РОЗДІЛ ІІ
Суспільні комунікації та міжнародна інформація

УДК 323.28:004.9](81)
Бекеша Олександра,
студентка факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі Українки,
Луцьк, Україна
Bekesha.Oleksandra2018@ eenu.edu.ua;
Матюшок Вікторія,
студентка факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі Українки,
Луцьк, Україна
Viktoriia.Matiushok2016@ eenu.edu.ua;
Вознюк Євгенія,
кандидат політичних наук,
доцент кафедри міжнародних відносин і регіональних студій
факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі Українки,
Луцьк, Україна
Voznyuk.Yevhenija@eenu.edu.ua
https://orcid.org/0000-0002-7828-7430

РОЗВИТОК КІБЕРБЕЗПЕКИ БРАЗИЛІЇ НА СУЧАСНОМУ ЕТАПІ

Питання безпеки кіберпростору стає предметом широких дискусій на міжнародному рівні та є актуальним для Бразилії, адже в сучасному світі простежено тенденцію до посилення ролі цифрового середовища. Саме від кіберпростору, його стану, функціональності та прогнозованості залежать стабільність розвитку світової економіки, безпека громадян та сталий розвиток. Водночас усе більш не прогнозованими й витонченими стають кібератаки, що можуть завдати шкоди різного рівня всім верствам суспільства на національному та міжнародному рівнях.

У цій статті зазначено, що Бразилія має високі показники використання Інтернету й активно розвиває онлайн-послуги, хоча рівень кібербезпеки залишає бажати кращого. Проаналізовано сучасний стан та проблеми розвитку безпеки кіберпростору Бразилії. Досліджено місце Бразилії на світовій арені кіберзлочинності, а саме різновиди злочинів та їх кількість, а також їх вплив на економічну, політичну й суспільну стабільність у країні. Охарактеризовано стан законодавства Бразилії щодо забезпечення кібербезпеки. Акцентовано на проблемах галузі. Зокрема, досліджено поняття «фішинг», що є найбільш поширеним видом шахрайства в інтернет-просторі Бразилії.

В основу статті покладено Національну стратегію кібербезпеки Бразилії E-Cyber на період 2020–2023 рр., затверджену 5-го лютого 2020 р. президентом республіки Жаїром Мессіасом Болсонару. Поява цієї стратегії є значним кроком для Бразилії на шляху до створення безпечного кіберпростору та вдосконалення інформаційного суспільства. Під час дослідження детально опрацьовано кожен пункт стратегії та звернено увагу на кроки, запропоновані урядом республіки задля розвитку галузі. Акцентовано увагу на необхідності комплексного бачення та співпраці в розвитку галузі державними органами, бізнес-структурами й суспільством.

Ключові слова: *кібербезпека, інформаційний простір, національна безпека, стратегія кібербезпеки.*

1. ВСТУП

Постановка проблеми. Цифрова революція докорінно трансформує суспільство. Протягом двох останніх десятиліть мільярди людей скористалися експоненціальним ростом доступу до мережі Інтернет, швидким освоєнням інформаційних ресурсів та комунікаційних технологій, а також економічними й соціальними можливостями, що виникли в цифровій сфері.

Швидкий прогрес у сфері інформаційних і комунікаційних технологій привів до інтенсивного використання кіберпростору широким спектром видів діяльності, уключаючи надання урядових послуг, відповідно до світових тенденцій. Однак нові кіберзагрози, які можуть завдати шкоди різного виду, із різним рівнем впливу на людей та установи, з‟являються в тій же пропорції та піддають ризику національну й міжнародну безпеку.

Отже, захист кіберпростору вимагає ретельно розробленого бачення та лідерства в управлінні політичними, технологічними, освітніми, правовими й міжнародними змінами. У цьому сенсі уряд, промисловість, наукові установи та суспільство загалом повинні заохочувати розробку інновацій, упроваджувати передові технології й підтримувати постійну увагу до національної безпеки.

