УДК 341.24:004.056.5:355 (477)
DOI https://doi.org/10.24144/2307-3322.2025.92.5.36

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРБЕЗПЕКИ: РОЛЬ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Цимбалюк В.І.,
кандидат юридичних наук,
професор кафедри правоохоронної діяльності
та спеціальних юридичних дисциплін,
Національний університет водного господарства
та природокористування
ORCID: 0000-0003-0542-6644

Багатко А.С.,
асистент кафедри інформаційного права
та юридичної журналістики,
Національний університет водного господарства
та природокористування
ORCID: 0000-0003-4673-7406

Цимбалюк В.І., Багатко А.С. Міжнародне співробітництво у сфері кібербезпеки: роль України в умовах гібридної війни.

У статті розглянуто сучасні аспекти міжнародного співробітництва у сфері кібербезпеки. Здійснено порівняльний аналіз ключових аспектів міжнародної співпраці у сфері кібербезпеки в умовах сучасних глобальних інформаційних загроз. Актуальність дослідження зумовлена швидким розвитком інформаційних технологій, що потребує нових підходів до захисту від кіберзагроз та інформаційних втручань.

Окрему увагу приділено важливості спільних заходів для протидії дезінформації та кібернападам, підвищення ефективності глобальної безпеки через обмін інформацією, стандартизацію процесів та розвиток національних стратегій кіберзахисту. Визначено, що поглиблене розуміння кіберзагроз вимагає нових підходів до аналізу воєнно-політичної ситуації, зокрема в контексті гібридних і мережевої війн.

Проаналізовано значення міжнародної співпраці у сфері кібербезпеки, яка має сприяти не лише оперативному реагуванню на кібернапади, а й створенню єдиних стандартів безпеки. Спільні ресурси для реагування на надзвичайні ситуації, зокрема на атаки на критичну інфраструктуру, є важливим аспектом захисту глобальної кіберінфраструктури. Окрема увага приділена досвіду країн Європейського Союзу та НАТО, зокрема співпраці України з НАТО у сфері кібербезпеки.

Підкреслено необхідність подальшої інтеграції України в міжнародну співпрацю, зокрема, через участь у міжнародних форумах, удосконалення національного законодавства та розвиток систем раннього запобігання та реагування на кіберзагрози.

З'ясовано, захист від інформаційних загроз потребує комплексного підходу. Крім технічних заходів кібербезпеки, важливо розвивати медійну грамотність, підтримувати незалежне журналістське середовище та сприяти прозорості у владі.

Визначено роль України в даному процесі в умовах гібридної війни. Встановлено основні напрями співробітництва міжнародних партнерів та України у галузі кібербезпеки. Розглянуто ключові аспекти сьогоднішнього стану міжнародного співробітництва у сфері кібербезпеки. Наведено подальші перспективи розвитку міжнародного співробітництва та окреслено загрози.

Ключові слова: міжнародне співробітництво; інформаційні війни, дезінформація, міжнародна співпраця, кібербезпека; кібератака; гібридна війна; кіберзагрози, міжнародні стандарти.

Tsymbaliuk V.I., Bahatko A.S. International cooperation in the field of cybersecurity: the role of Ukraine in the context of hybrid warfare.

The article examines modern aspects of international cooperation in the field of cybersecurity. A comparative analysis of key aspects of international cooperation in the field of cybersecurity in the context of modern global information threats is carried out. The relevance of the study is due to the rapid development of information technologies, which requires new approaches to protection against cyber threats and information interventions.

Particular attention was paid to the importance of joint measures to counter disinformation and cyberattacks, increase the effectiveness of global security through information exchange, standardization of processes, and the development of national cyber defense strategies. It has been determined that a deeper understanding of cyber threats requires new approaches to analyzing the military-political situation, particularly in the context of hybrid and network wars.

The importance of international cooperation in the field of cybersecurity is analyzed, which should contribute not only to a prompt response to cyberattacks, but also to the creation of uniform security standards. Shared resources for responding to emergencies, including attacks on critical infrastructure, are an important aspect of protecting global cyber infrastructure. Special attention is paid to the experience of the European Union and NATO countries, in particular Ukraine's cooperation with NATO in the field of cybersecurity.

