

УДК 377.7:35(417)

DOI <https://doi.org/10.32782/apfs.v051.2024.40>**М. М. Марусинець**ORCID ID: <https://orcid.org/0000-0001-7366-9328>

кандидат філологічних наук, доцент,

старший науковий співробітник,

доцент кафедри історії та суспільних дисциплін,

старший дослідник Науково-дослідного центру

імені Тіводора Легоцькі

Закарпатського угорського інституту імені Ф. Ракоці II

## ПОЛІТИКА БЕЗПЕКИ У СФЕРІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В РЕСПУБЛІЦІ ІРЛАНДІЯ

**Постановка проблеми.** В умовах розвитку інформаційно-комунікаційних технологій (ІКТ) і посилення глобалізації світової системи питання, пов'язані з дослідженням політики в галузі інформаційної безпеки, набувають особливої актуальності. Інформаційна безпека є складовою як національної, так і міжнародної безпеки. Забезпечення інформаційної безпеки включає широкий спектр областей, таких як міжнародні відносини, внутрішня та зовнішня політика, економіка, технологічний розвиток, наука та освіта, правоохоронна діяльність, судова система, духовна сфера та інші. Республіка Ірландія є одним із лідерів розвитку ІКТ у світі та в умовах стрімкого розвитку інформаційного суспільства та глобалізації гостро стоїть питання забезпечення її інформаційної безпеки. Членство Республіки Ірландія в ЄС накладає на неї певні обов'язки щодо дотримання стандартів організації в питаннях розвитку інформаційного суспільства та забезпечення інформаційної безпеки.

Стрімкий розвиток інформаційно-комунікаційних технологій призвів до виникнення нових загроз. Кіберзлочинці можуть проводити комплексні комп'ютерні атаки, достатні для нанесення серйозної шкоди державі. Досвід і політика Республіки Ірландії у сфері інформаційної безпеки є прикладом для інших, особливо невеликих держав. Вивчення політики безпеки у сфері ІКТ у Республіці Ірландія важливе для розроблення ефективних заходів зі збереження державного суверенітету і територіальної цілісності країни, а також захисту суспільної системи від протиправної зміни її соціально-економічного або політичного устрою. Країни, особливо невеликі, зацікавлені в розвитку власного сектору інформаційних технологій в економіці, можуть вивчити досвід і підходи уряду Республіки Ірландія. Це дасть їм змогу ухвалити більш обґрунтовані рішення щодо стимулювання, підтримки та забезпечення безпеки розвитку сектору інформаційних технологій у своїх країнах.

**Аналіз останніх досліджень і публікацій.** На сьогоднішній день інформація про формування та

реалізацію політики Республіки Ірландія в галузі інформаційної безпеки представлена у вигляді розрізнених матеріалів. Більшість ключових документів, що стосуються розвитку інформаційно-комунікаційних технологій і кібербезпеки, були розроблені протягом останніх двох десятиліть і доступні для вивчення. Однак наразі констатується відсутність комплексних досліджень, які б систематизували та проаналізували загальний розвиток політики Республіки Ірландія у сфері інформаційної безпеки.

В українській політичній науці тема інформаційної безпеки в контексті розвитку інформаційно-комунікаційних технологій викликає значний інтерес у дослідників. Водночас, Республіка Ірландія як держава у цьому напрямку залишається маловивченою. У сфері наукових досліджень, пов'язаних з інформаційною безпекою Республіки Ірландія, можна виділити значну кількість робіт вчених з Ірландії, Великобританії та США. Серед найбільш значущих робіт у цій галузі слід виділити дослідження таких вчених, як Гопкінс Н., Фальк К., Лібіцкі М., Кушнер Д., Мейварнс Т., Макінтайр Т., Ньюенхем П., О'Донован Б., Вінер Н., Вілмшерст Е.

Важливий внесок у теоретико-методологічне розуміння поняття «кіберпростір» зробив американський математик Вінер Н., який був піонером у галузі інформатики. Як і його сучасники, Вінер Н. опікувався питаннями, які нині належать до галузі міждисциплінарних досліджень. Вінер Н. просуває термін «кібернетика», визначаючи його так: «кібернетика – це уся сфера теорії управління і зв'язку, чи то в машині, чи то в тварині» [1, с. 19]. Наукову спадщину Вінера Н. продовжив британський математик Тьюринг А. та американський математик і фізик угорського походження Джон фон Нейман.

На сучасному етапі розвитку інформаційно-комунікаційних технологій значний внесок у дослідження кіберпростору і кібербезпеки на прикладі Республіки Ірландія зробив американський дослідник ірландського походження

Фальк К. У науковому дослідженні «Безпека в ірландському секторі інформаційних технологій» Фальк К. аналізує механізми, які використовуються урядом Республіки Ірландія для захисту кіберпростору. У цьому дослідженні аналізуються інструменти, які застосовує уряд Республіки Ірландія для забезпечення безпеки інформації в країні. Фальк К. проводить аналіз ефективності заходів, що вживаються урядом Республіки Ірландія для забезпечення безпеки інформаційних ресурсів. У разі виявлення проблем, він пропонує шляхи їх вирішення [2].

