УДК 327.5 (540+510+549)

Сябро А.В.*

ОСОБЛИВОСТІ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ ІНДІЇ

Анотація. *Інформаційний розвиток і впровадження нових технологій стали важливою складовою стратегії модернізації Індії. У статті показано, що держава має високі показники використання інтернету та онлайн послуг, але рівень розвитку кібербезпеки залишається незначним. Це обумовлює актуалізацію питання кібербезпеки як на національному, так й на міжнародному рівні. Доведено, що неефективність впровадження стратегії може негативно вплинути на подальший розвиток інформаційного сектору економіки Індії. У статті також розглянуто питання кіберзахисту та кібероборони. Окреслено сучасні проблеми двосторонніх відносин Індії та Китаю у сфері кібербезпеки, досліджено особливості використання кіберпростору як нового простору боротьби між Індією та Пакистаном.*

Ключові слова: *кібербезпека, кібероборона, кіберзагроза, кібертероризм, інформаційний суверенітет, ООН, Індія, Пакистан, Китай.*

Abstract. *Information development and the introduction of new technologies became an important part of India's modernization strategy. The article shows that the state has high rates of the Internet usage and online services, but the level of cybersecurity development remains low. This causes the updating of cybersecurity issues at both the national and international level. It is proved that ineffective implementation of the strategy can negatively affect the further development of the information sector of the Indian economy. The article also addresses cybersecurity and cyber defense issues. The current problems of*

* аспірантка кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.

India-China bilateral relations in the field of cybersecurity are outlined and the features of the cyberspace usage as a new space of struggle between India and Pakistan are explored.

Key words: *cyber security, cyber defense, cyber threat, cyber terrorism, information sovereignty, UN, India, Pakistan, China.*

Аннотация. Информационное развитие и внедрение новых технологий стали важной составляющей стратегии модернизации Индии. В статье показано, что государство имеет высокие показатели использования интернета и онлайн услуг, но уровень развития кибербезопасности остается незначительным. Это обусловливает актуализацию вопроса кибербезопасности как на национальном, так и на международном уровне. Доказано, что неэффективность внедрения стратегии может негативно повлиять на дальнейшее развитие информационного сектора экономики Индии. В статье также рассмотрены вопросы киберзащиты и кибероборонны. Определены современные проблемы двусторонних отношений Индии и Китая в сфере кибербезопасности, исследованы особенности использования киберпространства как нового пространства противостояния между Индией и Пакистаном.

Ключевые слова: *кибербезопасность, кибероборона, киберугрозы, кибертерроризм, информационный суверенитет, ООН, Индия, Пакистан, Китай.*

Постановка проблеми. В сучасних умовах бурхливого інформаційного та науково-технологічного розвитку для більшості країн АТР постає питання вироблення ефективних механізмів захисту від нових викликів та загроз для системи національної безпеки. Держави-лідери регіону, усвідомлюючи потенційні наслідки цього процесу, прагнуть виробити ефективні стратегії інформаційної безпеки та механізми реалізації національних пріоритетів в цій галузі. Проте, не всі країни здатні,

використовуючи позитивний досвід інших, швидко розгорнути ефективну систему національної інформаційної безпеки. Зокрема, Індія, яка є визнаним лідером інноваційного і науково-технічного розвитку, у 2019 р. за даними аналітичних досліджень була визнана однією з найменш захищених країн у сфері кібербезпеки. Тому для подальшого розвитку держави розробка ефективної стратегії кібербезпеки і оперативне впровадження механізмів її реалізації стали нагальним питання, що обумовлює подальший розвиток держави в цілому, з огляду на високі темпи її інформатизації та впровадження різноманітних цифрових проектів в рамках електронного державного управління.

