ISSN 3041-1238 № 6 (6) 2024

DOI: https://doi.org/10.26642/sas-2024-6(6)-37-43
УДК 327:004.056:351.86

Сумін Павло
аспірант
Київський університет культури
https://orcid.org/0009-0000-1029-4063

Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи

Анотація. Інформаційні технології (ІТ) стають одним з ключових інструментів забезпечення національної безпеки в умовах швидкого розвитку цифрового середовища. Сучасні виклики, такі як кібератаки, дезінформаційні кампанії, втручання у внутрішні справи держав та інші форми гібридних загроз, підвищують актуальність використання ІТ для захисту державних інтересів і безпеки. Однією з головних проблем у цій сфері є кібербезпека. З кожним роком збільшується кількість кібератак, націлених на критичну інфраструктуру, урядові структури та приватний сектор. Це зумовлює необхідність постійного вдосконалення засобів захисту інформаційних систем. У цьому контексті важливою є розробка ефективних механізмів захисту державних інформаційних ресурсів, а також створення надійної системи кібероборони. Водночас багато держав стикаються з проблемою недостатньої кваліфікації фахівців у цій галузі, що призводить до вразливості перед новими видами кібератак. Іншим важливим аспектом є питання захисту інформаційного простору від пропаганди та дезінформації. Інформаційні технології стали засобом впливу на масову свідомість та громадську думку, що використовують різні політичні сили для послаблення державних структур або зміни політичного курсу. Для боротьби з такими загрозами необхідно впроваджувати механізми моніторингу та аналізу інформаційних потоків, які дозволяють швидко виявляти фейкові новини та пропагандистські кампанії. Крім того, важливою є розробка ефективних засобів протидії інформаційним загрозам, які не порушуватимуть основоположних прав людини, таких як свобода слова. Перспективи розвитку інформаційних технологій у сфері національної безпеки полягають у подальшому вдосконаленні кіберзахисту, розширенні системи моніторингу інформаційного простору та розвитку технологій для оборонних потреб. Однак ці досягнення вимагають значних інвестицій у дослідження та освіту, щоб підготувати кваліфікованих фахівців і створити надійну інфраструктуру для забезпечення безпеки. Лише комплексний підхід до вирішення проблем, пов’язаних із впровадженням ІТ у національну безпеку, дозволить державам ефективно протистояти сучасним загрозам та захистити свої стратегічні інтереси.

Ключові слова: технології; безпека; інформаційна безпека; національна безпека; кібербезпека.

Актуальність теми. Інформаційні технології відіграють визначальну роль у забезпеченні національної безпеки в умовах сучасного глобалізованого світу. Інтеграція цифрових рішень у системи державного управління, оборони та критичної інфраструктури створює нові можливості для захисту національних інтересів. Першочергового значення набуває кібербезпека як компонент національної безпеки. Розвинені держави інвестують значні ресурси в розробку передових систем виявлення та протидії кіберзагрозам, захисту державних інформаційних систем та баз даних. Технології штучного інтелекту та машинного навчання дозволяють аналізувати великі масиви даних для прогнозування та запобігання потенційним загрозам.

Важливим аспектом є також використання інформаційних технологій для протидії дезінформації та інформаційним операціям. Системи моніторингу інформаційного простору, аналізу медіаконтенту та виявлення фейкової інформації стають критично важливими інструментами забезпечення інформаційної безпеки держави. Водночас розвиток технологій вимагає постійного вдосконалення нормативно-правової бази та механізмів міжнародної співпраці у сфері кібербезпеки. Лише комплексний підхід до впровадження інформаційних технологій може забезпечити належний рівень національної безпеки в сучасних умовах.

В умовах глобальних трансформацій та російської військової агресії проти України особливої актуальності набуває питання забезпечення національної безпеки за допомогою сучасних інформаційних технологій. Повномасштабне вторгнення рф продемонструвало критичну важливість технологічної переваги у протистоянні гібридним загрозам та веденні кібервійни.

Попри значний прогрес у розвитку інформаційних технологій та їх інтеграції в системи національної безпеки, залишається низка невирішених проблем. Зокрема, це питання вразливості критичної

інфраструктури до кібератак, недостатньої координації між різними безпековими структурами, необхідності модернізації технічного забезпечення та підготовки фахівців відповідного профілю.

Особливої уваги потребує дослідження механізмів протидії інформаційним операціям противника, захисту державних інформаційних ресурсів та розвитку потенціалу кіберзахисту в умовах постійної еволюції загроз національній безпеці.