The need for further integration of Ukraine into international cooperation was emphasized, in particular, through participation in international forums, improvement of national legislation, and development of early prevention and response systems for cyber threats.

It has been found that protection against information threats requires a comprehensive approach. In addition to technical cybersecurity measures, it is important to develop media literacy, support an independent journalistic environment, and promote transparency in government.

The role of Ukraine in this process in the context of hybrid warfare is determined. The main areas of cooperation between international partners and Ukraine in the field of cybersecurity are established. Key aspects of the current state of international cooperation in the field of cybersecurity are considered. Further prospects for the development of international cooperation are presented and threats are outlined.

Key words: international cooperation; information warfare, disinformation, international cooperation, cybersecurity; cyberattack; hybrid warfare; cyberthreats, international standards.

Постановка проблеми. В умовах повномасштабної гібридної війни, розв'язаної росією, міжнародне співробітництво у сфері кібербезпеки набуває для України критично важливого значення. Україна, перебуваючи на передовій кібервійни, не лише отримує підтримку, а й відіграє унікальну роль, ділячись неоціненним досвідом та сприяючи формуванню глобальних підходів до кіберзахисту. Україна, бувши повноправним суб'єктом міжнародного права, активно долучається до глобальної системи кібербезпеки, яка становить ключовий елемент сучасної архітектури міжнародної безпеки.

Стрімке впровадження цифрових технологій у всі сфери життя одночасно відкриває широкі перспективи для розвитку та створює вразливі точки, які дедалі активніше використовуються як державними, так і недержавними гравцями для проведення агресивних операцій у кіберпросторі.

В умовах сучасного світу кіберзагрози давно перестали бути локальним чи регіональним явищем – вони набули транснаціональної природи, здатної паралізувати інфраструктуру, порушувати стабільність цілих секторів економіки, втручатися у політичні процеси й підривати довіру до демократичних інституцій. Особливо гостро ця проблема проявляється під час загострення традиційних конфліктів, коли кіберпростір стає однією з головних арен протистояння.

Аналіз останніх досліджень і публікацій. Питання правового регулювання кібербезпеки та розвитку міжнародного співробітництва в цій сфері отримали значну увагу серед дослідників. Особливу роль у цьому аспекті відіграють роботи українських вчених-правників, які роблять важливий внесок у вивчення цієї складної тематики.

Зокрема, В. Кононенко детально досліджував проблеми посилення кібербезпеки, захисту інформаційно-комунікаційних технологій, а також аспекти національної та міжнародної інформаційної безпеки [2].

А. Тарасюк у своїх дослідженнях аналізувала стан кібербезпеки в Україні, водночас висвітлюючи перспективи її подальшого розвитку [4]. Своєю чергою, Р. Черниш зосередив увагу на питаннях міжнародного організаційного досвіду у забезпеченні кібербезпеки [6].

Публікації зазначених авторів, разом із багатьма іншими науковими напрацюваннями, створюють цінну базу знань та вирізняються високим рівнем опрацювання матеріалу. Проте дана сфера потребує постійного оновлення досліджень і глибокого наукового аналізу у відповідь на швидку динаміку розвитку технологій та нових викликів у галузі кібербезпеки.

Метою статті є загальнотеоретична характеристика міжнародного співробітництва у сфері кібербезпеки та визначення ролі України в умовах гібридної війни.

Виклад основного матеріалу дослідження. З огляду на постійно змінюваний характер сучасних військових конфліктів, методи та підходи до аналізу військово-політичної ситуації також повинні змінюватися. Трансформація характеристик сучасних воєнних конфліктів та військово-політичних відносин вимагає адаптації аналітичних підходів, зосередження уваги на нових аспектах та елементах, що потребують детального дослідження для забезпечення об'єктивності результатів оцінки ситуації.

Сучасні військові конфлікти суттєво відрізняються від попередніх, оскільки вони набули нових характеристик та особливостей, що потребують глибокого аналізу та розуміння.

Якщо в минулому стратегія ведення війни базувалася переважно на силовому примусі та прямому військовому протистоянні між сторонами конфлікту, то сучасні військові конфлікти демонструють набагато складніші та різноманітніші характеристики. Виявлення цих нових характеристик призвело до появи таких термінів, як «проксі-війна», «гібридна війна» та «мережева війна» [6, с. 113].