Мета статті полягає у дослідженні особливостей трансформації стратегії інформаційної безпеки Індії, визначенні базових пріоритетів політики у сфері інформаційної безпеки держави, з'ясування внутрішніх і зовнішніх чинників, що впливають на сучасні підходи до вирішення проблеми індійської національної інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Дослідження проблеми кібербезпеки країн АТР, зокрема, Індії, є вкрай актуальним, оскільки вони є лідерами інформаційного розвитку і демонструють високі темпи проникнення технологій і мереж у всі сфери життєдіяльності суспільства. Водночас, як свідчать численні аналітичні дослідження, саме ці країни нині найбільше потерпають від відсутності ефективних механізмів захисту від сучасних викликів і загроз, що є високотехнологічними і мають транскордонний характер. Отже, для Індії постає питання вироблення ефективної стратегії національної політики у сфері кібербезпеки. Оскільки процес ще триває і не набув завершено форми, а перебіг реалізації має суперечливий характер, дослідження феномену відбувається фрагментарно і не мають системного характеру. Так, загальні питання інформаційної безпеки держав, у тому числі, Індії, розглядаються у роботах таких зарубіжних та вітчизняних авторів – Зб. Бжезинського, М. Лібіцкі, Дж. Ная, У. Оуенса, О. Тоффлера, О. Манойла, Д.Дубова, О.Ожевана, Г. Почепцова

та ін. Дослідження проблеми ухвалення міжнародних документів у сфері інформаційної безпеки та ролі Індії у цьому процесі здійснили Р. Гурвітц, С. Бойко, О. Демідов, І. Кванталіані, А. Крутских, О. Маслакова, Н. Ромашкіна, В. Шерстюк, Є. Макаренко, О. Фролова та ін. Особливості впровадження стратегії кібербезпеки Індії досліджено у працях П. Вагрі, Н. Десаі, С.Кумара, Ш.Мехти, Р.Муді, Р.Сантанами та ін.

Виділення невирішених раніше частин загальної проблеми. Проблема кібербезпеки постає як нагальна для багатьох країн АТР, у тому числі, й для Індії. Бурхливий інформаційний і технологічний розвиток держави призвів до зростання кількості користувачів мереж і технологій. При цьому система захисту від загроз, які відтепер виникають для населення і бізнесу, не є ефективною. Отже, визначення проблем, що обумовлюють зростання актуальності питання вироблення стратегії кібербезпеки держави, чинників, які впливають на цей процес, дозволяє не тільки визначити причини виникнення небезпеки, але й визначити реальні і потенційні наслідки для забезпечення безпеки в економічній, політичній, суспільній та воєнній сферах. Власне така невизначеність для самої Індії призводить до формування особливої позиції держави й на міжнародній арені у вирішенні питань глобальної кібербезпеки та на рівні двосторонніх відносин, зокрема, з КНР та Пакистаном. Отже вивчення проблем, що впливають на ефективність реалізації стратегії національної кібербезпеки Індії із врахуванням комплексу як зовнішніх, так й внутрішніх чинників, є актуальним і заслуговує на більш ґрунтовне дослідження.

Виклад основного матеріалу дослідження. Сучасна політика інформаційної безпеки Індії формується під впливом цілої низки факторів. Першим і найбільш вагомим є пришвидшення інноваційного науково-технологічного розвитку, наслідком якого є широке впровадження технологій у всі сфери життєдіяльності індійського суспільства. Так, ще у 2014 р. інтернетом в Індії користувалося менше 20 % населення, яке становило за офіційними даними бл.1,2 млрд осіб. Основною проблемою

таких повільних темпів проникнення технології стали висока вартість послуг та бюрократизм і широкі можливості втручання держави у роботу телекомунікаційних компаній. Але вже у 2019 р. Індія посіла друге місце у світі за кількістю інтернет-користувачів, яких нараховується понад 560 млн.осіб, а рівень проникнення технологій становить бл. 41% [1]. Високим є й показник кількості користувачів смартфонами (345,92 млн.осіб), що надають можливість використовувати мобільний інтернет та онлайн-послуги [2; 3].

