УДК 342.4:327.7

***Т. Ю. Ткачук***
*кандидат юридичних наук, доцент,*
*заступник завідувача кафедри організації*
*захисту інформації з обмеженим доступом*
*Навчально-наукового інституту інформаційної безпеки*
*Національної академії Служби безпеки України*

## ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ ПОЗАБЛОКОВОГО СТАТУСУ

Постановка проблеми. Європейські країни, які умовно можуть бути узагальнені під назвою «країни позаблокового статусу», належать до найрозвиненіших на континенті, зокрема і щодо темпів розвитку інформаційного суспільства, а також усвідомлення необхідності протидії кіберзагрозам, вдосконалення форм і методів захисту інформації, критичної інформаційної інфраструктури, інформаційно-психологічної безпеки громадян і гарантування інформаційної безпеки загалом як складника національної безпеки. Отже, обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку провідних європейських країн в інформаційній сфері, критично оцінювати й адаптувати до власних реалій їхній позитивний досвід у сфері гарантування інформаційної безпеки. У такому контексті корисним і цікавим буде досвід таких країн, як Австрія, Швейцарія, Фінляндія й Ірландія, адже вони, як слушно зазначає В. Політанський, є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства, створення розвиненої інфраструктури інформаційних технологій і забезпечення високого рівня доступу населення до них [1, с. 35].

Стан дослідження. Дослідження з питань розвитку інформаційного суспільства і гарантування інформаційної безпеки в закордонних країнах, зокрема й у країнах Центральної Європи, здійснювали К. Андерсон, У. Боудіш, Г. Діллон, Т. Ламбо, М. Прайс, П. Сігел, Дж. Стейн, С. Хантінтон та інші науковці. Проблематику гарантування інформаційної безпеки в країнах Європи досліджували у своїх роботах О. Запорожець, В. Петров, О. Чернухін та інші науковці, однак питання гарантування інформаційної безпеки в країнах Європи, зокрема й у країнах позаблокового статусу, та оцінка корисності їх досвіду для України недостатньо висвітлені в науковій літературі.

Постановка завдання. Метою статті є дослідження гарантування інформаційної безпеки в європейських країнах позаблокового статусу, а також оцінка значущості їхнього досвіду в зазначені сфері для України в контексті євроінтеграційних прагнень.

Виклад основного матеріалу. Із закінченням холодної війни біполярний світ став набагато складнішим, втратила самостійну цінність концепція неприєднання, неучасті у військово-політичних союзах тощо. Зокрема, втратило свій безпосередній зміст поняття нейтралітету, пов'язане з неучастю у війнах, отже, нейтральний статус низки країн Європи значною мірою залишається даниною підтримці історичних традицій. Сьогодні такі держави позначають як постнейтральні або позаблокові (буквально – неприєднані, non-aligned). Кожна із цих держав має власну історію нейтралітету, однак протягом останніх 20 років усі вони зіткнулися із проблемою доцільності збереження нейтрального статусу та з необхідністю введення тих або інших обмежень до цього поняття. Така тенденція наявна і зараз, оскільки глобалізаційні процеси й характер новітніх загроз – регіональні конфлікти, міжнародний тероризм, поширення зброї масового знищення, кіберзлочинність – збільшують ступінь взаємної залежності країн і вимагають для протистояння таким загрозам спільних і узгоджених зусиль міжнародного співтовариства.

Особливе місце серед країн позаблокового статусу посідає Швейцарія, адже ця країна не є не лише членом НАТО, але й Європейського Союзу (далі – ЄС). З 1992 р. у Швейцарії діє Федеральний акт про захист даних, який втілює загальноєвропейські принципи захисту інформації, зокрема, так званих «чутливих» відомостей і персональних даних [2]. 2010 р. Верховний суд Швейцарії надав додаткові гарантії конфіденційності персональних даних, підтримавши місцевого уповноваженого із захисту персональних даних і ухваливши, що збір інформації про IP-адреси користувачів файлообмінних мереж без їхньої згоди (зокрема й у контексті боротьби з порушеннями авторських прав) є незаконним [3].