Аналіз останніх досліджень і публікацій. Проблему кібербезпеки Бразилії недостатньо досліджено у вітчизняній та зарубіжній літературі. Кібербезпеку як феномен міжнародних відносин розглядала О. Л. Доброжанська [1]. Принципи функціонування системи інформаційної безпеки на прикладі Японії розкрито в роботі Є. В. Вознюк [2]. Загрози для міжнародних відносин і глобальної безпеки в кіберпросторі дослідила В. Ю. Лук‟янчикова [3].

Мета роботи – проаналізувати сучасний стан кібернетичного простору Бразилії та визначити основні тенденції й характерні риси розвитку цієї сфери як пріоритетного напряму національної безпеки на основі нормативно-правової бази та Стратегії національної кібербезпеки Бразилії 2020–2023.

Методика дослідження. Під час проведення дослідження використано низку традиційних загальнонаукових методів. Зокрема, це методи аналізу, узагальнення, опрацювання документів і статистичних даних.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Бразилія є провідною державою Латинської Америки й учасницею G-20. В останнє десятиліття в країні простежено значне збільшення кількості послуг, що надаються громадянам через Інтернет. Серед них виділяються такі, як реєстрація, отримання довідок, сплата податків, дублікат документів і консультації, які надаються на онлайн-платформах федерального, державного та муніципального рівнів. Проте проблема кібербезпеки для Бразилії є актуальною як ніколи. Відповідно до глобального звіту компанії «Kroll» про шахрайство й ризики за 2017/2018 рр., 86 % опитаних керівників компаній стикалися з кібершахрайством по всьому світу. У Бразилії ж цей показник становить 89 %, що перевищує загальносвітовий рівень. Найбільш поширений вид шахрайства – шкідливий код, що становить 45 % випадків, а також фішинг через електронну пошту – 37 %, як наслідок – 63 % респондентів непокояться про вразливість систем до нових атак [4].

Відсутність відповідного законодавства про кіберзлочинність сприяє тому, що Бразилія є ціллю номер один і водночас провідним джерелом онлайн-атак у Латинській Америці; 54 % кібератак, повідомлених у Бразилії, нібито походять ізсередини країни. Подібно до США, Бразилія є одним із найпопулярніших осередків фішингових сайтів. Усе це призвело до того, що Бразилія є однією з перших у десятці світових джерел кібератак [5, с. 66].

Відповідно до звіту бразильської лабораторії безпеки, що спеціалізується на виявленні цифрових загроз «DFNDR Lab», кількість кібератак у Бразилії майже подвоїлась у 2018 р., порівняно з 2017 р. Лабораторія інформує, що 63,8 млн кібератак виявлено лише в другій чверті 2018 р., у середньому вісім щосекунди та понад 28 тис. на годину [6].

При цьому 57,4 % цих злочинів становить уже згаданий вище «фішинг» − шахрайська схема, мета якої – виманювання в користувачів мережі конфіденційної інформації, наприклад паролів і номерів соціального страхування. Вона, зазвичай, передбачає надсилання повідомлення-спаму, яке справляє враження, ніби походить із довіреного джерела, наприклад із банку (це наживка). У повідомленні

спаму міститься посилання на шахрайський веб-сайт, що видається за довірене джерело (це пастка). Користувач, нічого не підозрюючи, уводить інформацію, яка цікавить хакерів, уважаючи, що перебуває на сайті, котрий заслуговує на довіру. Вартий уваги той факт, що в законодавстві Бразилії немає конкретного положення, яке регулює фітинг [7].

Майже повна оцифрованість бізнес-моделей зробила глобальну економіку більш ефективною та динамічною, а також уразливою до кібератак. Ризик для економіки Бразилії, породжений вторгненням у комп‟ютери та розповсюдженням шкідливих кодів, що практикуються організованою злочинністю, уже є реальністю.Окрім того, значних утрат зазнає фінансова сфера. За даними Бразильської федерації банків Febraban, кіберзлочинність становить 95 % збитків, завданих банкам.

