаю є додаткові причини очікувати від Конвенції менших вигід, ніж у західних країн. Отже, поки не буде вжито заходів із компенсації відносних вигід, Росія та Китай і надалі утримуватимуться від співпраці в боротьбі з кіберзлочинністю.

З усіх можливих компенсацій деякі види заходів зміцнення довіри (СТВМ), що забезпечують, принаймні, обмежену гарантію від військових кібератак, можуть мати найкращі шанси бути реалізованими. Держави можуть домовитися про декларування незастосування таких заходів першими, мораторій на атаки на критично важливі об'єкти інфраструктури та проведення регулярних переговорів між воєначальниками високого рівня [ 5, p. 240–241]. Росія та Китай, можливо, могли б розцінювати ці кроки як відносний виграш, зумовлений нібито наявними у США передовими можливостями для завдання ударів. Крім того, США мають кращу репутацію щодо виконання міжнародних зобов'язань із контролю над озброєннями, ніж країни колишнього Радянського Союзу та інші авторитарні країни. Однак, крім СТВМ, простір

для компромісів досить є обмеженим. Авторитарні країни, безумовно, вітали б деякі розпливчасті угоди щодо обмеження контенту, які вони могли б використовувати як законне прикриття для внутрішньої інтернет-цензури та діяльності зі спостереження в кіберпросторі.

**Висновки з цього дослідження та перспективи подальших розвідок у цьому напрямі.** Урядування у сфері кібербезпеки – це нова і методологічно складна сфера досліджень. З огляду на мізерність емпіричних даних усі види висновків можуть бути тільки попередніми і до них слід ставитися з граничною обережністю. З огляду на ці застереження можна стверджувати, що кібербезпека за своїми основними характеристиками меншою мірою сприяє міжнародному співробітництву, ніж інші проблемні сфери, і це може призвести до загострення різного роду проблем співробітництва. Але більш проблематичним є те, що багато держав зі слабким кіберзахистом просто серйозно не дбають про вирішення цієї проблеми і тим самим створюють суспільну шкоду. На щастя, існує група держав та міжнародних організацій, готових і здатних надати допомогу в забезпеченні кібербезпеки. Чого досі не вистачає, так це надійних санкцій проти тих, хто нехтує питаннями забезпечення кібербезпеки.

Ініціативи щодо зміцнення довіри в кіберпросторі вимагають наявності надійних режимів моніторингу, якими, проте, можна легко зловживати з метою шпигунства, тому політика колективного стримування кіберзагроз потребує інституційних гарантій від такого ризику. Нарешті, існує проблема орієнтації на відносні вигоди: держава потерпає від різних рівнів уразливості, можливостей і публічно-приватних відносин. Через це глобальне регулювання будь-якого окремого аспекту кібербезпеки супроводжується асиметричним розподілом відносних вигід. І подолати цю проблему можна лише через вибудовування довірчих відносин співпраці між різними як глобальними, так і національними акторами.

Перспективним напрямом дослідження вважаємо аналіз різного роду шахрайств у кіберпросторі.

**References**

1. Axelrod, R. (2009). [1984]. Die Evolution der Kooperation. München: Oldenbourg.

2. Billo, C., Chang, W. (2004). Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States. Institute for Security Technology Studies at Dartmouth College. Hanover, NH.

3. Bygrave L.A., Bing J. Internet Governance: Infrastructure and Institutions. Oxford: Oxford University Press.

4. Carr, J. (2010). Inside Cyber Warfare. Sebastopol; CA: O'Reilly Media.

5. Clarke, R.A., Knake, R.K. (2010). Cyberwar: The Next Threat to National Security and What to Do about it. New York: Harper / Collins.

6. Daun, A. (2011). Auge um Auge? Intelligence-Kooperation in den deutsch-amerikanischen Beziehungen. Wiesbaden: VS Verlag für Sozialwissenschaften.

7. Falliere, N., O'Murchu, L., Chien, E. (2011). W32. Stuxnet Dossier. Symantec. Whitepaper. URL: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

8. Gaycken, S. (2011). Cyberwar: Das Internet als Kriegsschauplatz. München: Open Source Press.

9. Gilpin, R. (1981). War and Change in World Politics. Cambridge: Cambridge University Press.

10. Hansel, M. (2013). Internationale Beziehungen im Cyberspace. Macht, Institutionen und Wahrnehmung. Wiesbaden: VS Verlag.

11. Hansel, M. (2011). Stuxnet und die Sabotage des iranischen Atomprogramms: Ein neuer Kriegsschauplatz im Cyberspace? / Handbuch Kriegstheorien. T. Jäger, R. Beckmann (Eds.). Wiesbaden: VS Verlag, 564–576.

12. Harris, S. (2009). The Cyber Defense Perimeter. *National Journal, 02.05.2009*. URL: http://www.nationaljournal.com/njmagazine/id_20090502_5834.php.

13. ITU (2007). ITU Cybersecurity Work Programme to Assist Developing Countries 2007–2009. URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-workprogramme-developing-countries.pdf.

14. Keohane, R.O. (1984). After Hegemony: Cooperation and Discord in the World Political Economy. Princeton; NJ: Princeton University Press.

15. Kindleberger, C.P. (1981). Dominance and Leadership in the International Economy Exploitation. *Public Goods and Free Rides. International Studies Quarterly, vol. 25, № (2), 242–254*.

16. Klimburg, (2011). Mobilising Cyber Power. *Survival, 53 (1), 41–60*.

17. Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. Santa Monica; CA: RAND.