Загалом гарантування інформаційної безпеки електронних даних та інформаційних мереж здійснюється у Швейцарії відповідно до Національної стратегії захисту від кіберризиків, затвердженої 2012 р. Метою ухвалення вказаної Стратегії визначено: раннє виявлення кіберзагроз і небезпек; підвищення стійкості критичної інфраструктури; ефективне зниження кіберризиків, зокрема, кіберзлочинності, кібершпигунства й кіберсаботажу. Передумовами для зниження кіберризиків водночас вважається індивідуальна відповідальність і національне співробітництво між

приватним сектором і органами влади, а також співробітництво з іншими країнами. Держава має втручатися в процеси гарантування кібербезпеки тільки тоді, якщо суспільні інтереси перебувають під загрозою або якщо це відповідає принципу субсидіарності. Оброблення кіберризиків має розглядатися як елемент процесів бізнесу, виробництва чи управління, до яких повинні бути інтегровані всі суб'єкти – від адміністративних і технічних рівнів до вищого керівництва. Ефективний підхід до управління кіберризиками заснований на принципі розподілу обов'язків між владою, приватним сектором і населенням, відповідно до якого кожна організаційна одиниця (політична, економічна або соціальна) відповідає за те, щоб знати про кібераспекти й усувати інформаційні ризики, пов'язані з конкретними процесами, або зменшувати їх за можливості [4].

На початку поточного року у Швейцарії також було розпочато роботу над законом про інформаційну безпеку, оскільки незаконне використання інформації та втручання в роботу інформаційних систем може серйозно вплинути на істотні інтереси Швейцарії та права її громадян. Ґрунтуючись на загальновизнаних міжнародних стандартах, закон про інформаційну безпеку має створити єдину формально-правову основу для контролю й впровадження інформаційної безпеки у сфері компетенції Федерального уряду Швейцарії. Закон, насамперед, стосується федеральних органів державної влади, зокрема й парламенту, федеральних судів, федеральної прокуратури та Національного банку. Приватні особи й бізнес підпадають під дію закону тільки в разі здійснення інформаційно чутливої діяльності за доручення федеральних органів. Федеральна рада також прагне поглибити співробітництво з кантонами, які повинні бути представлені у відповідному координаційному органі й брати участь у стандартизації визначених заходів. Серед іншого закон регулює питання управління ризиками, класифікацію інформації та принципи безпеки у сфері використання інформаційно-технічних ресурсів. Передбачається, що закон про безпеку інформації матиме пріоритет над законодавством про свободу інформації [5].

Далі доцільно буде розглянути досвід гарантування інформаційної безпеки європейських країн, які не є членами НАТО, однак є членами ЄС – на прикладі Австрії, Фінляндії й Ірландії. Передусім, варто зазначити, що членство в ЄС накладає на ці країни обов'язки щодо дотримання стандартів згаданої організації в питаннях розвитку інформаційного суспільства та гарантування інформаційної безпеки. Так, ще в 1991 р. було розроблено «Європейські критерії безпеки інформаційних технологій» [6], якими, зокрема, визначені завдання гарантування інформаційної безпеки: захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності; забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення; забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні. У 1996 р. стандарти європейської інформаційної безпеки було втілено в «Єдиних критеріях безпеки інформаційних технологій» [7].

В Австрії, Фінляндії та Ірландії, як і в інших країнах ЄС, значна увага приділяється проблемам кібербезпеки, висвітленим у документі Європейської комісії «На шляху до загальної політики у сфері боротьби з кіберзлочинністю», в якому кіберзлочинність визначається як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж і систем, і охоплює: традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); публікацію незаконного контенту в електронних медіа; специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо) [8].

Однією із країн-лідерів ЄС за показниками розвитку інформаційного суспільства справедливо вважають Фінляндію, адже в рейтингу країн ЄС вона посідає перше місце за рівнем цифрової грамотності (понад 50% населення), друге місце – за показником поширення мережі широкосмужного зв'язку (34% населення) [9].

