УДК 004.056.5:351.86(569.4+477)
DOI https://doi.org/10.24144/2307-3322.2024.84.3.12

КІБЕРБЕЗПЕКА В УМОВАХ СУЧАСНИХ ЗАГРОЗ: ІЗРАЇЛЬСЬКИЙ ДОСВІД І ЙОГО ЗАСТОСУВАННЯ В УКРАЇНІ

Дзеньків В.,
аспірант 1-го року навчання за спеціальністю Право,
Науково-дослідний інститут публічного права

Дзеньків В. Кібербезпека в умовах сучасних загроз: ізраїльський досвід і його застосування в Україні.

У цій статті запропоновано детальний аналіз досвіду Ізраїлю у сфері правового регулювання кібербезпеки та його потенційну адаптацію для України. Ізраїль є однією з провідних країн у галузі кібербезпеки завдяки своєму інтегрованому підходу до захисту кіберпростору. Розглянуто основні законодавчі акти та організаційні заходи, запроваджені в Ізраїлі, що охоплюють створення спеціалізованих кіберпідрозділів, як-от TEHILA та Ізраїльський національний кібердиректорат (INCD), і координаційних центрів для забезпечення злагоджених зусиль між державними і приватними організаціями. Висвітлено важливість інтеграції кібербезпекових механізмів у національну оборонну стратегію Ізраїлю, а також активну участь приватного сектору, зокрема численних технологічних компаній і стартапів, у захисті інформаційної інфраструктури. Особливу увагу приділено питанням забезпечення постійного вдосконалення технологій кіберзахисту та підвищення кваліфікації фахівців у цій галузі.

У статті також акцентовано увагу на ролі міжнародної співпраці, зокрема з країнами ЄС та США, у розробці ефективної кіберстратегії, що може бути особливо важливо для України в умовах війни з Росією. Окреслено ключові аспекти адаптації ізраїльських підходів до українських реалій, зокрема, необхідність створення спеціалізованих органів, розробки національної кіберстратегії та залучення приватного сектору до забезпечення кібербезпеки. Підкреслено важливість міжвідомчої координації та співпраці з міжнародними партнерами для підвищення рівня кібербезпеки. Зауважено, що інтеграція найкращих ізраїльських практик може значно підвищити рівень кіберзахисту України, сприяючи ефективнішому реагуванню на кіберзагрози та захисту критично важливих інфраструктур. Крім того, розглянуто питання правового регулювання, яке охоплює як нормативно-правову базу, так і практичні аспекти імплементації кібербезпекових заходів на державному та місцевому рівнях. Особливо підкреслено необхідність постійного моніторингу та оцінки ефективності впроваджених заходів для своєчасного виявлення та нейтралізації потенційних загроз.

Ключові слова: кібербезпека, правове регулювання, Ізраїль, Україна, кіберзлочинність, координація, національна безпека, інформаційні технології.

Dzenkiv V. Cybersecurity in the context of modern threats: Israeli experience and its application in Ukraine.

This article comprehensively analyzes Israel's experience in the legal regulation of cybersecurity and explores its potential adaptation for Ukraine. Israel is a leading cybersecurity nation due to its integrated approach to cyber protection. The paper examines key legislative acts and organizational measures implemented in Israel, such as establishing specialized cyber units like TEHILA and the Israel National Cyber Directorate (INCD), and coordination centers that facilitate cohesive efforts between governmental and private organizations. The article highlights the significance of incorporating cybersecurity mechanisms into Israel's national defense strategy and the active involvement of the private sector, including numerous tech companies and startups, in safeguarding information infrastructure. The crucial role of international cooperation, particularly with the EU and the USA, in developing an effective cyber strategy is also discussed, emphasizing its relevance for Ukraine amidst the ongoing conflict with Russia.