Фальк К. пропонує свою інтерпретацію поняття кіберпростору і дає йому визначення. На переконання Фалька К. кіберпростір – це простір, де відбувається обмін і зберігання інформації. У цьому визначенні термін «простір» використовується в математичному сенсі, щоб охопити всі можливі стани, а не лише фізичний простір. Комп'ютерні мережі, мему, паролі, записані на папері, – усі вони пов'язані з кіберпростором, але не мають загальних конкретних характеристик. Сприйняття кіберпростору як невід'ємної складової інформаційного потоку дає змогу йому зберігати свою актуальність, незважаючи на стрімкий розвиток сучасних технологій та інновацій. На переконання Фалька К., якби кіберпростір визначався винятково з погляду конкретних технічних характеристик апаратного або програмного забезпечення, то таке визначення довелося б постійно переглядати [2].

Британський дослідник Вілмшерст Е. у науковому дослідженні «Визначення агресії» вносить ясність у розуміння сутності кібервійни. Вілмшерст Е. зазначає, що Резолюція ООН 3314 (XXIX), стаття 3, визначає війну, зокрема агресивну війну, наводячи список прикладів. Визначальною спільністю між усіма цими прикладами є те, що війна ведеться між двома національними державами. Так, «корпорація «Apple» не може вести війну з корпорацією «Microsoft», оскільки жодна з них не є державою. Така національна держава, як Сполучені Штати, не може вести війну з бідністю, оскільки бідність – це абстрактне поняття» [3].

На думку іншого британського дослідника Лібіцкі М., яку він висловив у рамках фундаментального дослідження «Завоювання в кіберпросторі», кібервійна – це війна між двома національними державами, що ведеться переважно в кіберпросторі. Або, як пояснює Лібіцкі М., це «використання інформації для нападу на інформацію» [4, 49].

У дослідженні американського вченого Кушера Д. «Реальна історія stuxnet» у контексті вищезгаданої роботи Лібіцкі М. наголошується, що «хоча внаслідок кіберконфлікту можуть виникнути фізичні зовнішні ефекти, наприклад

знищені уранові центрифуги», вони мають другорядне значення для визначення кібервійни. Якщо кібервійна може відбуватися тільки між двома національними державами, то «кіберзлочин – це будь-який інший вид кібератаки, включно з шахрайством і крадіжками, псуванням і вандалізмом, зловмисним знищенням майна, хактивізмом та багатьом іншим. Деякі країни дотримуються діалектичної школи філософії і розглядають війну і злочин як рухомі точки на єдиному континуумі конфлікту. Ще більше ускладнює відмінність між війною і злочином проблема атрибуції кібератак» [5].

**Мета статті.** Головна мета дослідження полягає у всебічному аналізі політики безпеки у сфері інформаційно-комунікаційних технологій в Республіці Ірландія, оцінці ефективності заходів, які вживає уряд Республіки Ірландія для захисту інформаційних ресурсів, а також визначенні можливих напрямків для покращення ситуації в цій галузі.

**Виклад основного матеріалу.** У 2013 р. на Всесвітньому економічному форумі кібербезпеки було визнано однією з «найбільш значущих глобальних загроз як із погляду потенційного збитку, так і ймовірності реалізації» [6]. Цей висновок був підтверджений на національному рівні ірландської держави в рамках Національної оцінки ризиків 2014 р., яка виявила, що критична інфраструктура, підприємства і громадяни залежать від надійної роботи інформаційно-комунікаційних технологій (ІКТ), зокрема Інтернету. Збої в роботі цих систем, незалежно від їх джерела, становлять пряму загрозу для держави та економіки, що має серйозні наслідки для повсякденного життя мільйонів людей.

У сучасному світі Інтернет відіграє важливу роль в соціально-економічному розвитку держав, а також має великий потенціал для подальшого прогресу економіки та суспільства. Тому будь-яка загроза його стабільності та безпеці вимагає рішучих і скоординованих дій як на національному, так і на міжнародному рівні, зокрема в рамках ЄС [7]. Інформаційна безпека є однією з найактуальніших проблем, з якою стикаються як Республіка Ірландія, так і інші країни ЄС та світу. У міру розвитку ІКТ зростають і ризики, пов'язаний з інформацією. Для забезпечення надійної захисту даних необхідно розробити та впровадити в державні структури, навчальні заклади та компанії передові стратегії і методи забезпечення інформаційної безпеки

Інформаційна безпека Республіки Ірландія є комплексом заходів, спрямованих на захист інформації. Багато організацій зберігають конфіденційну чи важливу інформацію в електронних базах даних. Це можуть бути різні дані, такі як особисті відомості клієнтів, банківська інформа-

ція або конфіденційні дані компанії. Чим важливішими є дані, тим серйознішими можуть бути наслідки їхньої втрати. Система захисту даних Республіки Ірландія спрямовано на забезпечення безпеки інформації. У системі управління інформаційною безпекою передбачені норми та методи, які забезпечують захист у всіх напрямках: правовому, фізичному та технічному.

Загалом можна констатувати, що інформаційну безпеку визначають як захист даних чи інформаційних систем від несанкціонованого доступу, знищення чи збоїв. Фахівці з безпеки часто посилаються на три основні поняття: 1. *Конфіденційність* – гарантія того, що лише авторизовані користувачі можуть отримати доступ до інформації; 2. *Цілісність* – це забезпечення неможливості несанкціонованої зміни даних, а також виявлення та запобігання будь-яким спробам такої зміни для підтримання узгодженості інформації; 3. *Доступність* – гарантія того, що інформація доступна і що канали зв'язку працюють коректно в потрібний момент [8].