Основними державними установами, відповідальними за розроблення та реалізацію політики інформаційної безпеки, є Міністерство транспорту та комунікацій і омбудсмен із питань захисту даних (Data Protection Ombudsman). До повноважень Міністерства транспорту та комунікацій входить розроблення законодавства щодо комунікаційних мереж, безпеки даних, забезпечення доступу до комунікаційних послуг, а також розроблення і реалізація національної політики у сфері інформаційної безпеки. Структурним підрозділом Міністерства транспорту та комунікацій є Управління Фінляндії з регулювання комунікацій (Finnish Communications Regulatory Authority – FICORA – Т. Т.), яке уповноважене здійснювати контроль і державне регулювання у сфері інформаційно-комунікаційних технологій. До повноважень FICORA входить контроль за функціонуванням електронних комунікаційних мереж, інформування про можливі загрози інформаційній безпеці, підвищення обізнаності громадян із питань інформаційної безпеки, планування й управління використанням радіочастот, мережевими адресами, а також контроль змісту програм і реклами на телебаченні та радіо. У структурі FICORA функціонує CERT-FI (Computer Emergency Response Team of Finland – Т. Т.) – фінська комп'ютерна

група швидкого реагування, основним завданням якої є попередження, виявлення та реагування на кіберінциденти, а також поширення інформації про загрози інформаційній безпеці [10]. У гарантуванні інформаційної безпеки також бере активну участь громадянське суспільство. Серед неурядових організацій, що опікуються проблематикою інформаційної безпеки, провідна роль належить Фінській федерації комунікацій та телеінформатики (Finnish Federation for Communications and Teleinformatics – FiCom – Т. Т.) та Фінській асоціації з питань інформаційної безпеки (Finnish Information Security Association – FiSA – Т. Т.). FiCom здійснює планування і координацію заходів щодо розвитку інформаційно-комунікаційних технологій, здійснення моніторингу ситуації в ІКТ-секторі, здійснення впливу у сфері регулювання ринку інформаційно-комунікаційних технологій тощо, тоді як метою FiSA є розвиток професіоналізму й обізнаності у сфері інформаційної безпеки. Діяльність асоціації включає організацію дискусій, конференцій, участь у різних програмах з інформаційної безпеки [11]. У 2015 р. компанія CGI також відкрила у Фінляндії центр інформаційної безпеки, завданням якого є відстеження кібератак [12].

Стратегія кібербезпеки Фінляндії, затверджена 2013 р., наголошує на тому, що загрози, які виходять із кіберпростору, стають все більш серйозними, адже кібератаки можуть використовуватися як засіб політичного й економічного тиску, зокрема й поряд із традиційними засобами військової сили. Водночас кіберпростір є джерелом величезного потенціалу та ресурсів, адже збільшує можливості розвитку бізнесу, працевлаштування та залучення іноземних інвесторів. Стратегія також визначає, що Фінляндія як невелика й відкрита до співробітництва країна має «відмінні шанси піднятися до авангарду кібербезпеки», тоді як бачення кібербезпеки таке: Фінляндія може забезпечити свої життєво важливі функції і протистояти кіберзагрозам у всіх ситуаціях; громадяни, органи влади та юридичні особи можуть ефективно використовувати безпечний кіберпростір, що виникає в результаті заходів кібербезпеки, здійснюваних на національному й міжнародному рівнях; до 2018 р. Фінляндія має стати провісником цілковитої готовності до протидії кіберзагрозам і управління порушеннями, що викликані такими загрозами. Якщо розслідування кіберінцидентів здійснює поліція, то організація всеосяжного кіберзахисту покладається на Сили оборони Фінляндії під керівництвом Міністерства оборони. Можливості військового кіберзахисту охоплюють розвідку, а також кібератаку та ведення кібервійн, однак основним елементом військової сили в кіберпросторі є інтелектуальне попередження загроз. Зауважимо, що у 2015 р. Міністерство внутрішніх справ Фінляндії виступило з ініціативою оновлення закону про розвідувальну діяльність із метою надання поліції та військовим права на розвідку в інформаційних мережах [13].