Важливим етапом в інформаційному розвитку Індії стало прийняття у 2015 р. національної програми «Цифрова Індія», покликаної забезпечити електронний доступ населення до державних послуг шляхом розвитку інтернету та удосконалення інфраструктури зв'язку [4]. Основними завданнями Програми стали: забезпечення кожного можливістю широкосмугового доступу, сприяння поширенню мобільних технологій, створення системи надання цифрових державних послуг, створення нової моделі економічної діяльності, що базується на послугах, розвиток соціальних медіа, розвиток освіти та навчання, нові можливості для молоді тощо. До пріоритетних сфер діяльності було віднесено: розвиток цифрової економіки, створення системи цифрової ідентифікації особистості (система Aadhaar охопила у 2019 р. понад 90 % населення), розбудова електронного державного урядування (реалізація програми e-Kranti: National e-Governance Plan 2.0), сприяння розвитку смарт-міст [5]. Таким чином програма мала на меті суттєво змінити інформаційну інфраструктуру держави і суттєво розширити цифрові можливості усіх громадян Індії. За прогнозами експертів, до 2020 р. понад 140 млн індійців завдяки реалізації «Цифрової Індії» отримують доступ до мобільних фінансових сервісів, а 75 млн. дітей зможуть скористатися можливостями онлайн-навчання [4]. На сучасному етапі Програма зорієнтована на розширенні можливостей доступу до онлайн-послуг у сфері державного управління, освіти та медичного

обслуговування, а також впровадження ринку криптовалюти та підвищення загального рівня цифрової готовності держави [6].

Нині Індія не тільки продовжує успішно втілювати пріоритети програм цифрового розвитку у всі сфери життєдіяльності суспільства, але й виступає активним гравцем на світовому і регіональному ринку інформаційних продуктів та послуг. Так, згідно з даними, представленими у звіті Національної асоціації компаній з виробництва програмного забезпечення та ІТ-послуг, прибутки галузі у 2017-2018 рр. склали 125 млрд. дол. США, темпи зростання становлять 16 %, кількість зайнятих – бл. 4 млн. осіб, а ще майже 9 млн. були залучені у суміжні галузі. Як наслідок – відбулося суттєве зростання долі цього сектору у ВВП країни – з 1,2% у 1998 р. до 7,7% у 2017 р. [7].

Водночас, незважаючи на такі темпи інформаційного розвитку, Індія суттєво відстає у розвитку системи інформаційної безпеки. Це ставить під загрозу усі досягнення держави, оскільки при такому рівні інформатизації безпека перетворюється на визначальний фактор подальшого розвитку суспільства. Як зазначають експерти, Індія має достатньо високий рівень системи правового регулювання сфери інформаційної безпеки, але при цьому демонструє високі показники рівня інформаційних загроз, зокрема, зараження шкідливими програмними продуктами комп’ютерів та мобільних пристроїв, атаки на фінансові установи та банківські структури, незахищеність ринку криптовалюти тощо [8].

Інформаційні атаки стають дедалі більш руйнівними за масштабами враження та наслідками їх застосування. Така ситуація може призвести до поглиблення багатьох проблем не тільки у сфері власне інформаційної безпеки, а й у сфері політичної, економічної, суспільної безпеки Індії, оскільки об’єктами нападів стають критично важливі елементи інфраструктури суспільства. Під загрозою опиняються такі важливі національні ініціативи, як «Розумні міста», «Електронне управління», «Управління цифровою публічною ідентичністю», від реалізації яких

залежить ефективність стратегії розвитку держави загалом. До того ж Індія вважається одним з кращих місць для аутсорсингу в усьому світі, тому ключові світові бренди – Apple, Sapient, Citi Bank, HSBC, Bank of America, DSM та ін. – створили свої глобальні центри доставки, центри обслуговування та сервісної підтримки в Індії [6]. Тому недостатній рівень інформаційної безпеки може вплинути не тільки на саму країну, але й на міжнародних бізнес-партнерів, інтереси яких страждатимуть внаслідок кібератак або неефективність стратегій швидкого реагування на них.