Отже, у Республіці Ірландія забезпечення кібербезпеки є одним із ключових аспектів стратегії захисту інформації. Заходи щодо забезпечення інформаційної безпеки не тільки дають змогу зберегти наявні ресурси та компанії, а й сприяють розвитку нових продуктів і підприємств. У рамках аналізу поточної ситуації в галузі кібербезпеки в Республіці Ірландія можна виділити три основні групи зацікавлених сторін: 1. Академічні організації, такі як коледжі та університети, які займаються підготовкою фахівців у галузі високих технологій для ірландського ринку праці; 2. Промислові підприємства, які можуть зіткнутися із загрозами в разі кібератак; 3. Державні органи, що забезпечують функціонування державної цивільної служби [9].

Республіка Ірландія має багату історію в галузі освіти, і вона відіграє важливу роль у розвитку країни. Згідно з даними Організації економічного співробітництва та розвитку (ОЕСР) 37% населення Республіки Ірландія мають вищу освіту. Університети Республіки Ірландія займають передові позиції в галузі інформаційних технологій і комунікацій. Одним із прикладів є ступінь магістра наук у галузі технологій та управління інноваціями, яку пропонує Дублінський технологічний інститут (англ. Technological University Dublin). Його програма спрямована на підготовку ірландських студентів до керівництва розвитком сектора ІКТ [9].

Подібні програми були створені в результаті податкових пільг, введених у 1980-х рр. Ідея полягала в тому, що якби галузі ІКТ були в Республіці Ірландія, ними могли б керувати кваліфіковані ірландські професіонали. Дублінський університет (англ. University of Dublin) пропонує ступінь

кібер-криміналіста. Ця програма також доступна для співробітників правоохоронних органів. Відповідно до принципів інтернаціоналізму, прийнятих в Республіці Ірландія, ця програма доступна для співробітників поліції з будь-яких країн. Важливою подією в рамках програми стало відкриття випробувальних центрів у співпраці з Університетом Вісконсін-Медісон у США, щоб надати північноамериканській поліції більш зручне місце для тестування. Програму також добре прийняли співробітники внутрішньої поліції, і ірландська поліція вважає цю програму цінною і буде самостійно фінансувати здобуття ступеня магістра, щоб поліпшити свою кар'єру [2].

Приватний сектор відіграє важливу роль в економіці Республіки Ірландія. У 1970-х і 1980-х рр. ірландський уряд ухвалив низку політичних рішень, які лягли в основу сучасної промислової бази країни. У приватному секторі Республіки Ірландія, як і раніше, присутні міжнародні компанії, що мають представництва в країні. Ці компанії активно впроваджують інновації та прагнуть розвивати нові підприємства на території Республіки Ірландія [10].

Чимало великих міжнародних корпорацій розподіляють свою діяльність за географічними регіонами, такими як Європа, Близький Схід і Африка. В Республіці Ірландія розташовані регіональні офіси таких компаній, як «Facebook», «Microsoft», «Google» і «Oracle». У 2015 р. «Yahoo» перенесла свій офіс із Великої Британії до Республіки Ірландія через побоювання щодо збору даних британського Центру урядових комунікацій (англ. Government Communications Headquarters, GCHQ). Цей крок розглядається як прояв ірландської м'якої сили, оскільки він демонструє здатність країни залучати великі корпорації [11].

У цьому контексті необхідно зазначити, що Центр урядових комунікацій є спецслужбою Великої Британії, відповідальною за ведення радіоелектронної розвідки та забезпечення захисту інформації урядових структур та армії. Центр урядових комунікацій перебуває у віданні Міністра закордонних справ Великої Британії, але формально не є його частиною. Директор Центру має ранг Постійного секретаря Уряду Великої Британії. Більшість персоналу базується в штаб-квартирі в Челтнемі. Центр є учасником альянсу «UK-US SIGINT» і несе відповідальність за збір та аналіз інформації в країнах Європи (включно з європейською частиною РФ) і Африки [12].

У зв'язку з великою кількістю корпорацій зі списку 500 найбільших компаній США за розміром прибутку, що складається журналом «Fortune», розташованих в Республіці Ірландія, виникають проблеми зі зв'язком. Ірландська служба звітності та інформаційної безпеки (англ. The Irish

Reporting and Information Security Service, IRISS), некомерційна організація, створена приватними компаніями, виступає як перша група реагування на комп'ютерні надзвичайні ситуації в Республіці Ірландія. В обов'язки Служби входить поширення інформації про вразливості та атаки, ведення історичних даних і надання рекомендацій щодо передових методів роботи. Основна мета Служби полягає в наданні допомоги ірландським організаціям і громадянам у забезпеченні безпеки їхніх інформаційних технологій відповідно до визначених галузевих стандартів і вимог [13].

Життєво важливою вимогою бізнесу як у Республіці Ірландія, так і в інших країнах ЄС є захист конфіденційної інформації від конкурентів і хакерів-зловмисників. У багатьох випадках ця вимога є етичною та юридичною необхідністю. Підвищення рівня інформаційної безпеки в державних структурах, навчальних закладах та різноманітних організаціях може допомогти уникнути неправих фінансових втрат і репутаційного збитку. [14].