Additionally, the article delves into the continuous improvement of cybersecurity technologies and the professional development of specialists in this field. It highlights the importance of a holistic approach encompassing technological advancements and strategic planning. The paper also emphasizes the need for interagency coordination and the collaboration with international partners to elevate the overall cybersecurity posture. Key aspects of adapting Israeli approaches to Ukrainian realities are outlined, including the necessity of establishing specialized bodies, developing a national cybersecurity strategy, and engaging the private sector in cybersecurity efforts. By integrating Israel's best practices, Ukraine can significantly bolster its cyber defense capabilities, enhancing its ability to respond to cyber threats more effectively and protecting its critical infrastructures. Furthermore, the study addresses legal regulation issues, including both the regulatory framework and practical aspects of implementing cybersecurity measures at national and local levels. Continuous monitoring and evaluation of the effectiveness of these measures are essential to identify and neutralize potential threats timely.

Key words: cybersecurity, legal regulation, Israel, Ukraine, cybercrime, coordination, national security, information technology.

Постановка проблеми. Активний розвиток кібертехнологій та ІТ-бізнесу в Україні, яка перебуває у стані війни з Росією, створює нові можливості для злочинів онлайн та у сфері інформаційних технологій, що робить захист інформаційної інфраструктури надзвичайно актуальним. Інформаційні технології посідають важливе місце в економіці України, стабільно входячи до трійки галузей ВВП.

Більшість громадян має доступ до Інтернету та активно використовує електронну пошту, соціальні мережі, що робить їх потенційними цілями для кіберзлочинців. Традиційні методи захисту, такі як криптографія та міжмережеві екрани, стають недостатніми проти сучасних кіберзагроз, які ставлять під удар інформацію з фінансовою, військовою або політичною цінністю, додаючи ризик перехоплення управління критичними об'єктами.

Введення воєнного стану впливає на права та свободи громадян, вимагаючи забезпечення ефективного контролю за обмеженнями прав, щоб гарантувати баланс між національною безпекою та захистом прав. Вивчення ізраїльського досвіду правового регулювання кібербезпеки може надати Україні ефективні моделі для посилення захисту в інформаційній сфері та впровадженні найкращих практик. Ізраїль, маючи багатий досвід у боротьбі з кіберзлочинністю, розробив ефективні механізми правового регулювання, які можуть бути корисними для України у забезпеченні інформаційної безпеки в умовах сучасних загроз.

Аналіз останніх досліджень і публікацій. Аналіз наукових публікацій свідчить про значний внесок як закордонних, так і вітчизняних науковців у дослідження правового регулювання кібербезпеки. Серед закордонних вчених, таких як Д. Шелдон, Г. Раттрей, П. Домровський, Дж. Наямол, С. Старр та А. Клімбург, було здійснено глибоке дослідження різних аспектів кіберзлочинності та захисту інформаційного простору. В Україні кібербезпеку та, зокрема, проблему кібертероризму досліджували Д. Дубов, В. Пилипчук, В. Петров, М. Ожеван та М. Погорецький [2].

Особливу увагу в українських наукових колах привертає досвід Ізраїлю в галузі забезпечення кібербезпеки. Вітчизняні дослідники, такі як Гребенюк М.В. та Леонов Б.Д., аналізують ізраїльські практики, зосереджуючись на їхньому високому рівні інтеграції між державними та приватними структурами, а також на розвитку спеціалізованих кіберпідрозділів [1]. На основі цих досліджень розробляються рекомендації щодо вдосконалення українського законодавства у сфері кібербезпеки з урахуванням ізраїльського досвіду. Водночас, зазначається, що в науковій літературі системні дослідження, присвячені комплексному аналізу ізраїльських підходів до кібербезпеки та їхньої адаптації до умов України, залишаються недостатніми.

Мета дослідження. Метою статті є визначення можливостей удосконалення законодавства України у сфері кібербезпеки на основі аналізу передового досвіду держави Ізраїль. Для досягнення цієї мети здійснено вивчення основних елементів ізраїльського правового регулювання кібербезпеки, оцінено їх ефективність, та розроблено рекомендації щодо їх адаптації та впровадження в Україні.

Виклад основного матеріалу. Особливістю кіберпростору є його екстериторіальність, що робить його надзвичайно складним для регулювання національними засобами. Незважаючи на це, дедалі більше держав наголошують на міжнародному рівні на необхідності встановлення кордонів і принципів національно-державного суверенітету в цьому специфічному «просторі». Про-

відні країни світу активно нарощують свої можливості для агресивних дій у кіберпросторі, що проявляється у розробці та застосуванні складних програмних комплексів, основною метою яких є завдання шкоди об'єктам атаки [2].