Перші кроки індійського уряду у сфері кібербезпеки безпеки, зокрема, щодо вироблення практичних механізмів захисту національного кіберпростору відносяться до 2004 р., коли було створено спеціалізований підрозділ «Індійська команда реагування на надзвичайні ситуації в Інтернеті (CERTIn), який мав функціонувати як національне агентство з реагування на інциденти в кіберпросторі. У 2000 р. уряд Індії прийняв Закон про інформаційні технології для формування нормативної бази стратегії кібербезпеки держави. Цей закон залишається базовим правовим актом у сфері регулювання питань національної інформаційної безпеки і постійно оновлюється відповідно до нових аспектів (зокрема, у 2008 р.), які включаються до пріоритетів національної політики з кібербезпеки [9; 10]. Так, у законі визначаються такі загрози для сфери національної інформаційної безпеки: навмисне втручання у роботу систем і мереж та несанкціонований доступ до електронних документів, злом комп'ютерної системи, викрадення персональних даних, паролів та кодів доступу до персональної і банківської інформації, поширення персональної інформації без дозволу її власника, кібершахрайство, кібертероризму, поширення забороненої інформації, зокрема, порнографічного характеру тощо. Враховуючи зростання масштабів кіберзагроз для системи національної безпеки Індії, Закон надає уряду держави широкі можливості впровадження цензури та здійснення державного контролю за інформаційною діяльністю громадян [9].

У 2012 р. під час Мюнхенської конференції з безпеки індійські фахівці у сфері ІКТ заявили, що працюють над створенням власних мікропроцесорів і планують скорочення імпорту програмного забезпечення у військовій сфері та збільшення інвестицій у власні розробки. У тому ж році було запропоновано створити центр командування і контролю для моніторингу критичної інфраструктури та ліквідації прогалин у кіберзахисту [11].

Вже у 2013 р. ситуація почала стрімко змінюватися. Поштовхом став інцидент з Е.Сноуденом та публікація документів, що свідчили про тотальне спостереження та здійснення кібероперацій спецслужбами США, спрямованими як на вороже налаштовані країни, так й на союзників. Як наслідок, Індія, яка також потрапила до переліку держав, які опинилися в зоні уваги американських спецслужб, незважаючи на свій статус держави-союзника, була змушена прискорити процес розробки національної стратегії у сфері кібербезпеки. «Національна політика у галузі кібербезпеки» стала першим індійським доктринальним документом, покликаним забезпечити комплексне бачення пріоритетів держави, приватного сектору та суспільства щодо вирішення питань кібербезпеки, а також закласти основи для систематизованої та узгодженої діяльності усіх зацікавлених сторін задля втілення пріоритетів на практиці. Отже, «Національна політика» стала важливим етапом на шляху створення індійської національної стратегії кібербезпеки, розробка якої розпочалася у тому ж 2013 р. Слід зазначити, що документ переважно розрахований на вирішення внутрішньополітичних питань, а питання міжнародного співробітництва з метою підвищення ефективності протистояння кіберзагрозам та боротьби з транснаціональною кіберзлочинністю було вирішено представити в окремих документах [11].

Основними принципами стратегії стали: трансформація сприйняття проблеми кібербезпеки та надання цим питанням першочергового значення; розширення підходів до вирішення проблеми кібербезпеки, яку не слід звужувати лише до технічних питань попередження або ліквідації наслідків

кібератак, при цьому система повинна стати гнучкою, динамічною і швидко адаптуватися до нових викликів і загроз; підготовка спеціалістів, здатних ефективно протистояти загрозам у кіберпросторі; включення безпеки як фундаментального принципу концептуального проектування, у тому числі, у сфері розбудови інформаційної інфраструктури.

Основні цілі реалізації стратегії полягали у наступному: створити ефективну систему захисту персональної інформації громадян Індії, фінансової і банківської інформації та дані, що мають значення для державного управління і безпеки, від несанкціонованого доступу та кібератак; досягнути високого рівня надійності роботи ІКТ-систем та їх повномасштабного впровадження в усі сектори економіки; підготувати необхідну кількість (близько 500 тисяч) професіоналів протягом наступних 5 років для підвищення рівня безпеки та надійності інформаційного простору держави [12].