У цьому контексті важливу роль відіграє Міжнародна організація зі стандартизації (англ. International Organization for Standardization, ISO). Ця організація є найбільшою у світі мережею національних органів зі стандартизації, яка забезпечує безпеку, надійність і високу якість продукції та послуг. Міжнародною організацією зі стандартизації та Міжнародною електротехнічною комісією (англ. International Electrotechnical Commission, IEC) було розроблено міжнародний стандарт з інформаційної безпеки – «ISO/IEC 27001». Цей стандарт встановлює вимоги в галузі інформаційної безпеки, необхідні для створення, розвитку та підтримки системи менеджменту інформаційної безпеки [15].

Найважливішим елементом у забезпеченні кібербезпеки є Національна Стратегія кібербезпеки Республіки Ірландія (англ. National Cyber Security Strategy). Першу Стратегію було опубліковано у 2015 р. і вона була розрахована на два роки. У Національній стратегії кібербезпеки на 2015–2017 рр. викладено підхід уряду Республіки Ірландія до забезпечення стійкої та надійної роботи комп'ютерних мереж і пов'язаної з ними інфраструктури, якими користуються громадяни і підприємства. Відповідно до Національної стратегії кібербезпеки на 2015–2017 рр., Республіка Ірландія визначає основні напрямки взаємодії зі складними аспектами цифрових технологій, що динамічно розвиваються. Ця стратегія спрямована на усунення ризиків і загроз, пов'язаних зі стрімким розвитком ІКТ. Вона встановлює стратегічні цілі високого рівня, які складають основу національної політики в цій галузі, і визначає заходи, які необхідно вжити для їх досягнення [16].

Важливо зазначити, що в Національній стратегії кібербезпеки на 2015–2017 рр. було передбачено створення Національного центру кібербезпеки при Міністерстві зв'язку, енергетики та природних ресурсів (англ. Department of Communications, Energy and Natural Resources of Ireland). У стратегії детально описується, як цей орган буде взаємодіяти з трьома основними сферами своєї відповідальності: державними мережами, приватними і бізнес-системами, а також із захистом найважливішої національної інфраструктури. Національну стратегію кібербезпеки на 2015–2017 рр. було розроблено на основі наявної Групи реагування на інциденти у сфері комп'ютерної безпеки Республіки Ірландія (англ. Computer Security Incident Response Team, CSIR), створеної наприкінці 2011 р. [16].

Наступна Національна Стратегія кібербезпеки Республіки Ірландія була опублікована в грудні 2019 р. і є продовженням першої Стратегії країни, опублікованої у 2015 р. Це більш широкий і всеосяжний документ, ніж попередній, і він враховує досвід роботи Національного центру кібербезпеки з 2015 р. по 2019 р., а також поточні національні та міжнародні заходи в цій галузі. Необхідно зазначити, що Національна стратегія кібербезпеки Республіки Ірландія на 2019–2024 рр., залишається чинною і у 2025 р. до ухвалення наступного документа.

У чинній Стратегії визнається, що кібератаки та гібридні загрози стають дедалі актуальнішими в контексті забезпечення міжнародної безпеки. Масштаби проблеми вимагають надійного і скоординованого підходу з боку ЄС і на національному рівні. На міжнародному рівні Республіка Ірландія тісно співпрацює з країнами-однодумцями, маючи на меті спільну мету – захищати і просувати безпечний, надійний, доступний, вільний і відкритий Інтернет, в якому дотримуються права людини та основні свободи як он-лайн, так і оф-лайн [17].

У сфері забезпечення кібербезпеки Міністерство закордонних справ Республіки Ірландія (англ. Department of Foreign Affairs of the Republic of Ireland) здійснює тісну взаємодію з Національним центром кібербезпеки, що був створений у рамках попередньої Національної Стратегії кібербезпеки Республіки Ірландія на 2015–2017 рр., а також Департаментом довкілля, клімату та комунікацій (англ. The Department of the Environment, Climate and Communications) уряду Ірландії з питань, пов'язаних із кібербезпекою та кібердипломатією. Крім того, Міністерство закордонних справ співпрацює з Міністерством юстиції в галузі боротьби з кіберзлочинністю [17].

Мета Національна стратегія кібербезпеки Республіки Ірландія на 2019–2024 рр., рік полягає в тому, щоб Республіка Ірландія могла й надалі

безпечно користуватися перевагами цифрової революції та відігравати повноцінну роль у формуванні майбутнього Інтернету. Ця мета буде досягнута завдяки: 1. Захисту ірландської держави, її громадян і критично важливої національної інфраструктури від загроз у сфері кібербезпеки; 2. Розбудові потенціалу ірландської держави, науково-дослідних інституцій, бізнесу і людей, щоб краще розуміти й розв'язувати проблеми, з якими стикається Республіка Ірландія в цій сфері; 3. Участь ірландської держави на національному і міжнародному рівнях у стратегічній підтримці вільного, відкритого, мирного і безпечного кіберпростору [18].