Аналіз останніх досліджень та публікацій. Питанням інформаційної безпеки держави та ролі технологій в її забезпеченні присвячена значна кількість наукових праць вітчизняних науковців. Українська науковиця В.Аніщук [1] досліджує інформаційну безпеку як один із ключових елементів національної безпеки України, акцентуючи увагу на тому, як інформаційна безпека стає об'єктом посягань у контексті злочинів проти основ державної безпеки. Дослідники Т.Васильєва та П.Костельскій [2] аналізують механізми, які сприяють підвищенню цифрової інклюзії населення, що, на їхню думку, є важливим фактором для забезпечення інформаційної безпеки держави. Виздрик В. та Мельник О. [3] розглядають сучасний стан інформаційної безпеки в Україні, вивчаючи її основні проблеми та виклики, з якими стикається держава в умовах швидкого розвитку технологій. Гайдук О. та Звєрєв В. [5] зосереджують свою увагу на аналізі кіберзагроз, що виникають у зв'язку зі стрімким розвитком інформаційних технологій, а також на способах їх нейтралізації.

Горулько В. [6] розглядає роль та місце інформаційної безпеки в загальній системі національної безпеки держави, аналізуючи її взаємозв'язок з іншими елементами національної безпеки. Котерлін І. [7] досліджує інформаційну безпеку в умовах воєнного стану, звертаючи увагу на забезпечення інформаційних прав та свобод громадян у такий складний період. Котляров В. [9] зосереджує свою увагу на аналізі сучасного стану інформаційної безпеки в Україні, виділяючи основні проблеми та напрями розвитку в цій сфері. Кривцов В. [10] аналізує інформаційні заходи оборони держави в сучасних умовах, особливо в контексті захисту від зовнішніх інформаційних загроз.

Куперштейн Л., Луцишин Г. та Кренцін М. [11] розробляють інформаційні технології, призначені для моніторингу безпеки даних програмного забезпечення, що має важливе значення для захисту від кіберзагроз. А Мігус І. [12] досліджує розвиток індустрії 4.0 та її вплив на економічну безпеку держави, особливо з урахуванням міжнародного контексту та викликів, що виникають у процесі технологічного прогресу. Поронюк Р. та Гапеєва О. [13] вивчають діяльність груп моніторингу інформаційного простору та заходи протидії, що є важливим аспектом забезпечення інформаційної безпеки держави, особливо у воєнній сфері. Пучков О., Субач І. та Рибак О. [14] розробляють інформаційні технології для визначення політичного спрямування джерел інформації з метою забезпечення інформаційної безпеки держави в умовах кризових ситуацій.

Метою статті є систематизація проблем та перспектив використання інформаційних технологій в контексті забезпечення національної безпеки держави на сучасному етапі розвитку.

Викладення основного матеріалу. Інформаційні технології – це сукупність методів, інструментів, процесів і засобів, спрямованих на збір, опрацювання, зберігання, передачу та використання інформації для забезпечення вирішення різноманітних завдань у різних сферах діяльності [10]. Основою інформаційних технологій є сучасні апаратні засоби (комп'ютери, сервери, мережеве обладнання) та програмне забезпечення, що реалізує алгоритми автоматизованої обробки даних.

Інформаційні технології охоплюють широкий спектр інструментів і рішень, зокрема:

1. Обчислювальні системи та мережі, які забезпечують обмін даними та їхній централізований аналіз;
2. Програмні платформи, що містять операційні системи, бази даних, вебдодатки та спеціалізоване програмне забезпечення для аналітики;
3. Алгоритми обробки даних, зокрема ті, що використовують штучний інтелект і машинне навчання, для автоматизації рутинних процесів і прогнозування;
4. Засоби захисту інформації, такі як криптографічні алгоритми, брандмауери, антивірусне програмне забезпечення;
5. Хмарні обчислення, які забезпечують гнучкість і масштабованість обробки даних [14].

Таким чином, сучасні інструменти, що у сукупності складають інформаційні технології, включають системи аналізу даних, шифрування, штучний інтелект, хмарні обчислення, а також засоби моніторингу та виявлення загроз. Вони відіграють ключову роль у забезпеченні інформаційної безпеки держави. Зокрема, вони забезпечують захист від сучасних загроз, таких як кібератаки, дезінформація, несанкціонований доступ до надважливих даних і навіть маніпуляції суспільною думкою.