Для того щоб підвищити стійкість Бразилії до кіберзагроз, зробити її процвітаючою й надійною в цифровому середовищі й посилити успішність держави на міжнародній арені, президент республіки затвердив Національну стратегію кібербезпеки. Документ уключає десять стратегічних кроків [8].

Посилити дії в галузі кіберуправління. Управління в кіберсфері пов‟язане з діями, механізмами та заходами, яких потрібно вжити задля спрощення й модернізації менеджменту людськими, фінансовими та матеріальними ресурсами, а також для моніторингу ефективності й оцінки зусиль, докладених у цій галузі. Серед дій, які можна вжити з цього приводу, згадано:

1) проведення форумів управління;

2) створення контролю обробки інформації з обмеженим доступом;

3) установлення мінімальних вимог до кібербезпеки під час укладання контрактів державними установами;

4) реалізацію програм та проектів у галузі кіберуправління;

5) прийняття, крім норм управління, виданих Управлінням інституційної безпеки Президентства Республіки, правил, стандартів і моделей управління, визнаних у всьому світі;

6) посилення боротьби з програмним піратством;

7) розширення використання цифрового сертифіката, що гарантує конфіденційність, достовірність та підтвердження авторства в підписаних електронних транзакціях.

Створення централізованої моделі управління на національному рівні, яка об‟єднає всіх державних і недержавних суб‟єктів, що перебувають під егідою кібербезпеки. Така система сприятиме необхідному стратегічному, доктринальному та оперативному узгодженню дій, що стосуються галузі, і федеральний уряд повинен заохочувати обговорення альтернатив, спрямованих на інституційне зміцнення кібербезпеки Бразилії. У цьому контексті важливо, щоб урядова установа відповідала за керівництво на національному рівні та включала участь представників усіх верств суспільства. Виняток становлять лише аспекти, пов‟язані з кіберзахистом і війною, за які відповідає Міністерство оборони, що жодним чином не перешкоджає необхідній взаємодії установ.

Модель централізованого управління кібербезпекою є життєздатною та ефективною альтернативою, і її прийняли такі країни, як Сполучені Штати Америки, Великобританія, Португалія, Франція, Індія, Малайзія, Сингапур, Південна Корея та Японія. Вони демонструють, що створення центральних структур із повноваженнями щодо встановлення конкретних правил і дій дає хороші результати для координації та консолідації кібербезпеки як державного питання, сприяючи синергії між урядом, приватним сектором, суспільством і науковими колами та висвітлює стратегічний характер захисту кіберпростору.

У випадку Бразилії серед структур Федерального уряду виділяється Управління інституційної безпеки Президентства Республіки. Отже, немає гострої необхідності у створенні нових дороговартісних державних установ. Достатньо розширити вже наявну структуру до національного рівня. Окрім того, стратегія рекомендує створити національну раду з питань кібербезпеки, яка б об‟єднувала різні державні та недержавні суб‟єкти, аби досліджувати кібербезпеку під усеосяжною, сучасною призмою й з акцентом на реальні національні потреби. Стратегія передбачає створення декількох дискусійних груп під координацією Управління інституційної безпеки при Президентові республіки, щоб гарантувати залучення професіоналів зі знаннями спеціальності для кращого розуміння викликів, які потрібно вирішити в різних секторах відповідно до конкретних реалій.

Сприяти спільному, надійному та безпечному середовищу між державним і приватним секторами й суспільством. Цей пункт стратегії включає такі дії:

1) заохочувати обмін інформацією про кіберінциденти;

2) установити механізми, які уможливлюють взаємодію та обмін інформацією на різних рівнях;

3) зміцнити Центр реагування на кіберінциденти уряду – CTIR.gov (Brazilian Computer Security and Incident Response Center) і продовжувати оновлювати персонал та матеріали центру;

4) збільшити роль Центрів реагування на кіберінциденти – національних CSIRT (Computer Security Incident Response Team);

5) покращити національну інфраструктуру розслідування кіберзлочинності;

6) заохочувати створення та функціонування команд для боротьби з кіберінцидентами та реагування на них, з акцентом на використання нових технологій.