Забезпечення кібербезпеки відбувається у таких сферах діяльності: кібербезпека, кіберзахист, кіберрозвідка. Так, відповідно до положень документу, кібербезпека розглядається як діяльність, спрямована на захист інформації та інформаційних систем (мереж, комп'ютерів, баз даних, центрів обробки даних та додатків) із застосуванням відповідних процедурних та технічних заходів безпеки. У цьому сенсі поняття кібербезпеки є доволі широким і охоплює усі види діяльності із захисту. Кіберзахист тлумачиться у документі як більш вузький вид діяльності, пов'язаний з певними аспектами та організаціями. Основна відмінність між кібербезпекою та кіберзахистом у мережевому середовищі полягає у характері загроз для того, що має бути захищеним з використанням усього спектру доступних інструментів. Кіберзахист відноситься до оборонних дій, спрямованих на протидію деструктивній діяльності ворожих акторів, які мають політичну, квазіполітичну або економічну мотивацію, що впливає на національну безпеку, громадську безпеку або економічний розвиток суспільства [12].

Як зазначалося у документі, реалізація цілей у сфері кібербезпеки потребує таких практичних кроків: підвищення рівня обізнаності щодо загроз інфраструктурі ІКТ для оперативного визначення та реалізація відповідного типу реагування; створення сприятливого правового середовища для підтримки безпечного кіберпростору, підвищення рівня довіри та впевненості в електронних транзакціях, посилення повноважень правоохоронних органів, що має забезпечити можливість підвищення рівня відповідальності за протиправні дії та притягнення до відповідальності винних; захист ІКТ-мереж та критично важливих елементів інформаційної інфраструктури; введення механізму оперативного реагування на кіберінциденти, надзвичайні ситуації у кіберсередовищі в режимі 24/7; реалізація політики у сфері кібербезпеки, дотримуючись міжнародних норм і стандартів; створення культури кібербезпеки та відповідальної поведінки у кіберсередовищі тощо [12].

Для досягнення поставлених цілей було створено відповідну структуру організацій, установ та відомств, базових пріоритетом діяльності яких стала кібербезпека, зокрема, Національний центр координації кіберпроблем, Національний центр захисту критичної інформаційної інфраструктури, а також окремі галузеві команди реагування на надзвичайні ситуації в рамках CERTIn тощо. Уряд Індії також ухвалив Національний план управління кризовими ситуаціями щодо боротьби з кібератаками та кібертероризмом, який оновлюється щороку відповідно до нових реалій у сфері кібербезпеки [6].

Починаючи з 2011 р. Індія також активно включилася у міжнародні дискусії щодо кібербезпеки. Зокрема, у питаннях управління інтернетом держава зайняла власну позицію – між мультилатералізмом та мультистейкхолдерізмом – «нюансовий мультилатералізм», коли проводяться консультації з широким колом зацікавлених сторін, але вони не беруть участь у впровадженні обговорюваних механізмів. У питаннях суверенітету в кіберпросторі, Індія тяжіє до позиції Росії та Китаю, але

утримується від остаточного рішення та безумовної їх підтримки, намагаючись знайти свій варіант вирішення дилеми між прибічниками «жорсткого» контролю діяльності держав у кіберсередовищі та «м'якого» регулювання проблеми [13]. Беручі активну участь в обговоренні резолюції ГА ООН «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки», Індія представила свою позицію з цієї проблеми у 2016 р. та 2018 р.[14; 15]. Так, індійська позиція, представлена у 2016 р. базувалася на визнанні ролі і значення технологічного прогресу, особливо для економічного і соціального розвитку держав світу. Водночас, як підкреслюється у позиції держави, збільшення кількості і масштабів загроз для кібербезпеки, ставить на порядок денний питання вироблення ефективних механізмів забезпечення відкритого і безпечного кіберсередовища, досягнути яке можливо у тому числі завдяки вироблення загальних правил поведінки держав у кіберпросторі [14].