Сучасні автоматизовані системи моніторингу інформаційного простору, побудовані на базі штучного інтелекту та технологій машинного навчання, дозволяють здійснювати цілодобовий аналіз великих обсягів інформації. Це допомагає оперативно виявляти потенційні загрози, наприклад, кібератаки чи поширення фейкових новин, у режимі реального часу, що суттєво підвищує ефективність реагування [3, 6–10, 13]. Завдяки прогнозуванню ризиків на основі аналізу патернів даних, можна заздалегідь реагувати на кіберзагрози, мінімізуючи їхній вплив. Алгоритми штучного інтелекту можуть

прогнозувати можливі ризики для національної безпеки, дозволяючи державним установам вживати превентивних заходів.

Криптографічні алгоритми та системи шифрування відіграють важливу роль у захисті конфіденційної інформації. Вони забезпечують надійну передачу та зберігання даних, що відіграє надзвичайно важливу роль у міжвідомчій комунікації. Хмарні технології створюють додаткові можливості для забезпечення стійкості державних інформаційних систем. Їхня здатність до масштабування сприяє швидкій модернізації інфраструктури, дозволяючи адаптуватися до нових викликів. До того ж розподілений характер хмарних сервісів підвищує захист від фізичних загроз, таких як природні катастрофи або техногенні аварії. Автоматизовані платформи координації, які поєднують державні установи, забезпечують швидкий обмін інформацією, що є важливим у боротьбі з дезінформацією. Такі платформи дозволяють оперативно реагувати на інформаційні атаки, об'єднуючи зусилля різних органів влади [1, 2, 5, 14].

Проте, незважаючи на очевидні переваги, існують і певні проблеми у використанні інформаційних технологій для забезпечення національної безпеки (рис. 1):

1. Кіберзагрози та кібератаки на критичну інфраструктуру як виклик для національної безпеки. Критична інфраструктура держави, до якої належать енергетичні системи, транспортні мережі, системи водопостачання, охорони здоров'я та державні інформаційні ресурси, є одним із головних об'єктів кібератак. Особливо це стосується умов військової агресії, коли атаки стають частиною гібридної війни. Наприклад, атаки на енергетичну інфраструктуру України у 2015–2016 роках, що призвели до відключення електроенергії у кількох регіонах, продемонстрували руйнівний потенціал цілеспрямованих дій кіберзлочинців [4]. Ці інциденти підтверджують високу ефективність кібератак у дестабілізації державних систем і підриві суспільної довіри.

Крім того, зростає частота застосування шкідливого програмного забезпечення, такого як віруси-шифрувальники або ботнет-мережі, які порушують роботу стратегічних об'єктів. Такі дії можуть призвести не лише до економічних втрат, але й створити гуманітарну кризу, якщо порушення торкаються базових послуг. З огляду на це, захист критичної інфраструктури є пріоритетним завданням для національної безпеки;

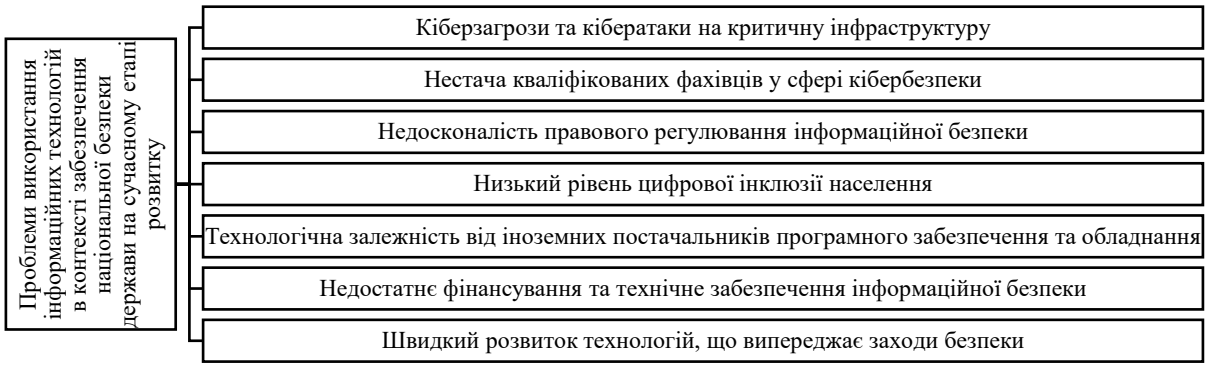
2. Нестача кваліфікованих фахівців у сфері кібербезпеки. Один із найбільш виражених викликів у протидії кіберзагрозам – це дефіцит спеціалістів, які мають відповідний рівень підготовки. Згідно зі звітами провідних аналітичних компаній, наприклад Gartner, глобальний попит на експертів у сфері кібербезпеки значно перевищує пропозицію, що створює проблему як для приватного сектора, так і для державних структур [16]. У контексті України проблема посилюється через військову агресію, що ставить перед фахівцями нові складні виклики.