Профілактичні заходи, засновані на оцінках ризиків, можуть зменшити зростаючу кількість кіберінцидентів, однак вони не можуть їм повністю запобігти. Тому потрібна функція реагування для швидкого виявлення загроз і мінімізації втрат, які вони можуть спричинити. У цьому контексті підкреслено актуальність ресурсів та механізмів, що дасть змогу взаємодіяти й обмінюватися інформацією на різних рівнях, між державними та приватними установами, а також міжнародними організаціями, які мають досвід моніторингу тенденцій кіберзагроз, ураховуючи регіональні й глобальні наслідки виникнення інцидентів у цифровому середовищі. У Бразилії центрами, що працюють у цій сфері, є CERT.br (Brazilian National Computer Emergency Response Team) і CTIR Gov. Перший відповідає за розгляд інцидентів комп‟ютерної безпеки, пов‟язаних із мережами, підключеними до Інтернету, більш орієнтованих на комерційні та приватні установи, другий має подібні завдання, але спрямований на урядові мережі. Країна ще потребує зміцнення й удосконалення своїх державних органів, які займаються кібербезпекою. Оскільки CTIR є центральним органом уряду, що координує та виконує дії, спрямовані на управління інцидентами, рекомендується надати цьому органу можливості ефективніше діяти на національному рівні. У цьому ж напрямку рекомендовано вдосконалити національну структуру розслідування кіберзлочинності.

Підвищення рівня захисту уряду. Країна перебуває в процесі оцифровування державних послуг, що викликає прогресивну критику урядових мереж і систем, що підтримують (забезпечують) надання цих послуг громадянам. Той самий процес спостерігається й стосовно структур зв‟язку між державними структурами (інституціями), рівень захисту яких повинен бути адекватним і пропорційним до їх актуальності. У зв‟язку з посиленням інтеграції баз даних та цифрових платформ в урядових мережах та системах простежено збільшення кількості вразливих місць, якими можуть скористатися хакери.

Витік або втрата інформації державними установами має негативний вплив на надання послуг населенню. Тому рекомендовано створювати резервні копії даних, які часто оновлюються, автоматично відокремлюються та зберігаються в захищених місцях. Ця практика значно звузить спектр діяльності зловмисників і зменшить ризики викрадення даних, фінансових утрат та негативного впливу на імідж установ.

Мобільні пристрої, підключені до мережі, часто використовуються державними органами і є об‟єктами кіберзлочинності, особливо у випадку IT-політики BYOD, що розшифровується як «bring your own dewice» або – «принеси свій власний пристрій». Така політика дає змогу використовувати особисті технічні засоби для доступу до корпоративних систем. Ця практика має низку переваг, зокрема економія бюджету та ефективність. З іншого боку, існують такі ризики: пристрій може бути втраченим або викраденим разом із корпоративною інформацією, вірус з одного пристрою може поширитися на всю систему тощо. Тому рекомендовано розробити конкретні вимоги до використання обладнання державними установами.

Підвищити рівень захисту національних критичних інфраструктур. Захист критичних інфраструктур заслуговує на конкретний підхід. У Бразилії цими інфраструктурами є телекомунікаційний, транспортний, енергетичний та фінансовий сектори. Окрім того, стратегічне значення має фармацевтична галузь. За даними порталу CSO, фармацевтичні організації є вразливими мішенями для кіберзлочинності, переважно через можливість утрати інтелектуальної власності [9].

У 2018 р. затверджено Національну політику безпеки національної критичної інфраструктури, що спрямована на забезпечення безпеки та стійкості критичної інфраструктури країни й безперервності надання її послуг.