Класичні війни до винаходу ядерної зброї зазвичай велися між державами або коаліціями з чіткими політичними цілями, використовуючи великі військові формування та зосереджуючись на застосуванні сили. Сучасні концепції, такі як «інформаційна війна», містять не тільки електронні та кіберкомпоненти, а й управління інформацією в комп'ютерних мережах.

Термін «інформаційні операції» розширює даний підхід, охоплюючи аналіз соціальних мереж та людський фактор, зокрема вплив на поведінку, прийняття рішень та процеси управління.

Згідно з концепцією НАТО, метою інформаційної війни є досягнення інформаційної переваги над противником, що є важливим елементом сучасної військової стратегії. Це передбачає використання інформаційних ресурсів і технологій для маніпулювання інформацією, впливу на громадську думку та дезорієнтації ворога [2, с. 245].

Досягнення інформаційної переваги не лише забезпечує стратегічну ініціативу, але й дозволяє ефективно впливати на військові, політичні та економічні процеси в конфліктних ситуаціях. Цей аспект набуває особливої важливості в умовах глобалізації та розвитку цифрових технологій, які значно розширюють можливості проведення інформаційних операцій.

Інформаційна війна, яка є одним з основних елементів сучасних військових конфліктів, проявляється в широкому спектрі форм і методів, спрямованих на маніпулювання інформацією, вплив на громадську думку та дезінформацію. Цей аспект сучасних конфліктів вирізняється своєю багатогранністю, яка включає як технологічні, так і психологічні стратегії.

Для детального розуміння та аналізу інформаційної війни корисно розглянути її основні форми та методи [4, с. 133]:

– глушіння інформації та маніпулювання нею – заглушення телевізійних, інтернет- та радіопрограм з метою порушення зв'язку та поширення дезінформації;

– логістичні збої – відключення комунікаційних мереж для обмеження доступу до інформації та ускладнення управління;

– атаки в соціальних мережах – маніпулювання або порушення роботи комунікаційних мереж противника з метою створення негативного іміджу ворога;

– саботаж фінансових ринків – електронне втручання або поширення дезінформації з метою спричинення фінансової турбулентності;

– використання дронів та роботизованих систем – розвідувальні операції для збору інформації з віддалених районів;

– управління комунікацією – контроль поширення інформації, підтримка іміджу та формування позитивного ставлення до власної партії;

– синтетичні медіа – створення фейкових новин або матеріалів для маніпулювання громадською думкою.

Ці методи підкреслюють складність сучасних конфліктів та необхідність комплексних стратегій захисту інформаційної безпеки.

Аналізуючи сучасні реалії інформаційної війни в контексті міжнародних відносин, можна зробити висновок про її критичне значення та вплив на геополітичні процеси.

На межі XXI ст. іміджевий компонент інформаційної війни став одним із найважливіших інструментів, оскільки маніпулювання інформацією про події, спотворення фактів та створення ілюзій стали ключовими факторами формування світогляду та впливу на суспільну свідомість. У цьому контексті важливо наголосити, що роль інформаційних технологій у цих процесах не лише зростає, а й постійно змінюється, вимагаючи адаптації до нових викликів та стратегій [2, с. 247].

У сучасну епоху цифрових технологій питання кібербезпеки набула критичної актуальності. Зростання кількості підключених пристроїв спричинило значне розширення спектра кіберзагроз, які створюють серйозні ризики як для національної, так і для міжнародної безпеки.

За таких умов співробітництво між державами стає ключовим фактором у захисті суверенітету та забезпеченні стійкої кібербезпеки на глобальному рівні. Україна, маючи значний досвід у протидії кіберзагрозам, активно бере участь у міжнародних ініціативах і співпраці в цій сфері. Вона є не лише об'єктом кібератак, але й провідним учасником міжнародної кіберспільноти, який сприяє розробці й впровадженню сучасних механізмів колективної безпеки [5, с. 263].