Освітні програми у цій сфері не завжди відповідають швидкості розвитку інформаційних загроз. Наприклад, кіберзагрози, які базуються на використанні штучного інтелекту, вимагають від фахівців не лише розуміння існуючих технічних засобів захисту, але й глибоких знань у галузі алгоритмів машинного навчання. Відсутність таких навичок значно знижує ефективність боротьби з новими загрозами;

3. Недосконаліть правового регулювання інформаційної безпеки. Ефективне реагування на кіберінциденти потребує узгоджених і чітких дій державних структур, однак недосконаліть нормативно-правової бази часто ускладнює цей процес. В Україні, а також в інших країнах законодавство не встигає за розвитком технологій і виникненням нових форм загроз, таких як деструктивні інформаційні операції чи атаки на основі соціальної інженерії. Відсутність чітких механізмів координації дій між державними установами під час кризових ситуацій є суттєвим недоліком. Наприклад, недостатня інтеграція між службами кібербезпеки та правоохоронними органами може призводити до затримок у реагуванні на інциденти. Для розв'язання цієї проблеми необхідно розробити комплексну нормативно-правову базу, яка враховувала б міжнародний досвід та відповідала сучасним загрозам. Законодавство також має стимулювати впровадження новітніх технологій кіберзахисту в державному секторі, враховуючи використання штучного інтелекту та систем автоматизованого моніторингу;

4. Низький рівень цифрової інклюзії населення. Цифрова інклюзія, яка визначає рівень доступу громадян до інформаційних технологій та їхніх навичок використання, є важливим елементом національної безпеки. Недостатня обізнаність громадян про правила кібергігієни (наприклад, безпечне поводження з паролями чи уникнення фішингових атак) робить їх легкою мішенню для шахрайства і маніпуляцій. Згідно з дослідженням Міжнародного союзу електрозв'язку (ITU), близько 60% населення країн із середнім рівнем доходу не володіє базовими цифровими навичками, що відкриває шлях для поширення соціальної інженерії [18]. У випадках масових інформаційних кампаній, організованих зовнішніми загрозами, це ускладнює захист інформаційного простору, адже маніпуляції громадською думкою можуть використовуватися для дестабілізації ситуації в країні;

5. Технологічна залежність від іноземних постачальників. У більшості країн світу залежність від закордонного програмного забезпечення та обладнання створює високі ризики, особливо у стратегічно важливих секторах. Наприклад, у випадках, коли іноземні розробники залишають у системах так звані «бекдори» (задні двері), виникає загроза несанкціонованого доступу до конфіденційної інформації. Звіт аналітичного центру RAND вказує, що залежність від сторонніх постачальників у сфері кібербезпеки може призводити до втрати контролю над національними технологіями, а також до економічних втрат через можливу зупинку роботи систем у разі геополітичних конфліктів [19]. У контексті України це особливо актуально через геополітичну напруженість із сусідніми країнами;



Джерело: сформовано автором на основі [1–14]

Рис. 1. Проблеми використання інформаційних технологій в контексті забезпечення національної безпеки держави на сучасному етапі розвитку

6. Недостатнє фінансування та технічне забезпечення. Фінансові обмеження є однією з головних причин низької ефективності кіберзахисту у державному секторі. Відповідно до даних Глобального індексу кіберготовності, країни з обмеженими ресурсами значно відстають у впровадженні сучасних технологій моніторингу та захисту [17]. У випадку України, за даними Держспецзв'язку, лише 15 % державних установ мають доступ до оновлених систем кіберзахисту, тоді як інші покладаються на застарілі рішення. Це створює значні ризики як для захисту інформації, так і для безпеки систем, що обслуговують громадян;

7. Розрив між існуючими заходами безпеки та актуальними викликами. Постійне вдосконалення засобів кіберзлочинців, таких як використання штучного інтелекту для автоматизації атак чи квантових обчислень для зламу шифрування, підкреслює важливість адаптації систем кібербезпеки до нових викликів. За даними Європейського агентства з кібербезпеки (ENISA), понад 80 % існуючих кіберзахисних інструментів стають менш ефективними через 3–5 років після впровадження через стрімкий технологічний прогрес [15]. У разі відсутності постійного оновлення технологій держави залишаються вразливими до атак, що можуть спричинити серйозні економічні та соціальні наслідки.