На початку 2019 р. Індія стала жертвою двох кібератак на критично важливі елементи інфраструктури – атомну електростанцію Куданкулам та Індійську організацію космічних досліджень. І хоча суттєвих збитків або шкоди атаки не завдали, цього виявилося достатньо для того, щоб Індія продовжила активну участь в обговоренні проблем кібербезпеки на всіх рівнях міжнародного співробітництва. Як й у випадку з міжнародним тероризмом та захистом навколишнього середовища, співпраця є необхідною умовою боротьби з кіберзагрозами з огляду на їх транскордонний характер. У Національній політиці кібербезпеки 2013 р. ці аспекти не були враховані, як й не був створений механізм моніторингу та оцінки ефективності виконання поставлених завдань. Тому, реалізація пріоритетів набула дещо хаотичного характеру, що призвело до неспроможності держави досягнути значну кількість поставлених завдань. Отже, ці недоліки Індія планує усунути під час реалізації нової Національної політики у сфері кібербезпеки на 2020-2025 рр. [13].

У 2018 р. Індія також розпочала реалізовувати ініціативу щодо створення власної кібероборони. Так, було утворено військову агенцію з питань кібербезпеки – Оборонну кіберагенцію, яка має співпрацювати з апаратом національного радника з питань безпеки. Планувалося, що агенція дозволить готувати тисячі експертів, які забезпечуватимуть кібербезпеку армії, ВМС та ВПС країни, а також здійснюватимуть наступальні операції у кіберпросторі. У майбутньому ця структура має перетворитися на повноцінне кіберкомандування. Нині апарат агенції займається розробкою доктрини кібероперацій. Важливим є також зрушення у сфері кіберрозвідки. Так, результатом співпраці Центральних резервних поліцейських сил, Прикордонної служби та стартапа Innefu було створено платформу Prophecy, яка складається з декількох інструментів, що дозволяють аналізувати великі масиви інформації, здійснювати моніторинг соціальних мереж, ідентифікувати людей, в тому числі в режимі реального часу. Отже, індійські розробники створили продукт, який можна використовувати у розвідувальних і контррозвідувальних цілях для аналізу величезних масивів інформації [11].

Таким чином, усвідомлюючи факт появи нових типів загроз для системи національної безпеки, в Індії розпочали створювати необхідні засоби реагування на сучасні кіберзагрози із врахуванням реалій кібервійни, тобто як війни, що ведеться незважаючи на державні кордони, із застосуванням дій, які не регулюються існуючими міжнародно-правовими документами, що дозволяє державам-ініціаторам інформаційної агресії приховати свою причетність до кібератак. При цьому індійська влада, яка дедалі більшу увагу почала приділяти проведенню оборонних і наступальних операцій в кіберпросторі, намагається знизити залежність від інструментів іноземного походження і спиратися в цьому питання переважно на використання продуктів вітчизняного виробництва [11].

На думку експертів, на даний момент ключовими супротивниками Індії в кіберпросторі вважаються Пакистан і Китай. Наприклад, КНР постійно

здійснює повномасштабні кібероперації проти Індії, які вже набули такого розмаху, що іноді можуть бути охарактеризовані як повномасштабна кібервійна. Так, у травні 2016 р компанія Symantec повідомила про атаку на низку індійських ресурсів, здійснену китайської групою кібершпигунів Suckfly. Об'єктами несанкціонованого доступу стали інформаційні системи центрального уряду і великих фінансових інституцій. Але витік даних почалася ще у квітні 2014 р. і тривав протягом усього 2015 р. Метою кібершпигунської діяльності, на думку представників Symantec, є підрив економічної інфраструктури Індії. У своїй роботі Suckfly використовує шпигунські програми або застосовує шкідливе програмне забезпечення Backdoor.Nidoran. Того ж року компанія KasperskyLab заявила, що відстежила вторгнення групи кібершпигунів Danti в системи центрального уряду Індії по каналах, що використовують дипломатичні відомства [16]. Отже, протистояння між державами може набувати різних форм – від злому індійських мереж до проявів кіберзлочинності і кібертероризму; але при цьому Пекін і Нью-Делі на офіційному рівні продовжують зміцнювати відносини не тільки в політичній і військовій сфері, а й у сфері кібербезпеки.

