Вісник Національного університету "Львівська політехніка".
Серія "Проблеми економіки та управління"

№ 2(6), 2020

УДК 336
JEL Classification Code O 33, D 89

О. Є. Шандрівська[1], Н. В. Шинкаренко[2]
[1] Національний університет "Львівська політехніка",
кафедра маркетингу і логістики,
[2] Національний технічний університет "Дніпровська політехніка",
кафедра маркетингу

ПРИКЛАДНА ОЦІНКА РИЗИКІВ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ПРОЦЕСІВ У КІБЕРПРОСТОРІ

http://doi.org/10.23939/semi2020.02.094

Здійснено дослідження безпеки соціально-економічних процесів у віртуальному просторі. З'ясовано вплив ключових тенденцій сучасності на формування превентивних та адаптивних механізмів забезпечення інформаційної та кібернетичної безпеки підприємств. До основних зараховано глобалізацію, інформатизацію та індивідуалізацію потреб споживачів, медіатизацію суспільних явищ, детериторіалізацію та універсалізацію соціальних явищ. Викладено авторське бачення моделі забезпечення безпеки в інформаційній віртуальній сфері та співвідношення домінуючих ризиків, загроз та вразливостей соціально-економічного простору України на прикладі ідентифікації та оцінювання ризиків у кіберпросторі в частині безпекового зрізу інформаційних та фінансових потоків.

Ключові слова: глобалізація; інформатизація; ризики; небезпеки; загрози; кіберпростір; інформаційна безпека; забезпечення інформаційної безпеки.

Постановка проблеми

Світова системна криза, посилена фінасовими кризами, техногенними катастрофами, пандемією коронавірусної інфекції тощо, спричиняє глибокі зміни у світовій економіці та підтверджує неминучість виникнення потреби переходу від економічного зростання, яке в термінах сучасної економіки означає збільшення виробництва і споживання товарів і послуг за експонентою, у недалекому майбутньому до простого відтворення, оптимального ступеня споживання, нульового циклу виробництва, відмови від прогресу матеріального добробуту на користь соціалізації та духовного розвитку. Поряд із віртуалізацією соціальних та бізнес-взаємодій глобального суспільства репрезентовано тееоретичні моделі глобалізації (моделі глобальної системи (Е. Гідденс і Л. Склер, 1991) [22], глобальної соціальності (Р. Робертсон, У. Бек, Г. Терборн, 1992) [21] та детериторіалізації соціального протору (А. Аппадураї, М. Уотерс, 1996) [17], які є відображенням суспільних змін, нині видозмінюються та набувають іншого якісного змісту в зв'язку із віртуалізацією інформаційного простору. Експансія соціально-економічних процесів у нові (віртуальні) форми просторовості, задекларовані як процеси постглобалізації/гіперглобалізації/деглобалізації (М. Уотерс), є свідченням радикальних змін світового устрою та глобального безпекового простору. Питання безпеки соціально-економічних процесів та її забезпечення у віртуальному прострі загострюються у зв'язку із необхідністю розкриття потенціалу, який формують можливості застосування інформаційно-комунікаційних технологій в інформаційному просторі та ідентифікації, моніторингу, контролювання та нейтралізації потенційних та реальних загроз, небезпек та ризиків інформаційних впливів у віртуальному просторі.

Аналіз останніх публікацій

Дослідження проблем безпеки соціально-економічних процесів та забезпечення у кіберпросторі дотичне до багатьох суспільних та економічних процесів та явищ, а відтак вимагає аналізування таких понять, як "глобалізація" та "інформатизація суспільства", "кіберпростір" та "гібридна агресія", небезпеки, загрози та ризики економічних процесів тощо. У працях "Що таке глобалізація" (1997), "Космополітичне бачення" (2006), "Суспільство ризику" (2009) У. Бека [1] досліджено чинники глобалізації, зумовлені, домінантно, ризиками, з якими стикається суспільство. На думку науковця, у міру поглиблення глобалізаційних процесів ризики починають набувати універсального характеру, а стрімкий технологічний процес зумовлює постійне застосування новітніх інформаційних технологій. У міру модернізації індустріальне суспільство перетворюється на суспільство ризику, основне завдання якого – необхідність уберегтися від ризиків та запобігти їм.

Внеском українських вчених у теорію глобалістики, інформаційних впливів та операцій, вирішення проблем міжнародної безпеки стали праці Б. Гуменюка [4], О. Білоруса [6], В. Горбуліна [7] та ін.

Деякі науковці досліджують різні аспекти поняття "безпека" та пов'язують його із поняттями "ризик", "вразливість", "загроза", "небезпека", "конфліктність" тощо [2, с. 9; 3; 5; 8].

У праці [20, с. 16] під ризиком розуміють сукупність властивостей, спрямованих у три виміри – ризик як небезпека, ризик як невизначеність і ризик як можливість (шанс). Автори праці [9] стверджують, що ризик пов'язаний із подоланням невизначеності, випадковості та конфліктності в ситуації неминучого вибору і відображає ступінь досягнення очікуваного результату. У праці [12, с. 107] досліджено загрози, які виникають на стадії переходу небезпек із пасивної форми в активну, коли потенційні можливості негативного впливу трансформуються у конкретні наміри чіткого адресного спрямування.