18. Lord, K. M., Sharp, T. (2011). America's Cyber Future: Security and Prosperity in the Information Age. Vol. I. Washington; DC: Center for a New American Security.

19. Mathiason, J. (2009). Internet Governance: The new Frontier of Global Institutions. London; New York: Routledge.

20. Nakashima, E. (2011). NSA Alies with Internet Carriers to Thwart Cyber Attacks against Defense Firms. *Washington Post, 16.06.2011*. URL : http://www.washingtonpost.com/national/major-internet-service-providerscooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_story.html.

21. Offe, C. (2008). Governance – "Empty Signifier" oder sozialwissenschaftliches Forschungsprogramm / Governance in einer sich wandelnden Welt., G.F. Schuppert, M. Zürn (Eds.). Wiesbaden: VS Verlag. 61–76.

22. Olson, M. (1965). The Logic of Collective Action: Public Goods and the Theory of Groups. Cambridge: Harvard University Press.

23. Rieger, F. (2010). Der digitale Erstschlag ist erfolgt. Frankfurter Allgemeine Zeitung. URL : http://www.faz.net/s/RubCEB3712D41B64C3094E31BDC1446D18E/Doc~E8A0D43832567452FBDEE07AF579E893C~ATpl~Ecommon~Scontent.html.

24. Rohozinski, R., Haralampieva, V. (2008). Internet Filtering in the Commonwealth of Independent States / Access Denied: The Practice and Policy of Global Internet Filtering. Ronald Deibert et al. (Eds.). Cambridge; MA: The MIT Press. 177–185.

25. Samuelson, P.A. (1954). The Pure Theory of Public Expenditures. *Review of Economics and Statistics, 36 (4), 387–389*.

26. Sklerov, M.J. (2010). Responding to International Cyber Attacks as Acts of War. / Inside Cyber Warfare. Jeffrey Carr (Ed.). Sabastopol; CA : O'Reilly Media.

27. Sofaer, A.D., Clark, D., Diffie, W. (2010). Cyber Security and International Agreements. National Research Council / Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington; DC: National Academies Press. 179–206.

28. Sosa, G.C. (2009). Country Report on Cybercrime: The Phillipines. United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) (Eds.). Work Product of the 104th International Training Course "The Crminal Justice Response to Cybercrime". Tokio. URL: http://www.unafei.or.jp/english/pdf/RS_No79/No79_12PA_Sosa.pdf.

29. The White House (2011). International Strategy for Cyberspace: Prosperity, Security, and Openess in a Networked World. May 2011. URL : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

30. The White House (2009). Cyberspace Policy Review, Washington, DC. URL : http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

31. Thomas, T.L. (2009). Nation-state Cyber Strategies: Examples from China and Russia / Cyberpower and National Security. F.D. Kramer, S.H. Starr, L.K. Wentz (Eds.). Washington; DC: National Defense University Press, 465–488.

32. Thomas, T.L. (2000). Like Adding Wings to the Tiger. Chinese Information War Theory and Practice / Foreign Military Studies Office. Fort Leavenworth, KS. URL: http://libweb.uoregon.edu/ec/e-asia/read/tigerwings.pdf.

33. Zetter, K. (2010). Countries Should be Held Responsible for Cyber Attacks. *Wired, 30.07.2010.* URL: http://www.wired.co.uk/news/archive/2010-07/30/cyber-attack-countries.

***Obodiak V. K.,***
*PhD of Technical Science, Associated Professor, Associated Professor of Computer Science Department, Sumy State University , Sumy*
*ORCID 0000-0002-8539-1252;*
***Kotukh Ye. V.,***
*PhD of Technical Sciences, Associate Professor of Computer Science Department, Sumy State University, Sumy*
*ORCID 0000-0003-4997-620X*

## THE MAIN CHALLENGES OF GOVERNANCE IN THE FIELD OF CYBERSECURITY

The cross-border nature of cyberspace, its dependence on complex information technologies, the active use of sites and services of cyberspace by all countries in the globalized world not only provide new opportunities but also produce new threats to national security.

Some entities benefit from public goods without contributing to their production and support (the problem of free use). They can use the efforts of others because public goods have no price for consumers, are uncompetitive and cannot be excluded. Many countries are unable to protect the World Wide Web from their own hackers for technical, economic, political, etc. reasons. The assistance of third countries or the international community may be useful here. However, it should be pointed that those who protect foreign networks may use them in their own interests, including for espionage, because the same knowledge allows for both defensive and offensive nature. Probably not all states are ready to compromise their national security in this way.

In contrast, support for cybersecurity through technical and legal assistance is a low-risk model for the recipients. It is already quite actively practiced on a bilateral and multilateral basis. The United States is one of the most active providers of cybersecurity assistance. When considering such assistance to undemocratic regimes, it should be understood that it can be used to monitor and intimidate political dissidents, so there should be clear control and monitoring of the use of this assistance.

Initiatives to build trust in cyberspace require robust monitoring regimes, which can, however, be easily abused for espionage purposes, so a policy of collective deterrence of cyber threats requires institutional safeguards against such risks. Finally, there is the problem of focusing on relative benefits: the state suffers from different levels of vulnerability, opportunities and public-private relations. Because of this, global regulation of any particular aspect of cybersecurity is accompanied by an asymmetric distribution of relative benefits. Again, this problem can be overcome only by building trust in cooperation between different actors, both global and national.

**Keywords:** cybersecurity, cyberspace, governance, international cooperation.

*Надійшла до редколегії 20.11.2020 р.*