Ізраїль, як країна з обмеженими природними ресурсами та постійними військовими загрозами, зосередив свої зусилля на розвитку науки і технологій, ставши світовим центром інновацій. Відсутність сировинних ресурсів і безперервна потреба в обороні стимулювали Ізраїль досягти значних успіхів у різних галузях, включаючи медицину, де його технології є одними з найпередовіших, а також в IT-секторі, де країна швидко стала лідером інновацій. Жителі Ізраїлю, живучи в умовах терористичної загрози протягом 75 років, цінують поточні досягнення і прагнуть забезпечити стабільне та безпечне майбутнє, сприяючи зміцненню і розвитку держави.

Сфера кібербезпеки є одним із ключових пріоритетів для Ізраїлю, оскільки країна є однією з найбільш комп'ютеризованих на Близькому Сході.

Вразливість інформаційної інфраструктури може призвести до серйозних наслідків для обороноздатності та національної безпеки, тому Ізраїль приділяє особливу увагу розробці та впровадженню надійних кібербезпекових рішень, що захищають її критичну інформаційну інфраструктуру від потенційних загроз [1].

Ізраїль демонструє швидкі темпи збільшення інвестицій у кібербезпеку, на його частку припадає 15% світових інвестицій у розвиток цієї сфери. Ізраїльська модель кібербезпеки зосереджена на інтеграції новітніх технологій та створенні правових механізмів для захисту інформаційної інфраструктури. Сучасні кіберзагрози потребують не лише національних, а й міжнародних стратегій забезпечення безпеки, що підкреслює необхідність глобального підходу до регулювання кіберпростору. Мілітаризація кіберпростору створює нові виклики, оскільки спроби здійснити атаки на критичну інфраструктуру можуть мати непередбачувані наслідки. Для запобігання таким сценаріям провідні держави розпочали діалоги на різних рівнях та формують цілісні стратегії поведінки в кіберпросторі, що включає як національні, так і міжнародні заходи [2].

Хоча, Ізраїль вважається однією з провідних країн у сфері кібербезпеки і навіть лідером у цій галузі. Проте, за даними різних звітів та досліджень, Ізраїль не входить до числа провідних світових кібердержав. За класифікацією Міжнародного інституту стратегічних досліджень (IISS) Ізраїль належить до другого рівня серед глобальних кібердержав разом з Австралією, Канадою, Китаєм, Францією, Росією та Великою Британією [9]. У глобальному рейтингу кібербезпеки Міжнародної спілки електрозв'язку (ITU) Ізраїль посів 36 місце серед 194 країн і 23 місце серед європейських країн [11]. Національний індекс кібербезпеки (NCSI) у вересні 2023 року відвів Ізраїлю 39 місце серед 176 країн, що свідчить про зниження порівняно з 24 місцем у 2019 році [12]. У Національному індексі кіберпотужності 2022 року Ізраїль зайняв 19 місце серед 30 країн, [16] тоді як в Індексі кіберзахисту він взагалі не включений до переліку «основних світових економік» за критеріями колективних кібербезпекових активів, організаційних можливостей та політичних підходів [14]. Оскільки деякі з цих індексів враховують правову базу та заходи щодо забезпечення кібербезпеки як показники національних кіберспроможностей, важливо проаналізувати законодавство, ухвалене Ізраїлем для регулювання кіберсфери.

Сучасна інфраструктура кібербезпеки в Ізраїлі охоплює приблизно 450 компаній, включаючи відомі фірми, такі як «Check Point», а також численні стартапи та венчурні фонди, зокрема «Jerusalem Venture Partners (JVP) Cyber Labs», що активно інвестують у цю галузь. Крім того, значну роль відіграють науково-дослідні проєкти, які сприяють співпраці між високотехнологічними компаніями та дослідницькими центрами.