Серед основних завдань Національної стратегії кібербезпеки Республіки Ірландія на 2019–2024 рр. виділяються такі: 1. Продовжувати підвищувати здатність ірландської держави реагувати на інциденти, пов'язані з кібербезпекою, та керувати ними, у тому числі з урахуванням національної безпеки; 2. Виявляти та захищати критично важливу національну інфраструктуру, підвищуючи її стійкість до кібератак та забезпечуючи наявність у операторів життєво важливих служб відповідних планів реагування на інциденти, щоб скоротити та контролювати будь-які перебої у роботі служб; 3. Підвищити відмовостійкість та безпеку ІТ-систем державного сектору, щоб краще захищати сервіси, на які покладаються громадяни Республіки Ірландія, та їх дані; 4. Інвестувати в освітні ініціативи, щоб підготувати фахівців для роботи у сфері передових технологій та кібербезпеки; 5. Підвищити обізнаність компаній про їхню відповідальність за безпеку своїх мереж, пристроїв та інформації, а також стимулювати дослідження та розробки в галузі кібербезпеки в Ірландії, у тому числі шляхом сприяння інвестиціям у нові технології; 6. Продовжувати взаємодіяти з міжнародними партнерами та міжнародними організаціями, щоб кіберпростір залишався відкритим, безпечним, єдиним та вільним, а також сприяв соціально-економічному; 7. Підвищити загальний рівень навичок та поінформованості приватних осіб у питаннях базової кібергігієни та підтримувати їх у цьому за допомогою інформації та навчання [18].

Важливим моментом у Національній стратегії кібербезпеки Республіки Ірландія на 2019–2024 рр. є те, що в пункті 12 Стратегії йдеться про те, що «уряд продовжить забезпечувати розробку та впровадження програм навчання другого та третього рівнів у галузі комп'ютерних наук та кібербезпеки», а також зобов'язується підтримувати розробку короткострокових курсів з кібербезпеки для молодших школярів [18].

Короткий курс для молодших класів було розроблено робочою групою, до якої увійшли представники «Ірландського товариства з викори-

стання комп'ютерів в освіті (англ. Computers in Education Society of Ireland, CESI), Національна рада з навчальних програм та оцінювання (англ. National Council for Curriculum and Assessment), організації «Кібер Ірландія» (англ. Cyber Ireland), Національного центру кібербезпеки (англ. The National Cybersecurity Center) та групи з реалізації проекту з Дублінського університетського коледжу (англ. University College Dublin). У проміжному звіті «Розробка короткострокового курсу з кібербезпеки для молодших класів» описується передісторія створення робочої групи та команди з реалізації проекту, поточне фінансування, подробиці розробки короткострокового курсу та пов'язаних з ним заходів, інформація про школи, розробка веб-матеріалів Центру з навчання кіберстійкості та ключові рекомендації [19].

Важливим елементом у системі інформаційної безпеки Республіки Ірландія є Національний центр кібербезпеки Ірландії (англ. National Cyber Security Centre, NCSC), який було створено в рамках Національної стратегії кібербезпеки Республіки Ірландія на 2015–2017 рр. Національний центр кібербезпеки Республіки Ірландія – це державна організація, що займається питаннями забезпечення комп'ютерної безпеки. Центр є оперативним підрозділом Департаменту довкілля, клімату та комунікацій уряду Республіки Ірландія. Серед основних завдань Центру виділяють: 1. Управління великими інцидентами у сфері кібербезпеки в уряді; 2. Надання рекомендацій і порад громадянам і бізнесу щодо великих інцидентів у сфері кібербезпеки; 3. Розвиток ефективних міжнародних відносин у галузі кібербезпеки у глобальному масштабі для обміну інформацією [20].

4 листопада 2024 р. Національним центром кібербезпеки Республіки Ірландія було опубліковано Доповідь про національну кібербезпеку Ірландії за 2023 р. Доповідь є актуальним нагадуванням про важливість забезпечення кібербезпеки для захисту бізнесу і майбутнього Республіки Ірландія. У доповіді, підготовленій Департаментом довкілля, клімату та комунікацій уряду Республіки Ірландія, розглядається поточна Національна стратегія кібербезпеки, що перебуває на стадії реалізації. У 2023 р. Національний центр кібербезпеки Республіки Ірландія отримав 5276 повідомлень, 721 з яких було підтверджено як інциденти кібербезпеки. Це призвело до початку 309 розслідувань. Згідно зі звітом, більшість інцидентів було визнано незначними. Не було зафіксовано жодного інциденту, який можна було б класифікувати як серйозний або дуже серйозний [20].

Результати звіту підтверджують ефективність профілактичних заходів, що вживаються Національним центром кібербезпеки Республіки Ірландія. Це дає змогу гарантувати своєчасне

усунення потенційних загроз до того, як вони можуть завдати шкоди інфраструктурі країни. Щорічний звіт публікується в рамках проміжної звітності Національної стратегії кібербезпеки і містить детальну інформацію про роботу, виконану урядовими департаментами міністерств та агентствами з боротьби з кібератаками. Документ узагальнює інформацію, отриману від Департаменту довкілля, клімату та комунікацій (англ. Department of Environment, Climate and Communications) уряду Республіки Ірландія, Національним центром кібербезпеки Республіки Ірландія, Національної поліції, Сил оборони та Міністерства закордонних справ Республіки Ірландія. У цьому контексті державний міністр Департаменту довкілля, клімату та комунікацій уряду Республіки Ірландія Сміт О. зазначив: «Оновлення даних стало прямою відповіддю на вимоги громадськості щодо частішого звітування, глибшого розуміння та прозорості зусиль уряду у сфері кібербезпеки». Щорічний звіт демонструє прихильність уряду Республіки Ірландія забезпеченню безпеки критично важливої інфраструктури країни, розвитку навичок кібербезпеки та потенціалу громадян, а також забезпеченню плавного переходу країни до цифрової економіки [20].