Програми становлення інформаційного суспільства Австрійської Республіки втілюють політичну стратегію об'єднання Європи на базі новітніх технологій, інформаційно-комунікаційної інфраструктури й інтелектуального потенціалу регіону. Істотно впливають на інформаційну політику Австрії міжнародні організації, резиденції яких розміщені у Відні, і складником програм діяльності яких є розвиток інформаційного суспільства. У Плані дій уряду Австрії передбачено такі напрями інформаційної інтеграції країни, як: координація трансформації інформаційного сектору; створення відповідних державних інституцій із регулювання ринку інформаційних технологій; стимулювання виробництва інформаційних продуктів і послуг; підтримка лідерства Австрії в галузі електронних технологій, зокрема й виробництва мікрочіпів та інтегрованих електронних схем; лібералізація торгівлі інформаційними продуктами і послугами; розвиток електронної комерції; сприяння торгівлі інноваційними технологіями із третіми країнами; створення об'єднаних мереж австрійських і європейських центрів прикладних досліджень інформаційного суспільства; використання потенціалу міжнародних організацій; наукова кооперація (на двосторонній основі) тощо; розроблення проектів для соціальної сфери, освіти, охорони здоров'я та навколишнього середовища; міжнародне співробітництво за гуманітарними напрямами.

Стратегія кібербезпеки Австрії визначає, що звичайні напади на Австрію стали малоймовірними в недалекому майбутньому, натомість для Австрії та ЄС загалом усе більш актуальними стають нові проблеми, ризики й загрози, насамперед, міжнародний тероризм; поширення зброї масового знищення; внутрішні й регіональні конфлікти або заворушення, які стосуються Європи або мають глобальні наслідки; «відмова держави»; природні або техногенні катастрофи; кібератаки; загрози для стратегічної інфраструктури; транснаціональна організована злочинність; торгівля наркотиками, корупція, незаконна міграція; безуспішна інтеграція; нестача ресурсів (енергії, продовольства, води), зміна клімату, екологічна шкода і пандемії; піратство й загрози транспортним маршрутам, а також наслідки міжнародної фінансово-економічної кризи у сфері безпеки [14]. Напади з кіберпростору становлять безпосередню загрозу безпеці й належному функціонуванню державного апарату, економіки, науки й суспільства. Недержавні суб'єкти (наприклад, злочинці, учасники організованих злочинних угруповань або терористи), а також державні суб'єкти (наприклад, секретні служ-

би й військові) можуть зловживати можливостями кіберпростору у своїх власних цілях і перешкоджати його належному функціонуванню. Як загрози в кіберпросторі, так і продуктивне використання кіберпростору практично не лімітовані. Тому головним пріоритетом Австрії є гарантування безпеки й кібербезпеки на національному та міжнародному рівнях. Всеосяжна політика кібербезпеки означає, що зовнішня й внутрішня безпека, а також всі аспекти цивільної та військової безпеки тісно пов'язані та взаємозалежні. Гарантування кібербезпеки виходить за межі повноважень традиційних органів безпеки і вимагає залучення інструментів багатьох інших сфер політики безпеки. Інтегрована політика кібербезпеки повинна наголошувати на поділі завдань між державою, економікою, науковими колами й громадянським суспільством, зокрема й заходи в таких сферах: політико-стратегічне управління, оцінювання ризиків, запобігання загрозам і забезпечення готовності, визнання й реагування, обмеження наслідків і відновлення, а також розвиток урядових і неурядових можливостей. Політика кібербезпеки має бути проактивною, що означає роботу із запобігання загроз кіберпростору й людям у кіберпросторі або з пом'якшення їхнього впливу («налаштування безпеки»). Політика кібербезпеки також має бути заснована на солідарності, зважаючи на те, що через глобальний характер кіберпростору кібербезпека Австрії, ЄС і всього світового співтовариства тісно взаємозалежна. Тому для гарантування кібербезпеки потрібне інтенсивне співробітництво на основі солідарності на європейському й міжнародному рівні.

Стратегією кібербезпеки Австрії національним координатором і центральним органом у сфері кібербезпеки визначено Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ Австрії (Cyber Crime Competence Center (C 4) of the Federal Ministry of the Interior). Крім того, на нього покладено головні функції щодо здійснення правоохоронної діяльності у сфері кібербезпеки та боротьби з кіберзлочинністю [15].