Більш активним є протистояння у кіберпросторі між Індією і Пакистаном. Незважаючи на те, що експерти оцінюють можливості обох країн вести кібервійну як досить обмежені, вони активно вдаються до різноманітних засобів протистояння, особливо під час ескалації двостороннього конфлікту у політичній площині. Як правило, пакистанські спецслужби або організують злом сайтів індійських відомств і пов'язаних з державою компаній (подібні операції завдають порівняно малий збиток), або через інтернет вербують діючих співробітників індійських силових структур для інсайдерської діяльності. Двосторонній кіберконфлікт часто переходить у форму подання недостовірної інформації, новин або чуток через Facebook та мессенджери, зокрема, WhatsApp, що призводить до проблеми мілітаризації соцмереж. Програмне забезпечення, розроблене

Пакистаном та приховане у спеціально створених фейкових блогах та новинних сайтах, може активувати веб-камери, викрадати інформацію, що передається через електронну пошту, робити знімки екрана комп'ютерів жертв. Індія ж розробила складну технологію шпигування, що використовується на платформі Android, яка вважається найбільш популярною мобільною операційною системою в регіоні [17].

Найбільшу небезпеку сьогодні становить використання соцмереж та мессенджерів для впливу на масову аудиторію обох країн. Як показують статистичні дані, у 2018 р. в Індії кількість користувачів соціальними медіа становила понад 326 млн. осіб, а рівень проникнення – майже 31 %. Найбільш популярним ресурсом є Facebook, на який припадає понад 50 % відвідувань інтернету користувачами, а кількість індійських власників аккаунтів у 2019 р. нараховувалося понад 323 млн. осіб. Зростання популярності спілкування у соціальних мережах через мобільні пристрої призвело то зростання кількості користувачів додатків типу WhatsApp до 70 млн. осіб лише у 2014 р. [18].

Таке швидке зростання кількості користувачів інтернет-сервісами позитивно оцінюється з погляду розвитку електронної комерції та цифрової економіки, але для сфери інформаційної безпеки така статистика викликає занепокоєння. Наприклад, уряд Індії був змушений у 2018 р. обмежити використання WhatsApp внаслідок хвилі масових вбивств, спровокованих поширенням фейкових новин серед користувачів сервісу [19].

Висновок. Стратегія національної інформаційної безпеки Індії має свої унікальні характеристики, що обумовлює достатньо специфічні підходи уряду держави до вирішення питання безпеки у кіберсередовищі. Так, з одного боку, держава активно розвиває інформаційний сектор, орієнтуючись на інноваційні технології і намагаючись максимально посилити власні технічні спроможності для забезпечення попиту на технології та інформаційні послуги всередині країни. Значні масштаби інформатизації та проникнення технологій і онлайн-сервісів на сучасному

етапі призвели до актуалізації питання інформаційної безпеки, вирішення якого повинно позитивно вплинути на подальший розвиток держави. Індія бере активну участь у міжнародних структурах, зокрема, системи ООН, з метою вироблення ефективних міжнародно-правових механізмів, які б дозволили удосконалити як міжнародну, так й національну систему інформаційної безпеки. З другого ж боку, держава все ще залишається у групі країн, які нездатні ефективно протистояти викликам і загрозам інформаційної доби, потрапляючи у рейтинг найменш інформаційно захищених держав. Це негативно впливає на загальні темпи розвитку держави і робить її інформаційний простір недостатньо прозорим і безпечним. Критиці піддається й політика державних структур, які сьогодні схильні вживати «жорсткі» механізми контролю замість «м'яких» механізмів регулювання. Показовою у цьому плані є підтримка Індією Правил поведінки держав у кіберпросторі, запропонованих Росією і Китаєм. Водночас, прагнучі зайняти гідне місце серед держав, які використовують свою кібермогутність для обстоювання національних інтересів на міжнародній арені, Індія продовжує розвивати і модернізувати стратегію кібербезпеки, про що свідчить рішення ухвалити нову стратегію у сфері кібербезпеки на 2020-2025 рр.