В умовах сучасних викликів національній безпеці, особливо під час російської агресії, ефективне використання інформаційних технологій стає критично важливим фактором захисту державних інтересів. Подолання виявлених проблем вимагає комплексного підходу, що містить модернізацію технічної інфраструктури, вдосконалення нормативно-правової бази, підготовку кваліфікованих фахівців та розвиток вітчизняних технологічних рішень. Лише системна робота у цих напрямках забезпечить належний рівень інформаційної безпеки держави.

Відповідно до дослідницької проблематики цієї наукової статті, здійснимо систематизацію та розкриття сутності ключових перспектив використання інформаційних технологій в контексті забезпечення національної безпеки держави на сучасному етапі розвитку, для цього скористаємося наведеною нижче блок-схемою (рис. 2).

Розглянемо більш детально ключові перспективи використання інформаційних технологій в контексті забезпечення національної безпеки держави на сучасному етапі розвитку:

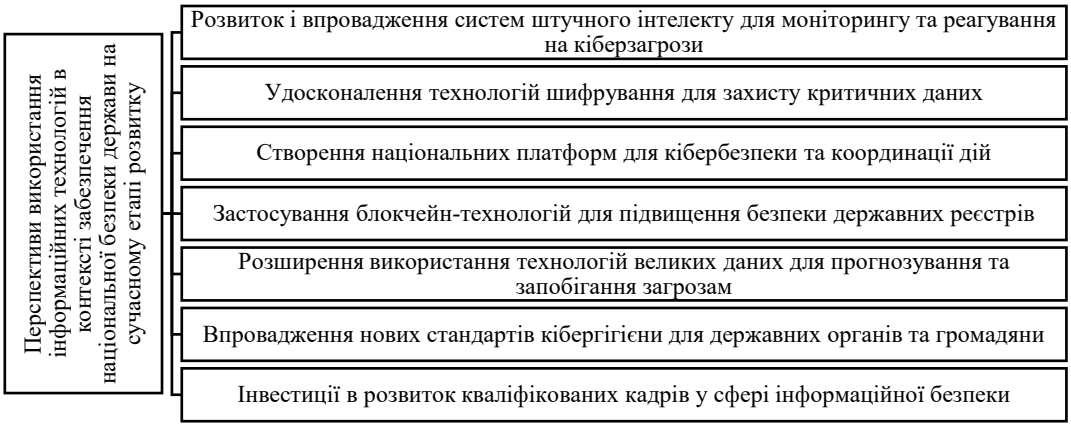
– розвиток і впровадження систем штучного інтелекту відкриває нові можливості для автоматизованого виявлення та нейтралізації кіберзагроз. Інтелектуальні системи здатні аналізувати величезні масиви даних у режимі реального часу, виявляти аномалії та потенційні атаки, що суттєво підвищує ефективність захисту інформаційної інфраструктури держави;

– удосконалення технологій шифрування стає критично важливим напрямком розвитку інформаційної безпеки. Впровадження передових криптографічних методів, зокрема квантової

криптографії, забезпечить надійний захист конфіденційної інформації та державних таємниць від несанкціонованого доступу та кібершпигунства;

– створення національних платформ для кібербезпеки дозволить централізувати управління інформаційною безпекою та покращити координацію між різними державними структурами. Єдина система моніторингу та реагування на інциденти підвищить ефективність протидії кіберзагрозам на національному рівні;

– застосування блокчейн-технологій у державних реєстрах забезпечить безпрецедентний рівень захисту та прозорості даних. Децентралізована структура та криптографічні механізми блокчейну унеможливлять несанкціоноване втручання та модифікацію інформації, підвищуючи довіру до державних інформаційних систем;



Джерело: сформовано автором на основі [1–14]

Рис. 2. Перспективи використання інформаційних технологій в контексті забезпечення національної безпеки держави на сучасному етапі розвитку

– розширення використання технологій великих даних (Big Data) відкриває нові горизонти у сфері національної безпеки. Застосування передових аналітичних інструментів дозволяє обробляти та аналізувати масштабні інформаційні потоки, виявляти приховані закономірності та потенційні загрози, а також формувати прогностичні моделі для превентивного реагування на виклики інформаційній безпеці держави;