У 2017 році інвестиції у сферу кіберзахисту в Ізраїлі становили 10,8 мільйона доларів, що на 26% більше порівняно з 2016 роком. На сьогодні Ізраїль є другим за обсягом експортером програмного забезпечення у світі після США. Таким чином, Ізраїль перетворюється з постачальника стартапів на міжнародний центр високих технологій, і, перш за все, стає одним із провідних світових лідерів у галузі кібербезпеки [2].

Вважається, що 1997 рік став визначальним моментом у регулюванні кіберпростору Ізраїлю завдяки створенню TEHILA (акронім від «Урядова інфраструктура для Інтернет-епохи») при Міністерстві фінансів Ізраїлю. TEHILA, як одна з перших у світі урядових кібербезпекових агенцій, забезпечувала державні установи безпечною платформою для підключення до Інтернету та надання послуг громадськості, захищаючи їх від кіберзагроз. Центр державної інформаційної безпеки Ізраїлю, створений у рамках TEHILA, здійснював моніторинг глобальних подій у сфері

інформаційної безпеки, координував взаємодію між урядовими структурами, розв'язував питання безпеки, підтримував зв'язки з зовнішніми організаціями та проводив дослідження [8].

У 2002 році, згідно з рішенням B/84 Міністерського комітету з національної безпеки, в Ізраїлі було створено Національне управління з інформаційної безпеки (NISA), яке діє в рамках Загальної служби безпеки (Шабак). NISA отримало мандат на захист критично важливої комп'ютеризованої інфраструктури держави. Його основними завданнями стали розробка інструкцій та забезпечення захисту для критичних комп'ютеризованих систем в обраних державних і приватних цивільних організаціях. Це рішення підкреслило важливість захисту національної інформаційної безпеки та заклало основу для організованого кіберзахисту в Ізраїлі. Таке управління стало центральним елементом у забезпеченні кібербезпеки на національному рівні, включаючи координацію між різними урядовими та приватними організаціями, що мають стратегічне значення для держави [11].

З часом, в рамках розвитку та модернізації національної кібербезпеки, функції NISA були інтегровані до Ізраїльського національного кібердиректорату (INCD), що був створений у 2018 році. Це дозволило об'єднати стратегічні та оперативні аспекти кібербезпеки під єдиним керівництвом, забезпечуючи більш ефективний захист кіберпростору Ізраїлю.

Цей орган відповідальний за всі аспекти кіберзахисту, починаючи від розробки державної політики та нарощування технологічних потужностей до оперативної діяльності спеціальних підрозділів. Він також забезпечує кібероборону в цивільному секторі, сприяючи ефективній координації та співпраці між державними установами та приватним сектором. Очікується, що Ізраїльський національний кібердиректорат, як нова комплексна державна структура, стане платформою для реалізації цілеспрямованої і збалансованої політики у сфері боротьби з кіберзлочинністю і тероризмом, об'єднуючи можливості військового і цивільного секторів. Вона відіграватиме ключову роль у захисті інтересів громадян, суспільства та держави в кіберпросторі [2].

Регулювання інформаційної безпеки в Ізраїлі базується на комплексному законодавстві, яке охоплює широкий спектр нормативних актів. Окрім законів, діє багато підзаконних актів, включаючи положення Міністерства юстиції та урядові постанови. Значний вплив на формування політики мають правила, розроблені неурядовими організаціями щодо надання інтернет-послуг. Ця нормативна база забезпечує захист як для користувачів інформаційних послуг, так і для національної безпеки, не порушуючи при цьому свободу інформації. Органи, що мають повноваження на доступ до інформації, такі як правоохоронні органи та спецслужби, дотримуються принципів прозорості та підзвітності перед громадськістю [1].

Як зазначають дослідники, система регулювання інформаційної безпеки в Ізраїлі більше схожа на європейську модель [10]. Вона включає детальний законодавчий опис прав і обов'язків власників баз даних. Ізраїльський закон «Про захист персональних даних» від 1981 року, розроблений із залученням провідних юристів і комітетів Кнесету у 1970-х роках, був новаторським у цій галузі. У 1994 році створена Ізраїльська Інтернет-асоціація, яка з 1997 року займається реєстрацією доменних імен для ізраїльських сайтів та надає послуги з переадресації і хостингу DNS (Система доменних імен) для ізраїльських інтернет-провайдерів [17].