Список використаних джерел

1. Internet world stats, 2019. *Top 20 countries with the highest number of internet users.* – [online]. Available at: <https://www.internetworldstats.com/top20.htm> [Accessed 21 November];

2. Holst, A., 2019. *Smartphone users by country worldwide 2019.* – [online] (October 23). Available at: <https://www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users/> [Accessed 30 December];

3. Holst, A., 2019. *Smartphone penetration rate by country 2019.* – [online] (October 23). Available at:

<https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/>[Accessed 27 December];

4. CISCO, 2016. *Цифровая революция в Индии*. – [online]. Доступно: <https://www.cisco.com/c/ru_ua/about/press/2016/0222i.html> [Дата звернення 20 грудня 2019];

5. Digital India, 2015. – [online]. Available at: <https://www.digitalindia.gov.in> [Accessed 27 December];

6. Rijksdienst voor Ondernemend Nederland, 2018. *Cyber Security in India. Opportunities for Dutch companies* – [online]. Available at: < https://www.thehaguesecuritydelta.com/media/com_hsd/report/218/document/Cyber-Security-in-India.pdf > [Accessed 21 November];

7. Устюжанцева, О., 2018. *Информационно-коммуникационные технологии Индии: история отрасли, факторы успеха*. [online]. Доступно: <https://www.academia.edu/37810136/Информационно-коммуникационные_технологии_Индии_история_отрасли_факторы_успеха > [Дата звернення 24 грудня 2019];

8. Moody, R., 2019. *Which countries have the worst (and best) cybersecurity?* – [online]. Available at: <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/> [Accessed 13 December];

9. Ministry of Law, Justice and Company Affairs (Legislative Department), 2000. *The Information Technology Act*. – [online]. Available at: <https://meity.gov.in/writereaddata/files/itbill2000.pdf> [Accessed 26 November];

10. Ministry of Law And Justice, 2008. *The Information Technology Act (Amendment)* . – [online] Available at: <https://meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf> [Accessed 21 November].

11. Куприянов, А., 2019. *Индия в эпоху кибервойн*. – [online] (25 июля). Доступно: <https://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyn/#detail>> [Дата звернення 20 січня 2019];

12 Ministry of Electronics & Information Technology, Government of India, 2013. *National Cyber Security Policy-2013*. – [online] Available at: <https://meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf> [Accessed 21 November];

13. Waghre, P. and Mehta Sh., 2019. 'India's National Cybersecurity Policy Must Acknowledge Modern Realities. India's National Cybersecurity Policy must bolster its global ambitions'. *The Diplomat* (December 20) Available at: <https://thediplomat.com/2019/12/indias-national-cybersecurity-policy-must-acknowledge-modern-realities/> [Accessed 29 December];

14. United Nations, 2016. *Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General*. – [online]. Available at: <https://undocs.org/A/71/172> [Accessed 21 November];

15. United Nations, 2018. *Current developments in science and technology and their potential impact on international security and disarmament efforts. Report of the Secretary-General* – [online]. Available at: < https://undocs.org/A/73/177> [Accessed 21 November];

16. Шмыров, В., 2016. *Пакистан и Китай нещадно бьют по правительственным ИТ-системам Индии.* – [online] (27 октября). Доступно: <https://safe.cnews.ru/news/top/2016-10-27_pakistan_i_kitaj_neshchadno_byut_po_pravitelstvennym > [Дата звернення 20 січня 2019]

17. Fazzini, K., 2019. *In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides*. – [online]. (February 27). Available at: <https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html > [Accessed 21 November];

18. STATISTA, 2019. *Number of social network users in India from 2015 to 2023*. – [online]. Available at: <https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/ > [Accessed 29 December].

19. Goel, V., Raj, S. and RavichandranJuly, P., 2018. *How WhatsApp Leads Mobs to Murder in India.* – [online]. Available at: <https://www.nytimes.com/interactive/2018/07/18/technology/whatsapp-india-killings.html > [Accessed 21 November].