Україна впевнено інтегрується у глобальну систему безпеки, зосереджуючи свої зусилля на ключових пріоритетах, таких як розвиток міжнародного партнерства та співробітництва в кіберсфері, підтримка ініціатив, які узгоджуються з національними інтересами, а також активізація взаємодії з НАТО для зміцнення власних можливостей у забезпеченні кібербезпеки.

Важливими аспектами також є участь у заходах зі створення довірчих механізмів у кіберпросторі. В рамках міжнародних угод Україна провадить продуману політику, спрямовану на вдосконалення співпраці у сфері кібербезпеки.

З огляду на швидку цифровізацію, зростання масштабів транснаціональної кіберзлочинності та небезпечну динаміку поширення кіберзагроз у світі, надзвичайно важливим для країни стає визначення пріоритетних напрямків міжнародного співробітництва, що дозволить посилити її спроможності у боротьбі з викликами кібербезпеки [3, с. 130]. Міжнародні партнери взаємодіють з Україною у таких ключових сферах (табл. 1).

Таблиця 1

Напрями співробітництва міжнародних партнерів та України у галузі кібербезпеки

Сфера	**Характер взаємодії**
Обмін розвідувальними даними та інформацією про загрози	Регулярний та оперативний обмін даними про кібератаки, вразливості та методи ворога між українськими кіберструктурами та розвідувальними органами країн-партнерів (США, Велика Британія, країни ЄС).
Технічна допомога та передача технологій	Надання Україні сучасного програмного та апаратного забезпечення для кіберзахисту, засобів виявлення загроз, систем аналізу інцидентів та передових хмарних рішень.
Навчання та підвищення кваліфікації	Організація спільних тренінгів, навчальних програм та кібернавчань для українських фахівців з кібербезпеки, що сприяє обміну найкращими практиками.
Правова та нормативна співпраця	Взаємодія у сфері розробки міжнародних конвенцій та угод щодо боротьби з кіберзлочинністю, а також визначення відповідальності держав за агресію у кіберпросторі. Україна активно підтримує ініціативи щодо створення механізмів притягнення до відповідальності за кіберзлочини на державному рівні.
Фінансова підтримка	Надання коштів та грантів на розвиток кібербезпекової інфраструктури, закупівлю обладнання та навчання персоналу.
Взаємодія з НАТО та ЄС	Україна активно бере участь у програмах НАТО (наприклад, через Фонд цільової допомоги з кібербезпеки) та ініціативах Європейського Союзу, спрямованих на посилення кіберстійкості.

Джерело: розроблено автором

Важливим аспектом міжнародного співробітництва у сфері кібербезпеки є формування ефективної системи колективного стримування кіберзагроз, що передбачає не лише оперативне реагування на атаки, а й запровадження механізмів запобігання кіберагресії на основі міжнародного права.

В умовах гібридних війн, що дедалі частіше включають кібернетичні операції, особливої актуальності набуває розробка універсальних міжнародно-правових стандартів, які б регулювали питання відповідальності за використання кіберпростору у воєнних, інформаційних та економічних конфліктах [1, с. 592].

Станом на середину 2025 р., міжнародне співробітництво у сфері кібербезпеки характеризується зростальною інтенсивністю та адаптацією до нових, дедалі складніших викликів. Ось ключові аспекти сьогоднішнього стану міжнародного співробітництва у сфері кібербезпеки [3, с. 132]:

зростання рівня загроз та їхньої складності:

– геополітичні чинники: геополітична напруженість, зокрема війна в Україні, кардинально змінює ландшафт кібербезпеки. Держави-агресори використовують кібератаки як інструмент зовнішньої політики, шпигунства та дестабілізації. Близько 60% організацій заявляють, що геополітична напруженість вплинула на їхню стратегію кібербезпеки;

– використання штучного інтелекту (ШІ) зловмисниками: проліферація інструментів генеративного ШІ дозволяє менш досвідченим зловмисникам швидко підвищувати свої можливості, що призводить до зростання обсягів атак. Майже 47% організацій вважають досягнення супротивників, обумовлені ШІ, своєю головною проблемою;

– атаки на ланцюги постачання: уразливості в ланцюгах постачання стають головним кіберризиком для екосистем. Висхідна складність ланцюгів постачання та відсутність прозорості в рівнях безпеки постачальників роблять їх мішенню для каскадних атак;