Поняття «інформаційна безпека» чітко визначене в статті 7 Закону Ізраїлю «Про захист персональних даних» від 1981 року. Цей закон передбачає захист інформації від незаконного розкриття, використання та копіювання, забезпечуючи цілісність даних. Це положення узгоджується з умовами обмеження поширення інформації, зазначеними в статтях 9-11 Закону Ізраїлю «Про свободу інформації» від 1998 року. Наприклад, стаття 9 регулює повну заборону на розповсюдження інформації, яка може загрожувати державі, тоді як стаття 11 визначає умови для обмеженого поширення інформації або її передачі з певними умовами. Стаття 13 описує порядок нерозповсюдження інформації для захисту інтересів третіх сторін. Інформаційні ресурси в Інтернеті прирівнюються до засобів масової інформації і регулюються тими ж правовими нормами, що й інші медіа-джерела. Крім того, згідно з Правилами оборони (надзвичайний час) від 1945 року, у країні діє система військової цензури, яка надає право цензору забороняти будь-які публікації, що можуть загрожувати безпеці Ізраїлю, його мирному існуванню або громадському порядку [1].

У червні 2018 року Ізраїльський національний кібердиректорат (INCD) оприлюднив проєкт закону про кібербезпеку для обговорення громадськістю. Цей проєкт закону спрямований на регулювання діяльності INCD відповідно до рішень уряду та є завершальною стадією створення національної кібербезпекової структури. Документ складається з трьох основних розділів: 1) **організаційний розділ** визначає структуру та організаційні аспекти INCD; 2) **оперативний розділ**

описує повноваження щодо виявлення та реагування на кібератаки; 3) **регуляторний розділ** встановлює національні та секторальні регуляції, спрямовані на підвищення стійкості різних секторів та визначає роль INCD як національного регулятора у сфері кібербезпеки.

Протягом 2019-2020 років INCD провів понад 30 зустрічей з різними зацікавленими сторонами, установами та урядовими міністерствами для обговорення коментарів щодо цього проєкту закону. На основі цих обговорень у березні 2021 року був опублікований доопрацьований проєкт закону, який зазнав значної критики через надані INCD повноваження та питання захисту приватності громадян [13].

У липні 2016 року Армія оборони Ізраїлю (ЦАХАЛ) ухвалила стратегію, що підкреслює важливість розвитку кіберпотенціалу через два основні напрями. По-перше, було вирішено створити окреме кіберкомандування, яке підпорядковуватиметься начальнику Генерального штабу. Це командування відповідає за стратегічне планування та реалізацію кібероперацій, забезпечуючи інтеграцію кіберзахисту в загальну військову стратегію країни. По-друге, наголошується на необхідності розвитку технологічних можливостей для кіберзахисту, що включає як операційні, так і підтримувальні функції, як-от персонал і логістичні системи. Цей підхід дозволяє ЦАХАЛу ефективно реагувати на сучасні кіберзагрози та забезпечує безперервну оперативну готовність для захисту критичних військових систем та інфраструктури [15].

У 2017 році Ізраїль зайняв позицію серед провідних країн світу в плані підготовки та ефективності своїх кібервійськ. Щорічно на кібербезпеку виділяється 150 мільйонів доларів США, а понад 1000 спеціалістів працюють у кіберпідрозділах. Лідером у цій галузі є США, які вкладають 7 мільярдів доларів на рік і мають приблизно 9 тисяч кіберфахівців.

Ізраїль, спільно зі США, реалізує проєкти з кібербезпеки, спрямовані на освітню підготовку школярів та дітей дошкільного віку, як частину своєї комплексної боротьби з хакерськими загрозами. Починаючи з 2016 року, ізраїльський уряд запровадив новий тип робочих віз для залучення іноземних фахівців у сфері високих технологій. Завдяки цьому Ізраїль, відомий як постачальник стартапів, поступово перетворюється на глобальний центр передових технологій. На цьому тлі Ізраїль активно інтегрує компанії приватного сектору у сферу кібербезпеки. У 2017 році в країні діяло 420 кібербезпекових підприємств, а загальні витрати на цей сектор становили 815 мільйонів доларів США. Така активність закріпила за Ізраїлем репутацію глобального лідера в галузі інноваційних кібернетичних технологій.