Удосконалення правової бази щодо кібербезпеки. Для вдосконалення нормативно-правової бази щодо кібербезпеки потрібно переглянути та оновити наявні норми й розробити нові інструменти регулювання цієї галузі права. Стратегією рекомендовано вдатися до таких дій:

1) виявити та розв’язати проблеми, які відсутні в чинному законодавстві;

2) уключити до Кримінального кодексу нових видів кіберзлочинів;

3) створити стимулювальну політику щодо найму кваліфікованої робочої сили в галузі кібербезпеки;

4) під координацією Управління інституційної безпеки при Президентстві республіки підготувати проект закону про кібербезпеку з настановами, які забезпечать макростратегічне узгодження сектору та вирішальний внесок у підвищення безпеки організацій і громадян.

Заохочення розробки інноваційних рішень у сфері кібербезпеки. Останні кілька десятиліть ознаменувались інтенсивною технологічною революцією, яка сприяла важливим змінам у повсякденному житті людей, особливо стосовно форм спілкування, взаємодії та доступу до інформації.Заохочення досліджень і новітніх розробок у сфері кібербезпеки сприятимуть необхідним інноваціям національної продукції в цій критичній, сучасній та важливій галузі.

У Бразилії існує дисонанс між проектами, які реалізовують державні й приватні університети, та потребами в кібербезпеці. Такий стан речей демонструє необхідність більш тісного й ефективного діалогу між бізнес-сектором та науковими колами, щоб зусилля й проекти позитивно та конструктивно впливали на суспільство.

У цьому сенсі рекомендовано налагоджувати партнерські стосунки з Міністерством освіти, спрямовані на реалізацію програм сприяння розвитку потенціалу кібербезпеки для студентів базової освіти із метою виявлення талантів. Рекомендовано, щоб університети розробляти проекти відповідно до потреб виробничого сектору.

Наближення магістерських і докторських програм не лише в галузі прикладних обчислень, але й в інших галузях знань може бути ефективним способом підготовки, удосконалення та кваліфікації персоналу, зацікавленого в цій темі.

Розширити міжнародне співробітництво Бразилії у сфері кібербезпеки. На сучасному етапі існує нагальна потреба у співпраці між країнами задля пом‟якшення загроз, таких як кіберзлочини, кібер-шпигунство, перехоплення даних тощо. У цьому напрямі потрібно посилити дії Бразилії під час підготовки та перегляду міжнародних інструментів, пов‟язаних із кібербезпекою, шляхом стимулювання дебатів і заохочення міжнародної співпраці з цього питання. Окрім того, потрібно сприяти інтеграції між Бразилією й країнами Латинської Америки, акцентуючи на регіональному лідерстві Бразилії.

Примітно, що країна має намір шукати двосторонніх угод про співпрацю в кібербезпеці з якомога більшою кількістю країн, що демонструє намір установити в цій галузі плідні, конструктивні та прозорі відносини. Наразі Управління інституційної безпеки Президентства республіки здійснює моніторинг десятків угод щодо обміну й взаємного захисту секретної інформації.

Розширити партнерство у сфері кібербезпеки між державним сектором, приватним сектором, науковими колами та суспільством. Співпраця між державним управлінням, приватним сектором і суспільством у кількох сферах зазвичай приносить корисні результати та сприяє підвищенню довіри громадян до державних і приватних установ та покращує стосунки між цими суб‟єктами. У сфері кібербезпеки цей взаємозв‟язок є суттєвим.

На сьогодні в Бразилії процеси координації між різними суб‟єктами в кіберсередовищі містять широкий спектр домовленостей, які не завжди є інституціоналізованими та багаторічними, а також не пов‟язані зі звичайними механізмами регулювання. До цього факту додано наявність великої кількості установ, котрі безпосередньо чи опосередковано займаються кібербезпекою, що створює значні труднощі для співпраці й координації для бразильської держави. Тому рекомендовано створити відповідні канали комунікації, щоб можна було почути та врахувати думки всіх сегментів бразильського суспільства під час розробки, реалізації й просування публічної політики, пов‟язаної з кібербезпекою.