Уряд Республіки Ірландія також оголосив про створення фонду в розмірі 2 млн. євро для надання грантів малим і середнім підприємствам з метою підвищення рівня їхньої кібербезпеки. Ініціатива фінансується Республікою Ірландія спільно з ЄС у рамках програми «Цифрова Європа». Фонд надасть компаніям фінансову підтримку для зміцнення їхніх інформаційних технологій. Малі та середні підприємства, що відповідають вимогам, можуть подати заявку на фінансування в розмірі 80% вартості проекту з максимальною сумою гранту в розмірі 60 тисяч євро для реалізації ключових заходів щодо забезпечення кібербезпеки, повторного тестування своїх систем і отримання експертних рекомендацій щодо майбутніх покращень [20].

У серпні 2024 р. Національний центр кібербезпеки Республіки Ірландія опублікував Національний план екстреної кібердопомоги. Документ описує процес оголошення, управління та координації національної надзвичайної ситуації в цифровому просторі. План забезпечує чітке розуміння ролей і обов'язків усіх учасників під час такої ситуації та детально роз'яснює підхід уряду до серйозних кіберінцидентів. Національний план екстреної кібердопомоги передбачає гнучкий процес реагування на різні можливі сценарії. Документ був розроблений після широкої взаємодії з державним і приватним секторами. План описує процес оголошення, управління та координації національної надзвичайної ситуації в цифровому просторі.

План екстреної кібердопомоги спирається на три режими взаємодії: 1. **Постійний режим.** Стосується звичайної ділової діяльності, за якої підтримується ситуаційна обізнаність і проводяться підготовчі заходи; 2. **Режим попередження.** Активується за наявності доказів підвищеного цифрового ризику в певних секторах. Включає комунікацію із зацікавленими сторонами в уряді та приватному секторі; 3. **Повна активація.** Відбувається в разі інциденту, який відповідає порогу національної надзвичайної ситуації. Вимагає активації Національної координаційної групи з надзвичайних ситуацій, очолюваної Національним центром кібербезпеки Республіки Ірландія, для забезпечення ефективного, координованого міжвідомчого та міжурядового реагування [21].

Іншим значущим проектом у сфері забезпечення цифрової безпеки Республіки Ірландія є проект «Безпечний Інтернет в Ірландії» (англ. Safer Internet Ireland Project). Цей проект являє собою консорціум партнерів із різних сфер, таких як промисловість, освіта, соціальне забезпечення дітей та уряд. Проект функціонує як «Центр безпечного Інтернету» в Республіці Ірландія та спрямований на розроблення національних ініціатив, що сприяють підвищенню безпеки використання електронних засобів масової інформації, а також на посилення захисту вразливих верств населення, зокрема дітей, від негативних аспектів Інтернету. Основні цілі проекту: 1. Розроблення та впровадження скоординованих заходів на національному рівні щодо забезпечення безпеки в Інтернеті, стійких до розвитку технологій і використання нових медіа; 2. Створення та розповсюдження інформаційних матеріалів і програм, спрямованих на підвищення поінформованості дітей, вчителів і батьків щодо переваг і ризиків використання Інтернету; 3. Надання професійних консультаційних послуг, спрямованих на надання допомоги дітям, що зіткнулися з проблемами в Інтернеті; 4. Створення служби гарячої лінії для анонімного і конфігурації та консультування з питань безпеки в Інтернеті [22].

**Висновки.** За останні два десятиліття сектор інформаційних технологій в економіці Республіки Ірландія став одним із провідних постачальників товарів і послуг на міжнародному рівні. Це зростання багато в чому стало результатом реалізації державних програм, розроблених урядом Республіки Ірландія. Сьогодні сектор інформаційно-комунікаційних технологій є важливою складовою економіки Республіки Ірландія. Кіберпростір є невід'ємним елементом бізнес-процесів, освітньої сфери та державного управління ірландської держави. Це пов'язано з тим, що інформація поширюється по всьому світу з високою швидкістю, істотно впливаючи як на фінансові ринки, так і на політичні процеси.

Республіка Ірландія може слугувати прикладом для країн, що розвиваються, які прагнуть до розвитку інформаційних технологій у своїй економіці. Однак економічна політика, спрямована виключно на розвиток IT-сектору, не є повною, якщо не враховувати витрати на забезпечення безпеки та технічне обслуговування, пов'язані з розвитком цієї галузі. У цьому полягав основний недолік економічної політики уряду Республіки Ірландія. У минулому уряд Республіки Ірландія не приділяв належної уваги питанням кібербезпеки. Однак нині ситуація змінюється. Нещодавно були опубліковані нові звіти і стратегії, спрямовані на підвищення рівня кібербезпеки. У разі прояву громадянами Республіки Ірландія рішучості, зосередженості та готовності до співпраці, у майбутньому можливо знайти ефективне вирішення цієї проблеми.