З метою створення ефективної системи кібербезпеки уряд Ізраїлю ініціює та підтримує навчальні програми для підготовки спеціалізованих кадрів і інформування громадськості, включаючи навчання школярів навичок цифрового захисту. Також діють кілька освітніх програм для молоді віком 16-18 років. Ці програми сприяють підвищенню обізнаності населення у сфері інформаційної безпеки, що є важливим позитивним фактором для загального кіберзахисту країни.

Одна з ключових основ кібербезпеки в Ізраїлі – це протидія терористичним загрозам. 15 червня 2016 року ізраїльський Парламент ухвалив новий закон «Про боротьбу з тероризмом», який набув чинності 1 листопада 2016 року. Цей закон встановлює відповідальність за використання Інтернету та соціальних мереж у терористичних цілях. Він охоплює такі дії як використання кіберпростору для пропаганди терористичної діяльності, вербування, радикалізація суспільства, підбурювання до насильства та фінансування тероризму.

Ізраїльське кримінальне законодавство було доповнено положенням про кримінальну відповідальність за підбурювання до тероризму та демонстрацію солідарності з терористичними організаціями. Це включає діяльність в Інтернеті, яка підтримує або заохочує терористичні акти проти Ізраїлю та його громадян.

Законом передбачено кримінальну відповідальність за вербування до терористичних організацій, участь у тренуваннях, організованих терористами, публікацію закликів до терористичних актів, а також поширення повідомлень, які схвалюють або підтримують тероризм.

Додатково, закон надає суду право вимагати від адміністраторів соціальних мереж, таких як Facebook, YouTube, Twitter, видалення контенту, який пропагує тероризм. Зміни до закону, внесені на початку 2018 року, передбачають можливість застосування смертної кари до винних у тероризмі

Варто зауважити, що згідно зі статтею 1 Закону Ізраїлю «Про захист честі і гідності» від 1965 року, публікації в Інтернеті не включаються до джерел засобів масової інформації. Проте судова практика визнає, що статті, розміщені на вебсайтах і які порушують цей закон, можуть бути за-

криті як джерела інформації. Суд також визнає обов'язок редакторів та власників сайтів розкривати інформацію про осіб, які публікують незаконний контент, а також має право забороняти доступ винних осіб до таких сайтів і тимчасово зупиняти їхню діяльність. При цьому використовується аналогія зі статтею 9 цього закону. У 2008 році в поліції Ізраїлю був створений спеціальний підрозділ ЛАХАВ 443, який спеціалізується на боротьбі з кіберзлочинністю та незаконними азартними іграми в Інтернеті [1].

Законодавчі заходи Ізраїлю відображають його стратегічний підхід до кібербезпеки, спрямований на створення ефективної нормативної бази для управління цифровими загрозами та боротьби з кіберзлочинністю.

Україна знаходиться на початковому етапі боротьби з кіберзлочинністю, але влада вже активно розвиває цю сферу. Значним кроком стало створення у жовтні 2015 року кіберполіції, яка функціонує в межах Національної поліції України і спеціалізується на захисті прав і свобод громадян, а також на запобіганні, виявленні та розслідуванні кіберзлочинів.

З 2016 року, коли була прийнята Стратегія кібербезпеки України, почалася активна розбудова національної системи кібербезпеки. Були створені спеціалізовані центри кіберзахисту у ключових державних установах, таких як Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний банк України, Міністерство інфраструктури України, Міністерство оборони України, та Збройні Сили України.

У жовтні 2017 року був ухвалений Закон України «Про основні засади забезпечення кібербезпеки України», що визначає правові основи захисту національних інтересів у кіберпросторі. Він встановлює цілі та принципи державної політики у сфері кібербезпеки, повноваження державних органів та інші ключові аспекти.

У 2021 році було затверджено оновлену Стратегію кібербезпеки України та створено Національний координаційний центр кібербезпеки, що координує діяльність всіх органів у сфері кібербезпеки. Ці заходи доповнюються активною міжнародною співпрацею з країнами ЄС, США, НАТО та іншими партнерами для проведення кібернавчань та обміну передовим досвідом.