Ірландію, де розташовані великі європейські офіси таких компаній, як Google і Facebook, часто називають європейською Кремнієвою долиною, оскільки ця країна докладає багато зусиль для підготовки та працевлаштування IT-фахівців. 2013 р. компанія Microsoft проінвестувала 170 мільйонів євро у створення та розвиток європейського дата-центру в Ірландії. Ця ініціатива була підтримана місцевою владою, адже Ірландія прагне стати європейським лідером у сфері оброблення bigdata, а її кліматичні умови підходять для підтримки необхідної температури роботи серверів. Також у Дубліні має з'явитися тренінговий центр, який у тісному співробітництві з урядом Ірландії та навчальними закладами проводитиме навчання в таких перспективних галузях, як захист критичної інфраструктури й кібербезпека транспорту [16]. Національна стратегія кібербезпеки Ірландії на 2015–2017 рр. передбачає, що уряд Ірландії всіляко сприятиме стійкій та безпечній експлуатації комп'ютерних мереж і відповідної інфраструктури ірландськими громадянами й підприємствами. Розвиток і поширення інформаційно-комунікаційних технологій призвів до значного поліпшення якості життя, появі інноваційних послуг і радикальних змін в організації бізнесу, тому держава, критична інфраструктура, юридичні особи й громадяни залежать від надійного функціонування інформаційно-комунікаційних технологій та Інтернету. Порушення роботи цих систем, незалежно від джерела, створює безпосередню загрозу функціонуванню держави й економіки, і може суттєво вплинути на повсякденне життя мільйонів громадян. Тому будь-яка загроза безпеці кіберпростору вимагає надійного й послідовного реагування як на національному, так і на міжнародному рівні. Із цією метою Ірландія повинна: підвищити стійкість і надійність критично важливої інформаційної інфраструктури в найважливіших секторах економіки, і особливо в державному секторі; продовжувати взаємодію з міжнародними партнерами, аби кіберпростір залишався відкритим, безпечним, цілісним і безкоштовним, а також здатним сприяти економічному та соціальному розвитку; підвищувати обізнаність про відповідальність бізнесу й приватних осіб за безпеку своїх інформаційних мереж, інфраструктури та даних, а також підтримувати таку обізнаність за допомогою інформації, навчання й узагальнення практики; забезпечувати для державних органів всеосяжні та гнучкі нормативно-правові межі для боротьби з кіберзлочинністю, які були б доречними та співрозмірними з потребами захисту «чутливих» або особистих даних; створювати потенціал для органів влади та приватного сектора для функціонування й аварійного управління в умовах кіберінцидентів.

Висновки. Аналіз, оцінка та використання позитивних здобутків європейських країн мають велике значення під час розбудови системи гарантування інформаційної безпеки України, адже наразі наша країна стикається з новими викликами та загрозами в інформаційній сфері та перебуває на стадії становлення інформаційного суспільства, яка супроводжується стрімким розвитком інформаційної інфраструктури.

Сьогодні країни позаблокового статусу усвідомлюють безпосередню залежність свого добробуту від інформаційної сфери, тому питання гарантування інформаційної безпеки закономірно посідає одне з чільних місць у безпекових стратегіях відповідних держав. Водночас політика гарантування інформаційної безпеки позаблокових країн має проактивний характер і спирається на

засади управління ризиками інформаційної безпеки, передусім – кібербезпеки.

Досвід зміни парадигми гарантування національної безпеки з реактивної на проактивну для України в контексті її євроінтеграційного спрямування є надзвичайно важливим, адже дозволяє правильно визначати стратегічні пріоритети й оптимізувати зусилля щодо гарантування інформаційної безпеки, а також сприятиме плідному співробітництву з усіма європейськими країнами в розбудові систем регіональної та міжнародної інформаційної безпеки. Не менш важливим цей досвід є і для подальшої розбудови теорії національної безпеки і теоретичних засад гарантування інформаційної безпеки. Зокрема, до перспективних напрямів наукових пошуків належить, передусім, дослідження у сфері оцінювання загроз інформаційній безпеці України та методів управління ризиками в інформаційній сфері.

### *Література*

1. Політанський В. Світові моделі та фундаментальні принципи інформаційного суспільства / В. Політанський // Науковий вісник Ужгородського національного університету. Серія «Право». – Випуск 43. – Т. 1. – 2017. – С. 34–39.