Підвищити рівень обізнаності суспільства щодо кібербезпеки. Підвищення рівня обізнаності у сфері кібербезпеки в суспільстві надає можливість людям належно підвищити рівень зрілості в кібербезпеці в суспільстві, щоб зрозуміти загрози й ризики в кіберпросторі та дати можливість людям у необхідному обсязі використовувати процедури й інструменти та на користь безпечного застосування цифрового середовища. Стратегія рекомендує такі дії:

1) заохочувати державні агенції та приватні компанії проводити внутрішні інформаційні кампанії;

2) проводити акції з підвищення обізнаності населення;

3) створити державну політику, яка сприятиме поінформованості суспільства щодо кібербезпеки;

4) пропонують уключити кібербезпеку через її основні навички й етичне використання інформації в базовій освіті – дошкільній освіті, початковій школі та середній школі;

5) заохочувати створення вищих навчальних курсів із кібербезпеки;

6) запропонувати створити заохочувальні програми для студентів та аспірантів у Бразилії й за кордоном у сфері кібербезпеки;

7) заохочувати підготовку фахівців до дій у боротьбі з кіберзлочинами;

8) заохочення участі в національних та міжнародних форумах і заходах із кібербезпеки;

9) удосконалити механізми інтеграції, співпраці та стимулювання між університетами, інститутами, науково-дослідними центрами й приватним сектором стосовно кібербезпеки;

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Підсумовуючи наведені спостереження та детально проаналізувавши Стратегію кібербезпеки Бразилії, можемо стверджувати, що в країні на сучасному етапі немає єдиної та всеосяжної системи захисту кіберпростору, яка б сприяла зміцненню національної кіберстійкості. Чинні норми, указівки й стандарти пов‟язані з кібербезпекою, не були належно втілені державними й приватними структурами.

Підкреслимо, що кібербезпека представляє нову парадигму щодо безпеки для держави, оскільки всі національні суб‟єкти мають уразливі місця, які можуть бути використані кібершахраями, що матиме значні негативні наслідки для стабільності національних інститутів.

«Стратегія безпеки кіберпростору Бразилії» є адекватною та своєчасною відповіддю на проблеми в галузі безпеки в державі. Виконання рекомендацій стратегії зробить можливим запобігання та більш якісне й швидке реагування на інциденти в кіберпросторі.

Однією з найважливіших проблем, що стосується кібербезпеки, є те, що її потрібно розуміти цілісно, не доцільно підходити до неї обмеженим чином. Лише за умови узгодженої роботи державних органів, приватного сектору та суспільства можна втілити пункти стратегії в життя.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Доброжанська О. Л., Демцов А. А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин.* 2011. № 102. С. 111–116.
2. Vozniuk E. Principles and features of Japan‟s information security system. *Політичне життя.* 2017. № 4. С. 8–12.
3. Лук‟янчикова В. Ю. Кіберпростір: загрози для міжнародних відносин та глобальної безпеки. *Гілея: наук. вісник.* 2013. № 72. С. 793–796.
4. 8 a cada 10 executivosjáenfrentaramfraudescibernéticas. URL: https://itforum365.com.br/8-cada-10-executivos-ja-enfrentaram-fraudes-ciberneticas/
5. Internet organised crime threat assessment. *European Cyber crime Centre.* 2018. URL: https://www.europol. europa.eu/sites/default/ files/documents/iocta2018.pdf.
6. Relatórioda Segurança Digitalno Brasil. *DFNDR Lab.* 2018. URL: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf.
7. Ковтун Л. Ю., Нечипорук І. В. Фішинг як одна із форм шахрайства в інтернеті. 2015. URL: http://www.legalactivity.com. ua/index.php?option=com_content&view=article&id=1075%3A2015-09-15-06- 47-15&catid= 131%3A5-0915&Itemid=161&lang=ru.
8. Estratégia Nacional de Segurança Cibernética. URL: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm.
9. CSO. UNITED STATES. URL: https://www.csoonline.com/article/3387981/stakes-of-security-especially-high-in-pharmaceutical-industry.html.