Постановка цілей

Разом із тим, специфіку політичної, соціальної та економічної кон'юнктури інформаційного ринку, притаманної Україні в умовах поширення на її теренах тренду інформатизації суспільства та технологій, що зумовлює глобалізація, досліджено недостатньо.

Цілі дослідження: проаналізувати підходи до ідентифікації безпеки соціально-економічних процесів у віртуальному просторі; ідентифікувати вплив ключових тенденцій сучасності на формування превентивних та адаптивних механізмів забезпечення інформаційної та кібернетичної безпеки підприємств; висвітлити авторське бачення моделі забезпечення безпеки в інформаційній віртуальній сфері та оцінити співвідношення домінантних ризиків, загроз та вразливостей у частині безпеки інформаційних та фінансових потоків у кіберпросторі.

Виклад основного матеріалу

Ключові тенденції сучасності – глобалізація, інформатизація та індивідуалізація потреб, які зумовлюють розвиток перспективних інформаційно-комунікаційних систем та технологій, особливо в умовах активної фази гібридної війни, на порядок денний ставлять серед іншого необхідність формування превентивних та адаптивних механізмів забезпечення інформаційної та кібернетичної безпеки підприємств, держави та громадянського суспільства. Активне використання інформаційного, зокрема кіберпростору, з боку різних груп стейкхолдерів розглядають не тільки як прогресивний та результативний засіб ведення конкурентної та політичної боротьби на світовій арені у вимірах "простір–час–інформація", але і як агресивне та потужне джерело формування глобальних загроз та небезпек соціальних взаємодій.

Розвиток технологій побудови мереж, використання штучного інтелекту, поява хмарних і туманних технологій, нарощування потужностей баз даних і баз знань трансформувала інформаційний (домінантно кіберпростір) із засобу комунікації в активного агента впливу не тільки на суспільні та політичні процеси загалом, а й на окремі особистості, досягаючи індивідуалізованого впливу на них. За таких обставин кіберпростір перетворюється на специфічне соціальне, еконо-

мічне, політичне та культурне середовище, використання інструментів якого здатне кардинально змінити параметри соціальних взаємодій окремих індивідуумів та поглибити соціальні суперечності окремих соціальних груп, домінантно завдяки взаємопроникненню у реальний простір у загальному потоці соціальних взаємодій.

Можна констатувати, що формуються нові тенденції, зумовлені розвитком інформаційного простору та подальшої глобалізації, передусім – медіатизація суспільних явищ, внаслідок чого суспільні інститути та явища ідентифікуються як комплекс символічних відображень у свідомості громадян, а відтак стають учасниками та відображенням символічних, гібридних, асиметричних та інших медіапротистоянь у конкурентній та політичний боротьбі. Крім того, соціальні процеси та протистояння, завдяки віртуалізації, втрачають локальну (територіальну) прив'язку, а відтак започатковують тенденції детериторіалізації та універсалізації соціальних явищ, нівелювання автентичності окремих культур, універсалізації та стандартизації загроз та низки інших чинників. Окрім цього, розвиток процесів віртуалізації супроводжується поглибленням ідентифікації присутності суб'єктів у кіберпросторі (в частині посилення електронної ідентифікації споживачів: електронний підпис, електронні звернення, MobileID, BankID, ID-картка тощо), появою нових суб'єктів інформаційного ринку (провайдерів послуг, неурядових організацій, страхових компаній, наукових установ тощо), розвитком ідей свободи в інтернеті та інформаційної свідомості, формуванням інформаційно-комунікаційних компетентностей споживачів із метою нівелювання чи уникнення кіберзагроз, які надчасто є джерелом та супроводом класичних загроз (терористичних атак, міграційних потоків, антиглобалізаційного руху, екологічної, фінансової чи громадянської криз тощо). Отже, глобальний характер інформаційного, зокрема кіберпростору, спроможний підвищити рівень ризику, здійснюючи вплив на суб'єктів державного та приватного секторів.