Однак, забезпечення кібербезпеки не тільки являє собою проблему, а й відкриває нові можливості. В умовах зниження економічної активності громадяни Республіки Ірландія активно шукають можливості працевлаштування. Політика, спрямована на стимулювання ірландських студентів до вивчення питань кібербезпеки, може вирішити чимало завдань. Зокрема підготовка кваліфікованих фахівців у цій галузі може стати інструментом «м'якої сили» у зовнішній політиці Республіки Ірландія, даючи їм змогу виступати експертами і послами в цій сфері. Уряд Республіки Ірландія робить певні кроки в цьому напрямку. План дій з розвитку навичок у сфері інформаційно-комунікаційних технологій, розроблений Міністерством освіти і навичок, спрямований на подолання розриву між приватним і державним секторами в цій сфері.

Відповідно до Національної стратегії кібербезпеки Республіки Ірландія визначає заходи щодо забезпечення безпеки та надійності роботи комп'ютерних мереж і пов'язаної з ними інфраструктури, які використовують громадяни та підприємства країни. Розвиток інформаційно-комунікаційних технологій призвів до значного поліпшення якості життя, появи нових послуг і радикальних змін у способах ведення бізнесу. Однак широке застосування цих технологій також призвело до того, що суспільство почало залежати від безперервної роботи та стабільності цих систем. Сьогодні існує низка загроз для забезпечення безпеки та надійності функціонування інформаційно-комунікаційних технологій, таких як хакерські атаки, кіберзлочинність, хактивізм і кібершпигунство. Крім того, залежність від цих технологій і систем створює ризики, пов'язані з людським чинником, збоями в роботі програмного забезпечення та обладнання, а також надзвичайними ситуаціями.

Національна стратегія кібербезпеки Республіки Ірландія визначає стратегічні цілі висо-

кого рівня, які складають основу державної політики в цій галузі, а також заходи, які будуть вжиті щодо кожної із загроз. У рамках Стратегії важливу роль відіграє створення Національного центру кібербезпеки при Міністерстві зв'язку, енергетики та природних ресурсів. Центр національної кібербезпеки взаємодіє з урядовими мережами, персональними та діловими системами, а також забезпечуватиме захист критично важливої національної інфраструктури Республіки Ірландія.

### Література

1. Wiener N. Cybernetics, or Control and Communication in the Animal and the Machine. New York : John Wiley & Sons, 1948.
2. Falk C. Security in the Irish information technology sector. *Research Gate*. January 2015. URL: [https://www.researchgate.net/publication/283228143\\_Security\\_in\\_the\\_irish\\_information\\_technology\\_sector](https://www.researchgate.net/publication/283228143_Security_in_the_irish_information_technology_sector)
3. Wilmschurst E. Definition of Aggression. *United Nations Audiovisual Library of International Law*. 2008. URL: [http://legal.un.org/avl/pdf/ha/da/da\\_e.pdf](http://legal.un.org/avl/pdf/ha/da/da_e.pdf)
4. Libicki M. C. *Conquest in Cyberspace*. Cambridge : The Cambridge University Press, 2007.
5. Kushner D. The real story of stuxnet. *IEEE Spectrum*. 2013. Vol. 50(3). P. 48–53. <https://doi.org/10.1109/MSPEC.2013.6471059>
6. Global Risks Report, 2013. *World Economic Forum*. January 8, 2013. URL: <https://www.weforum.org/stories/2013/01/global-risks-2013-by-numbers/>
7. National Risk Assessment 2024 – Overview of Strategic Risks. *Department of the Taoiseach*. September 17, 2024. URL: <https://www.gov.ie/en/policy-information/448eb-national-risk-assessment-2024-overview-of-strategic-risks/>
8. McIntyre T. Regulating the Information Society: Data Protection and Ireland's Internet Industry / In Farrell and Hardiman (eds), *The Oxford Handbook of Irish Politics*. Oxford University Press, 2020. URL: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3590302](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3590302)
9. MSc in Digital Investigation & Forensic Computing. *Centre for Cyber security & Cyber crime Investigation*. 2014. URL: [https://www.ucd.ie/t4cms/UCD\\_MSc\\_DigitalInvestandForensicComp.pdf](https://www.ucd.ie/t4cms/UCD_MSc_DigitalInvestandForensicComp.pdf)
10. Newenham P. Silicon Docks: The Rise of Dublin as a Global Tech Hub. Dublin: Liberties Press, 2015.
11. Hopkins N., Mayworns T. Yahoo that its move to Dublin is a security worry. *The Guardian*, March 20, 2014.
12. Cyber Security. *Government Communications Headquarters (GCHQ)*. 2025. URL: <https://www.gchq.gov.uk/section/mission/cyber-security>
13. Ireland's First Computer Emergency Response Team. *Irish Reporting and Information Security Service*. 2022. URL: <https://iriss.ie/>
14. Information Security. *IT-governance of Europe*. URL: <https://www.itgovernance.eu/en-ie/information-security-ie>
15. ISO/IEC 27001:2022. *International Organization for Standardization, ISO*. 2022. URL: <https://www.iso.org/standard/27001>

16. National Cyber Security Strategy 2015-2017. *Department of Communications, Energy and Natural Resources*. 2017. URL: [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National\\_Strategies\\_Repository/Ireland\\_2015\\_NationalCyberSecurityStrategy20152017.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Ireland_2015_NationalCyberSecurityStrategy20152017.pdf)