Матеріал надійшов до редакції 23.10.2019 р.

CYBER SECURITY DEVELOPMENT IN BRAZIL AT THE PRESENT STAGE

The issue of cyberspace security is becoming the subject of wide international discussions and is relevant for Brazil, because in today‟s world there is a tendency to strengthen the role of the digital environment. It is from cyberspace, its state, functionality and predictability that the stability of the world economy, the security of citizens and

sustainable development depend. At the same time, cyberattacks are becoming more and more unpredictable and sophisticated, which can cause damage to all segments of society at the national and international levels.
This article states that Brazil has a high rate of Internet use and is actively developing online services, although the level of cybersecurity leaves much to be desired. The current state and problems of development of Brazil cyberspace security are analyzed. Brazil‟s place in the global cybercrime scene has been studied, namely the types of crimes and their number, as well as their impact on economic, political and social stability in the country. The state of Brazilian cybersecurity legislation is described. The emphasis is on the problems of the industry. In particular, the concept of «fishing», which is the most common type of fraud in the Internet space in Brazil.
The article is based on the National Cyber Security Strategy of Brazil E-Cyber for the period 2020–2023, which was approved on February 5, 2020 by the President of the Republic Jair Messias Bolsonara. The emergence of this strategy is a significant step for Brazil towards creating a secure cyberspace and improving the information society. During the study, each item of the strategy was elaborated in detail and attention was paid to the steps proposed by the government of the republic for the development of the industry. Emphasis is placed on the need for a comprehensive vision and cooperation in the development of the industry by government agencies, business structures and society.
Key words: cybersecurity, information space, national security, cybersecurity strategy.

REFERENCES

1. Dobrozhanska, O. L., Demtsov A. A. (2011). Kiberbezpeka yak fenomen mizhnarodnykh vidnosyn na prykladi Federatyvnoi Respubliky Nimechchyny. *Aktualni problemy mizhnarodnykh vidnosyn,* 102, 111–116.
2. Vozniuk, E. (2017). Principles and features of Japan‟s information security system. *Політичне життя,* 4, 8–12.
3. Lukianchykova, V. Iu. (2013). Kiberprostir: zahrozy dlia mizhnarodnykh vidnosyn ta hlobalnoi bezpeky. *Hileia: naukovyi visnyk,* 72, 793–796.
4. 8 a cada 10 executivosjáenfrentaramfraudescibernéticas. URL: https://itforum365.com.br/8-cada-10-executivos-ja-enfrentaram-fraudes-ciberneticas/.
5. Internet organised crime threat assessment. *European Cyber crime Centre,* 2018. URL: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.
6. Relatórioda Segurança Digitalno Brasil. *DFNDR Lab.* 2018. URL: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf.
7. Kovtun, L. Iu., Nechyporuk, I. V. (2015). Fishynh yak odna iz form shakhraistva v interneti. URL: http://www.legalactivity.com.ua/index.php?option=com_content&view=article&id=1075%3A2015-09-15-06-47-15&catid=131%3A5-0915&Itemid=161&lang=ru.
8. Estratégia Nacional de Segurança Cibernética. URL: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm.
9. CSO. UNITED STATES. URL: https://www.csoonline.com/article/3387981/stakes-of-security-especially-high-in-pharmaceutical-industry.html.

УДК 323.28:004](477:470+571)

Вознюк Євгенія,
кандидат політичних наук, доцент кафедри міжнародних відносин і регіональних студій
Східноєвропейського національного університету імені Лесі Українки, Луцьк, Україна.
Vozniukjane.vippo@gmail.com, Voznyuk.Yevhenija@eenu.edu.ua
https://orcid.org/0000-0002-7828-7430;
Романцов Дмитро,
студент факультету міжнародних відносин
Східноєвропейського національного університету імені Лесі Українки, Луцьк, Україна.
virtyalprofi@gmail.com, Romantsov.Dmytro@eenu.edu.ua;