– впровадження нових стандартів кібергігієни для державних органів та громадян сприятиме формуванню культури інформаційної безпеки. Розробка та імплементація сучасних протоколів захисту, навчальних програм та систем контролю забезпечить комплексний підхід до мінімізації ризиків кіберінцидентів;

– інвестиції в розвиток кваліфікованих кадрів у сфері інформаційної безпеки є стратегічно важливим напрямом зміцнення національної безпеки. Створення спеціалізованих освітніх програм, центрів підготовки та перепідготовки фахівців, залучення міжнародного досвіду та впровадження інноваційних методик навчання забезпечить формування потужного кадрового потенціалу.

Аналіз проблем та перспектив використання інформаційних технологій у сфері національної безпеки свідчить про необхідність системної трансформації підходів до забезпечення кіберзахисту держави. Попри наявність суттєвих викликів, впровадження інноваційних технологічних рішень, розвиток кадрового потенціалу та вдосконалення нормативно-правової бази створюють підґрунтя для побудови ефективної системи інформаційної безпеки держави. Особливої актуальності це набуває в умовах російської агресії та зростання кількості кіберзагроз глобального характеру в світі.

Висновки та перспективи подальших досліджень. У сучасних умовах глобальної цифровізації та військової агресії російської федерації проти України, комплексний аналіз проблем та перспектив використання інформаційних технологій у сфері національної безпеки набуває особливого значення. Виявлені проблеми, зокрема кіберзагрози критичній інфраструктурі, нестача кваліфікованих фахівців, недосконаліть правового регулювання та технологічна залежність від іноземних постачальників, створюють суттєві виклики для забезпечення інформаційної безпеки держави.

Водночас, окреслені перспективи розвитку демонструють значний потенціал для посилення системи національної безпеки через впровадження передових технологічних рішень. Використання штучного інтелекту, вдосконалення криптографічних методів, створення національних платформ кібербезпеки та застосування блокчейн-технологій відкривають нові можливості для протидії сучасним загрозам.

Ключовим фактором успішної реалізації окреслених перспектив є забезпечення комплексного підходу, що містить модернізацію технічної інфраструктури, розвиток вітчизняних технологічних рішень, підготовку висококваліфікованих фахівців та вдосконалення нормативно-правової бази. Лише системна робота у цих напрямах, забезпечена належним фінансуванням та міжнародною співпрацею, здатна створити належний рівень інформаційної безпеки держави в умовах сучасних викликів.

Список використаної літератури:

1. *Аніщук В.* Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України / *В.Аніщук* // Науковий вісник Ужгородського національного університету. Серія : Право. – 2023. – № 2 (77). – С. 139–143.
2. *Васильєва Т.* Механізми підвищення цифрової інклюзії населення для забезпечення інформаційної безпеки держави / *Т.Васильєва, П.Костельскій* // Економіка і регіон. – 2023. – № 3 (90). – С. 139–145.
3. *Виздрик В.* Інформаційна безпека в Україні : сучасний стан / *В.Виздрик, О.Мельник* // Grail of Science. – 2023. – № 24. – С. 196–202.
4. Відключення електроенергії в Україні було хакерською атакою / BBC News Україна [Електронний ресурс]. – Режим доступу : https://www.bbc.com/ukrainian/news–38585587.
5. *Гайдук О.* Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій / *О.Гайдук, В.Звєрєв* // Кібербезпека : освіта, наука, техніка. – 2024. – № 3 (23). – С. 225–236.
6. *Горулько В.* Роль і місце інформаційної безпеки в загальній системі національної безпеки держави / *В.Горулько* // Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Право. – 2022. – № 34. – С. 103–108.
7. Кібербезпека в інформаційному суспільстві : Інформаційно – аналітичний дайджест / відп. ред. *О.Довгань* ; упоряд. *О.Довгань, Л.Литвинова, С.Дорогих* ; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України» ; Національна бібліотека України ім. В.І. Вернадського. – К., 2023. – № 9 (вересень). – 351 с.
8. *Котерлін І.Б.* Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод / *І.Б. Котерлін* // Актуальні проблеми вітчизняної юриспруденції. – 2022. – № 1. – С. 150–155.
9. *Котляров В.* Аналіз сучасного стану інформаційної безпеки в Україні / *В.Котляров* // Mechanism of an economic regulation. – 2024. – № 2 (104). – С. 101–104.
10. *Кривцов В.Ю.* Інформаційні заходи оборони держави в сучасних умовах / *В.Ю. Кривцов* // Часопис Київського університету права. – 2023. – № 1. – С. 30–33.
11. *Куперштейн Л.* Інформаційна технологія моніторингу безпеки даних програмного забезпечення / *Л.Куперштейн, Г.Луцишин, М.Кренцін* // Кібербезпека : освіта, наука, техніка. – 2024. – № 3 (23). – С. 71–84.
12. *Мігус І.* Основні тенденції розвитку індустрії 4.0 та її вплив на економічну безпеку держави : міжнародний аспект / *І.Мігус* // Вчені записки Університету «КРОК». – 2023. – № 1 (69). – С. 52–59.
13. *Поронюк Р.О.* Діяльність груп моніторингу інформаційного простору та протидії як складова забезпечення інформаційної безпеки держави у воєнній сфері / *Р.О. Поронюк, О.Л. Гапеєва* // Військово–науковий вісник. – 2022. – № 38. – С. 266–280.
14. *Пучков О.* Інформаційна технологія визначення політичного спрямування джерел інформації для забезпечення інформаційної безпеки держави під час кризових ситуацій / *О.Пучков, І.Субач, О.Рибак* // Кібербезпека : освіта, наука, техніка. – 2023. – № 4 (20). – С. 142–152.
15. Foresight Cybersecurity Threats For 2030 – Update 2024 : Executive Summary / Enisa [Electronic resource]. – Access mode : https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for–2030-update–2024-executive-summary.
16. Gartner Forecasts Global Information Security Spending to Grow 15% in 2025 / Gartner [Electronic resource]. – Access mode : https://www.gartner.com/en/newsroom/press-releases/2024–08–28-gartner-forecasts-global-information-security-spending-to-grow–15-percent-in–2025.
17. Global Cybersecurity Index 2024 5th Edition / ITU [Electronic resource]. – Access mode : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.
18. Measuring digital development: Facts and Figures 2024 / ITU [Electronic resource]. – Access mode : https://www.itu.int/en/ITU-D/Statistics/pages/facts/default.aspx.
19. Threats to Critical Infrastructure / RAND [Electronic resource]. – Access mode : https://www.rand.org/pubs/research_reports/RRA2397–2.html

References:

1. Anishchuk, V. (2023), «Informatsiina bezpeka yak obiekt posiahannia zlochyniv proty osnov natsionalnoi bezpeky Ukrainy», *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. Seriia: *Pravo*, No. 2 (77), pp. 139–143.
2. Vasylieva, T. and Kostelskyi, P. (2023), «Mekhanizmy pidvyshchennia tsyfrovoi inkluzii naselennia dlia zabezpechennia informatsiinoi bezpeky derzhavy», *Ekonomika i rehion*, No. 3 (90), pp. 139–145.
3. Vyzdryk, V. and Melnyk, O. (2023), «Informatsiina bezpeka v Ukraini: suchasnyi stan», *Grail of Science*, No. 24, pp. 196–202.
4. *BBC News Ukrainian*, «Vykliuchennia elektroenerhii v Ukraini bulo khakerskoiu atakoiu», [Online], available at: https://www.bbc.com/ukrainian/news–38585587