Висновки. Отже, досвід Ізраїлю у формуванні ефективної системи кібербезпеки є надзвичайно цінним для України, особливо в умовах поточної війни з Росією. Україна, подібно до Ізраїлю, постійно перебуває у стані підвищеної готовності до різних загроз національній безпеці, що вимагає інтеграції комплексних підходів до захисту кіберпростору.

Ізраїль демонструє успішну інтеграцію правових, організаційних і технологічних заходів у сфері кібербезпеки, що включає створення спеціалізованих кіберпідрозділів і координаційних центрів. Ефективне залучення як державних, так і приватних зусиль, а також міжнародна співпраця відіграють ключову роль у забезпеченні кіберзахисту.

Для України, яка стикається з постійними кіберзагрозами, ізраїльський досвід може слугувати моделлю для розбудови власної системи кібербезпеки. Впровадження подібних стратегій та структур сприятиме підвищенню здатності України протидіяти кіберзлочинності і захищати національні інтереси.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бєлєвцева В. (2024). Основи правового регулювання інформаційної сфери у державі Ізраїль. *Інформація і право*, 1(48), 162–169.
2. Гребенюк М.В., & Леонов Б.Д. (2018). Досвід Ізраїлю у сфері забезпечення кібербезпеки. *Інформація і право*, 2(25), 45–50.
3. Конвенція про кіберзлочинність: від 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 22.04.2024).
4. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/234114?find=1&text=кібер#n1263 (дата звернення: 29.04.2024).
5. Указ Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України» від 14 травня 2021 року "Про Стратегію кібербезпеки України". URL: https://www.president.gov.ua/ documents/4472021-40013 (дата звернення: 04.05.2024).
6. Водовський В. (2023). Кіберзлочинність в Україні. URL: https://equity.law/press-center/publications/1169.html (дата звернення: 07.06.2024).
7. Legal IT Group. Правове регулювання відповідальності за кіберзлочини в Україні. URL:

https://legalitgroup.com/pravove-regulyuvannya-vidpovidalnosti-za-kiberzlochini-v-ukrayini/ (дата звернення: 03.06.2024).
8. Cohen M.S., Freilich C.D., & Siboni G. (2015). Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives, 1–15. URL: https://www.inss.org.il/ he/wpcontent/uploads/sites/2/systemfiles/Israel%20and%20cyberspace.pdf (дата звернення: 20.05.2024).
9. Cyber Power – Tier Two. (2021, 28 June). International Institute for Strategic Studies (IISS). URL: https://www.iiss.org/research-paper/2021/06/cyber-power---tier-two/ (дата звернення: 26.04.2024).
10. Directive 96/9/EC of the European Parliament and of the Council on 11 March 1996 on the Legal Protection of Databases. (1996). Official Journal of the European Union (L77), 20. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31996L0009 (дата звернення: 25.05.2024).
11. Global Cybersecurity Index 2020. (2021). URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (дата звернення: 10.06.2024).
12. NCSI: Israel. (2023, 01 September). National Cyber Security Index (NCSI). URL: https://ncsi.ega.ee/ncsi-index/?type=c&archive=1 (дата звернення: 23.05.2024).
13. Stancu A.-I., & Pavel T. (2023). Unveiling Israel's Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies. Perspectives of Law and Public Administration, 12(4), 643–650.
14. The Cyber Defense Index 2022/23. (2023). MIT Technology Review. URL: https://mittrinsights.s3.amazonaws.com/CDIreport.pdf (дата звернення: 24.05.2024).
15. The IDF Strategy. (2016). URL: https://www.inss.org.il/he/wp-content/uploads/ sites/2/2017/04/IDF-Strategy.pdf (дата звернення: 30.04.2024).
16. Voo J., Hemani I., & Cassidy D. (2022). National Cyber Power Index 2022. URL: https://www.belfercenter.org/project/cyber-project (дата звернення: 02.06.2024).
17. The Israel Internet Association (ISOC-IL). URL: http://www.isoc.org.il/ about_heb/index.html (дата звернення: 09.11.2023).