– зростання обсягу та деструктивності атак: збільшується кількість відомих типів атак, особливо фішингових та соціальної інженерії, а також атак програм-вимагачів, які часто націлені на критичну інфраструктуру та державні послуги;

посилення співпраці та обміну інформацією:

– оперативний обмін даними: відбувається інтенсивніший обмін розвідувальними даними та інформацією про загрози між національними CERT/CSIRT командами та розвідувальними органами. Досвід України є цьому яскравим підтвердженням;

– спільні кібернавчання: регулярні міжнародні кібернавчання, як-от Cyber Coalition НАТО, стають ще більш реалістичними, відпрацьовуючи сценарії протидії складним гібридним загрозам;

– розбудова потенціалу: розвинені країни продовжують надавати технічну, фінансову та експертну допомогу країнам, які прагнуть посилити свій кіберзахист, особливо тим, хто стикається з прямими загрозами;

правова та нормативна база:

– Будапештська конвенція: залишається ключовим міжнародним документом у боротьбі з кіберзлочинністю, спрямованою на гармонізацію національних законодавств та посилення міжнародного співробітництва;

– ініціативи ООН: на глобальному рівні в ООН тривають дискусії щодо розробки універсальних норм відповідальної поведінки держав у кіберпросторі. Нова Конвенція ООН про кіберзлочинність є значним кроком до більшої глобальної співпраці, фокусуючись на технічній допомозі та розбудові потенціалу, особливо для країн, що розвиваються;

– регіональні ініціативи: ЄС посилює свою кібербезпекову стратегію (Стратегія кібербезпеки ЄС на цифрове десятиліття, Директива NIS2), що включає посилення співпраці між державами-членами та розширення кібердіалогу з третіми країнами. ENISA активно публікує рекомендації та звіти щодо імплементації NIS2.

Наразі спостерігається ще одна важлива тенденція – стрімкий розвиток кібердипломатії та активізація застосування кіберсанкцій як ефективного інструменту міжнародного тиску. Зважаючи на збільшення кількості державних кібератак, які все частіше використовуються як частина гібридної війни, міжнародна спільнота активно впроваджує дипломатичні підходи, спрямовані на запобігання та усунення загроз у цифровій галузі [4, с. 135].

Ключовим напрямом кібердипломатії є створення універсальних норм поведінки держав у кіберпросторі. Ці норми передбачають дотримання принципу невтручання у цифрові системи

інших країн, недопущення атак на цивільну інфраструктуру та забезпечення відповідності міжнародному гуманітарному праву навіть під час кіберконфліктів.

У цьому контексті Європейський Союз і НАТО активно просувають ініціативу розробки спеціального Кодексу, який визначатиме зобов'язання та відповідальність держав у кіберпросторі, сприяючи таким чином зміцненню глобальної кібербезпеки [6, с. 118].

Досвід України підштовхує міжнародні організації (ООН, ОБСЄ, НАТО, ЄС) до прискореного формування нових міжнародних норм та правил відповідальної поведінки держав у кіберпросторі. Випадки масштабних кібератак на цивільні об'єкти та критичну інфраструктуру змушують переглядати поняття кібервійни, її наслідків та механізмів притягнення до відповідальності.

Активно ділячись своїм досвідом, Україна допомагає іншим країнам, які потенційно можуть стати мішенню схожих гібридних атак, підвищувати їхню власну кіберстійкість. Це сприяє створенню глобального ланцюга кіберзахисту, де слабша ланка може становити загрозу для всієї міжнародної системи безпеки.

Для України міжнародне співробітництво у сфері кібербезпеки залишатиметься стратегічним пріоритетом. Україна залишиться унікальним джерелом знань про кібервійну. Її досвід інтегруватиметься у міжнародні доктрини та стандарти кіберзахисту.

Поглиблення співпраці з ЄС та НАТО, імплементація їхніх стандартів та участь у спільних проєктах. Це включатиме обмін інформацією, навчання та участь у багатонаціональних кіберопераціях (за їхньої появи).