5. Haiduk, O. and Zvieriev, V. (2024), «Analiz kiberzahroz v umovakh strimkoho rozvytku informatsiinykh tekhnolohii», *Kiberbezpeka: osvita, nauka, tekhnika*, No. 3 (23), pp. 225–236.
6. Horulko, V. (2022), «Rol i mistse informatsiinoi bezpeky v zahalnii systemi natsionalnoi bezpeky derzhavy», *Visnyk Kharkivskoho natsionalnoho universytetu imeni V.N. Karazina*. Seriia: *Pravo*, No. 34, pp. 103–108.
7. Dovhan, O. (ed.) (2023), *Kiberbezpeka v informatsiinomu suspilstv*i, Informatsiino – analitychnyi daidzhest, uporiad. Dovhan, O., Lytvynova, L., Dorohykh, S., Derzhavna naukova ustanova «Instytut informatsii, bezpeky i prava NAPrN Ukrainy», Natsionalna biblioteka Ukrainy im. V.I.Vernadskoho, K., No. 9 (veresen), 351 p.
8. Koterlin, I.B. (2022), «Informatsiina bezpeka v umovakh voiennoho stanu u aspekti zabezpechennia informatsiinykh prav ta svobod», *Aktualni problemy vitchyznianoi yurysprudentsii*, No. 1, pp. 150–155.
9. Kotliarov, V. (2024), «Analiz suchasnoho stanu informatsiinoi bezpeky v Ukraini», *Mechanism of an economic regulation*, No. 2 (104), pp. 101–104.
10. Kryvtsov, V.Yu. (2023), «Informatsiini zakhody oborony derzhavy v suchasnykh umovakh», *Chasopys Kyivskoho universytetu prava*, No. 1, pp. 30–33.
11. Kupershtein, L., Lutsyshyn, H. and Krentsin, M. (2024), «Informatsiina tekhnolohiia monitorynhu bezpeky danykh prohramnoho zabezpechennia», *Kiberbezpeka: osvita, nauka, tekhnika*, No. 3 (23), pp. 71–84.
12. Mihus, I. (2023), «Osnovni tendentsii rozvytku industrii 4.0 ta yii vplyv na ekonomichnu bezpeku derzhavy: mizhnarodnyi aspekt», *Vcheni zapysky Universytetu «KROK»*, No. 1 (69), pp. 52–59.
13. Poroniuk, R.O. and Hapieieva, O.L. (2022), «Diialnist hrup monitorynhu informatsiinoho prostoru ta protydii yak skladova zabezpechennia informatsiinoi bezpeky derzhavy u voiennii sferi», *Viiskovo-naukovyi visnyk*, No. 38, pp. 266–280.
14. Puchkov, O., Subach, I. and Rybak, O. (2023), «Informatsiina tekhnolohiia vyznachennia politychnoho spriamuvannia dzherel informatsii dlia zabezpechennia informatsiinoi bezpeky derzhavy pid chas kryzovykh sytuatsii», *Kiberbezpeka: osvita, nauka, tekhnika*, No. 4 (20), pp. 142–152.
15. *Enisa*, «Foresight Cybersecurity Threats For 2030 – Update 2024: Executive Summary», [Online], available at: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for–2030-update–2024-executive-summary
16. *Gartner*, «Gartner Forecasts Global Information Security Spending to Grow 15 % in 2025», [Online], available at: https://www.gartner.com/en/newsroom/press-releases/2024–08–28-gartner-forecasts-global-information-security-spending-to-grow–15-percent-in–2025
17. *ITU*, «Global Cybersecurity Index 2024 5th Edition», [Online], available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
18. *ITU*, «Measuring digital development: Facts and Figures 2024», [Online], available at: https://www.itu.int/en/ITU-D/Statistics/pages/facts/default.aspx
19. *RAND*, «Threats to Critical Infrastructure», [Online], available at: https://www.rand.org/pubs/research_reports/RRA2397–2.html

---

Sumin P.

Information technologies as a tool for ensuring national security at the current stage of development: problems and prospects

Abstract. Information technologies (IT) are becoming one of the key tools for ensuring national security in the conditions of rapid development of the digital environment. Modern challenges, such as cyber-attacks, disinformation campaigns, interference in the internal affairs of states and other forms of hybrid threats, increase the urgency of using IT to protect state interests and security.

One of the main problems in this area is cyber security. The number of cyberattacks targeting critical infrastructure, government structures, and the private sector is increasing every year. This necessitates the constant improvement of means of protection of information systems. In this context, it is important to develop effective mechanisms for the protection of state information resources, as well as to create a reliable cyber defense system. At the same time, many countries face the problem of insufficient qualifications of specialists in this field, which leads to vulnerability to new types of cyber attacks.

Another important aspect is the issue of protecting the information space from propaganda and disinformation. Information technology has become a means of influencing mass consciousness and public opinion, which various political forces use to weaken state structures or change political course. In order to combat such threats, it is necessary to implement mechanisms for monitoring and analyzing information flows, which allow for quick detection of fake news and propaganda campaigns. In addition, it is important to develop effective means of countering information threats that do not violate fundamental human rights, such as freedom of speech.

Prospects for the development of information technologies in the field of national security consist in the further improvement of cyber defense, the expansion of the information space monitoring system, and the development of technologies for defense needs. However, these advances require significant investment in research and education to train skilled professionals and create a robust infrastructure to ensure security. Only a comprehensive approach to solving problems related to the introduction of IT into national security will allow states to effectively confront modern threats and protect their strategic interests.

Keywords: technologies; security; information security; national security; cyber security.

Стаття надійшла до редакції 26.10.2024.