2. Federal Acton Data Protection (FADP) of 19 June 1992 [Електронний ресурс]. – Режим доступу : https://www.admin.ch/opc/en/classified-compilation/19920153/ index.html.

3. Швейцария признала незаконным сбор IP-адресов в интересах правообладателей [Электронный ресурс]. – Режим доступа : http://www.itsec.ru/newstext.php?news_id=70187.

4. National strategy for Switzerland's protection against cyber risks [Електронний ресурс]. – Режим доступу : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf.

5. Федеральный совет Швейцарии прокомментировал закон об информационной безопасности [Электронный ресурс]. – Режим доступа : http://goldblum.eu/ru/pravovye-novosti/federalnyy-sovet-shveycarii-prokomm/.

6. Information Technology Security Evaluation Criteria [Електронний ресурс]. – Режим доступу : https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf.

7. Common Criteria for Information Technology Security [Електронний ресурс]. – Режим доступу : https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf.

8. Communication from the Commission : Towards a general policy on the fight against cyber crime. COM (2007) [Електронний ресурс]. – Режим доступу : http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf

9. ENISA Country Reports [Електронний ресурс]. – Режим доступу : http://www.epractice.eu/ files/media/media2624.pdf.

10. CERT-Fi [Електронний ресурс]. – Режим доступу : http://www.cert.fi/en/index.html.

11. Communication from the Commission on Critical Information Infrastructure Protection : Protecting Europe from larges cale cyber-attacks and disruptions : enhancing preparedness, security and resilience (2009) [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ index_en.htm.

12. В Финляндии открылся центр информационной безопасности [Электронный ресурс]. – Режим доступа : http://www.goodnewsfinland.ru/cgi-otkryvaet-v-finlyandii-novyj-tsentr-informatsionnoj-bezopasnosti/.

13. Finland's Cyber Security Strategy (2013) [Електронний ресурс]. – Режим доступу : http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy.

14. Austrian Security Strategy (2013) [Електронний ресурс]. – Режим доступу : https://www.bka.gv.at/DocView.axd?CobId=52251.

15. Austrian Cyber Security Strategy (2013) [Електронний ресурс]. – Режим доступу : https://www.bka.gv.at/DocView.axd?CobId=50999.

16. Microsoft вложит в дата-центр в Ирландии дополнительные 170 млн. евро [Электронный ресурс]. – Режим доступа : https://www.bka.gv.at/DocView.axd?CobId=52251http://www.itsec.ru/newstext.php?news_id=97395.

### Анотація

***Ткачук Т. Ю.* Забезпечення інформаційної безпеки в країнах позаблокового статусу.** – Стаття.

Стаття присвячена дослідженню політики й системи гарантування інформаційної безпеки в країнах позаблокового статусу. Під час дослідження визначаються пріоритети та проблеми гарантування інформаційної безпеки в зазначених країнах. Також оцінюється значущість досвіду країн позаблокового статусу у досліджуваній сфері для України.

*Ключові слова:* інформаційна політика, інформаційна безпека, безпека інформації, кібербезпека, країни позаблокового статусу.

### Аннотация

***Ткачук Т. Ю.* Обеспечение информационной безопасности в странах внеблокового статуса.** – Статья.

Статья посвящена исследованию политики и системы обеспечения информационной безопасности в странах внеблокового статуса. В ходе исследования определяются приоритеты и проблемы обеспечения информационной безопасности в указанных странах. Также оценивается значимость опыта стран внеблокового статуса в сфере обеспечения информационной безопасности для Украины.

*Ключевые слова:* информационная политика, информационная безопасность, безопасность информации, кибербезопасность, страны внеблокового статуса.

### Summary

***Tkachuk T. Yu.* Information security ensuring in the non-aligned countries.** – Article.

The article is devoted to the research of the policy and system of information security in the non-aligned countries. The study identifies priorities and problems of ensuring information security in the se countries. The importance of the experience of non-aligned countries in the field of information security for Ukraine is also assessed.

*Key words:* information policy, information security, information security, cyber security, non-aligned countries.