Попри позитивні перспективи подальшої співпраці, деякі чинні виклики залишатимуться актуальними та потребуватимуть пошуку варіантів вирішення [1, с. 593]:

– конфлікти інтересів та відсутність довіри між певними державами продовжуватимуть гальмувати досягнення універсального консенсусу;

– глобальна нестача кадрів у кібербезпеці буде зберігатися, вимагаючи міжнародних програм навчання та розвитку;

– кіберзлочинці та ворожі держави постійно адаптують свої методи, випереджаючи регуляторні та захисні ініціативи;

– міжнародне право часто не встигає за технологічним прогресом, створюючи «сірі зони» у питанні відповідальності за кібератаки.

Перспективи розвитку міжнародного співробітництва у сфері кібербезпеки безпомилково вказують на його поглиблення та розширення. Загрози стають надто комплексними та глобальними, щоб країни могли протистояти їм поодинці.

Майбутня співпраця буде характеризуватися більшою інтеграцією між державними та приватними секторами, фокусом на технологічних інноваціях, а також постійним прагненням до розробки ефективних міжнародних норм і правил поведінки у кіберпросторі. Україна, з її унікальним досвідом протидії гібридній агресії, відіграватиме ключову роль у формуванні цього нового ландшафту глобальної кібербезпеки.

Висновки. Сучасна інформаційна війна відіграє ключову роль у світовому політичному та військовому контексті. Новітні технології масової комунікації стали ефективним інструментом впливу на громадську думку, формування інформаційного дискурсу та маніпулювання міжнародними відносинами.

Зловживання соціальними мережами та іншими медіаплатформами створює можливості для авторитарних режимів маніпулювати громадською думкою, впливати на процес ухвалення рішень і підривати довіру до демократичних інституцій. Захист від інформаційних загроз вимагає комплексного підходу.

Окрім технічних заходів у сфері кібербезпеки, важливо розвивати медіаграмотність, підтримувати незалежне журналістське середовище та сприяти прозорості в уряді.

Міжнародна співпраця в галузі кібербезпеки має вирішальне значення для боротьби з інформаційними загрозами. Спільні стандарти, обмін інформацією та співпраця між країнами можуть підвищити ефективність заходів боротьби з дезінформацією та кібератаками.

Для України особливо важливо розвивати співпрацю з НАТО та іншими міжнародними партнерами для зміцнення національної кібербезпеки та ефективної боротьби із сучасними загрозами, що є важливим кроком на шляху до євроатлантичної інтеграції та покращення міжнародного іміджу країни.

У контексті гібридної війни, Україна є не просто отримувачем допомоги, а стратегічним партнером та джерелом унікального бойового досвіду у сфері кібербезпеки. Її роль як кіберщита де-

мократичного світу є беззаперечною, адже, витримуючи удари, Україна генерує знання та практики, які стають основою для формування глобальних стратегій кіберзахисту. Це партнерство не тільки допомагає Україні вистояти, але й сприяє побудові більш безпечного та стійкого глобального кіберпростору для всіх країн.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Вареник О.С. Тенденції міжнародного співробітництва у сфері кібербезпеки. *Юридичний науковий електронний журнал*. 2024. №11. С. 591–593. DOI https://doi.org/10.32782/2524-0374/2024-11/139.
2. Кононенко В.П. Інформаційна безпека як стан. *Науковий вісник Ужгородського університету*. 2023. Т. 2. Вип. 76. С. 244–250. DOI https://doi.org/10.24144/2307-3322.2022.76.2.39.
3. Поляков О.М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право.* 2021. № 2(37). С. 129–138. URL: file:///C:/Users/Client/Downloads/238348%D0%A2%D0%B5% D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96546543-1-10-20210804.pdf.
4. Тарасюк А.В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник*. 2020. Вип. 1. С. 133–136. DOI https://doi.org/10.32837/pyuv.v0i1(30).532.
5. Тєтєвін М.С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. Н*ауковий вісник Ужгородського Національного Університету*. 2024. Вип. 82. Ч. 3. С. 263–266. DOI https://doi.org/10.24144/2307-3322.2024.82.3.41.
6. Черниш Р.В. Міжнародний організаційний досвід у сфері забезпечення кібербезпеки. *Вісник кримінального правосуддя*. 2023. № 3-4 С. 112–121. DOI https://doi.org/10.17721/2413-5372.2021.3-4/112-121.