17. International Security Policy. *Department of Foreign Affairs of Ireland*. 2025. URL: <https://www.ireland.ie/en/dfa/role-policies/international-priorities/peace-and-security/international-security-policy/>

18. National Cyber Security Strategy 2019-2024. *The National Cyber Security Centre of Ireland (NCSC)*. 2019. URL: <https://www.ncsc.gov.ie/strategy/>

19. UCD Centre for Cyber Resilience Education. 2024. *Cyberwise of Ireland*. URL: <https://cyberwise.ie>

20. National Cyber Security Centre (NCSC) – Ireland. *European Cybersecurity Competence Centre and Network*. 2025. URL: [https://cybersecurity-centre.europa.eu/ireland-ncc\\_en](https://cybersecurity-centre.europa.eu/ireland-ncc_en)

21. The National Cyber Security Report, November 2024. *VIATEL technology group*. November 5, 2024. URL: <https://www.viatel.com/the-national-cyber-security-report-november-2024/>

22. Safer Internet Ireland Project. *Department of Justice of the Government of Ireland*. December 9, 2021. URL: <https://www.gov.ie/en/service/safer-internet-ireland-project/>

#### Анотація

**Марусинець М. М.** Політика безпеки у сфері інформаційно-комунікаційних технологій в Республіці Ірландія. – Стаття.

У статті проводиться аналіз механізмів, які використовує уряд Республіки Ірландія для забезпечення інформаційної безпеки країни. Метою статті є аналіз політики безпеки у сфері інформаційно-комунікаційних технологій в Республіці Ірландія, оцінка ефективності заходів, що вживаються урядом Республіки Ірландія для захисту інформаційних ресурсів, а також визначення можливих напрямків для поліпшення ситуації в цій галузі. Результати дослідження можуть бути корисними не тільки для Республіки Ірландія, а й для інших держав, які хочуть розвивати свою індустрію інформаційних технологій. Зокрема, невеликі країни, які прагнуть розвивати ІТ-сектор у своїй економіці, можуть вивчити досвід Республіки Ірландія та ухвалити обдумані рішення щодо того, як підтримувати та стимулювати цю галузь.

Аргументовано, що за останні два десятиліття сектор інформаційних технологій в економіці Республіки Ірландія став одним із провідних постачальників товарів і послуг на міжнародному рівні. Це зростання багато в чому стало результатом реалізації державних програм, розроблених урядом Республіки Ірландія. Нині сектор інформаційно-комунікаційних технологій є важливою складовою економіки Республіки Ірландія. Нині кіберпростір є невід'ємним елементом бізнес-процесів, освітньої сфери та державного управління ірландської держави. Це пов'язано з тим, що інформація поширюється по всьому світу з високою швидкістю, справляючи істотний вплив як на фінансові ринки, так і на політичні процеси.

Доведено, що Національна стратегія кібербезпеки Республіки Ірландія визначає стратегічні цілі висо-

кого рівня, що становлять основу державної політики в цій галузі, а також заходи, що вживатимуться щодо кожної із загроз. У рамках Стратегії важливу роль відіграє створення Національного центру кібербезпеки при Міністерстві зв'язку, енергетики та природних ресурсів. Центр національної кібербезпеки взаємодіє з урядовими мережами, персональними та діловими системами, а також забезпечуватиме захист критично важливої національної інфраструктури Республіки Ірландія.

**Ключові слова:** Республіка Ірландія, інформаційно-комунікаційні технології, інформаційна безпека, кіберприступність, ІТ-сектор, політика, управління, Національна стратегія кібербезпеки.

#### Summary

**Marusynets M. M.** Security policy in the field of information and communication technologies in the Republic of Ireland. – Article.

The article analyzes the mechanisms used by the Government of the Republic of Ireland to ensure the country's information security. The purpose of the article is to analyze the security policy in the field of information and communication technologies in Ireland, to assess the effectiveness of measures taken by the Government of Ireland to protect information resources, and to identify possible areas for improving the situation in this area. The results of the study can be useful not only for Ireland, but also for other countries that want to develop their information technology industry. In particular, small countries seeking to develop the IT sector in their economy can study the experience of Ireland and make informed decisions on how to support and stimulate this industry.

It is argued that over the past two decades, the information technology sector in the Irish economy has become one of the leading suppliers of goods and services at the international level. This growth was largely the result of the implementation of state programs developed by the Government of Ireland. Currently, the information and communication technology sector is an important component of the economy of the Republic of Ireland. Currently, cyberspace is an integral element of business processes, the educational sphere and public administration of the Irish state. This is due to the fact that information travels around the world at high speed, having a significant impact on both financial markets and political processes.

The National Cyber Security Strategy of the Republic of Ireland has been proven to set out high-level strategic objectives that form the basis of government policy in this area, as well as the measures that will be taken in relation to each of the threats. Within the framework of the Strategy, an important role is played by the establishment of the National Cyber Security Centre within the Department of Communications, Energy and Natural Resources. The National Cyber Security Centre interacts with government networks, personal and business systems, and also ensures the protection of the critical national infrastructure of the Republic of Ireland.

**Key words:** Republic of Ireland, information and communications technology, information security, cybercrime, IT sector, policy, governance, The National Cyber Security Strategy.