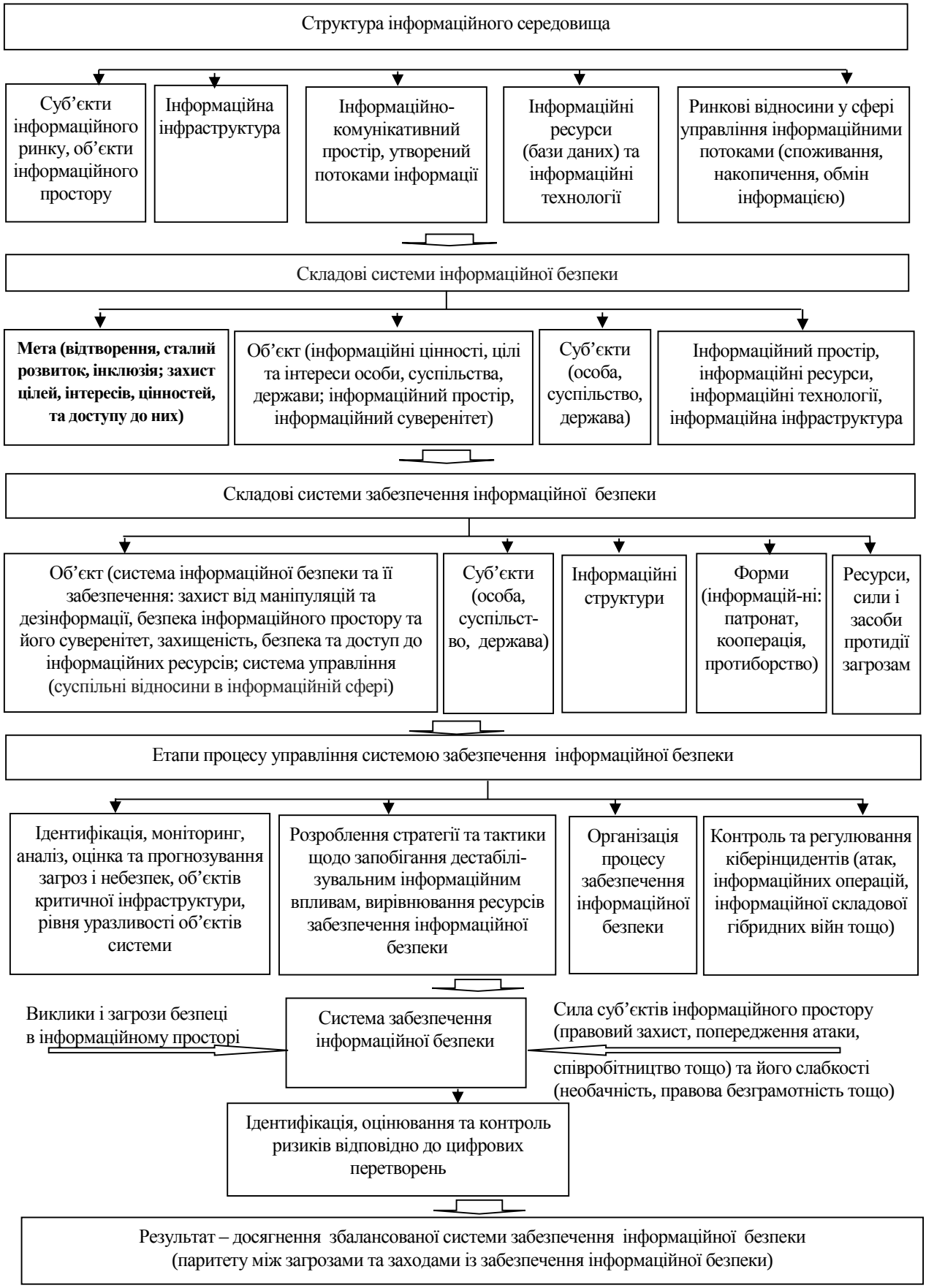
Науковий інтерес до проблематики соціально-економічної складової безпеки та її забезпечення в інформаційній сфері є втіленням змін, які відбуваються в економіці, з огляду на подальшу глобалізацію, технологічну революцію та цифровізацію суспільства, з одного боку, та зростанням невизначеності, нерівноважності та нелінійності процесів у економіці під впливом інновацій, інститутів, асиметрії інформації тощо – з другого, які, співіснуючи разом, стають драйверами розвитку продуктивних сил.

Зазначене актуалізує необхідність формування моделі забезпечення безпеки в інформаційній віртуальній сфері, до складу якої входить ідентифікація та управління ризиками, загрозами та вразливостями інформаційного простору, що з'являються унаслідок складностей моніторингу та контролювання тенденцій і процесів інформаційно-технологічного та соціально-економічного розвитку, займає важливе місце і спирається на сформовану авторами концептуальну схему ідентифікації системи забезпечення інформаційної безпеки (див. рисунок).

У системі забезпечення інформаційної безпеки важливе місце займає грунтовне дослідження питань ідентифікації, оцінювання та контролю ризиків відповідно до цифрових перетворень. У роботі запропоновано таку деталізацію оцінювання ризиків функціонування досліджуваного об'єкта: ідентифікація ризику → описання загроз, які він породжує → виявлення вразливих сегментів ринку → аналіз та оцінювання рівня ймовірності настання ризику → аналіз та оцінювання рівня наслідків прояву ризику → визначення бальної оцінки загального рівня ризику → пропонування пом'якшувальних заходів щодо нівелювання ризиків середовища розвитку об'єкта дослідження → ідентифікація чистого ризику.

Автори дотримуються підходу, запропонованого Європейським страховим комітетом (Європейським страхуванням), згідно із яким чистий ризик означає потенційну можливість зазнати збитку. Тобто у результаті слід вибрати одну із альтернатив – зазнавання збитку або його відсутність. На практиці, зазвичай, страхуються від чистого ризику.

У запропонованій моделі окреслено структуру інформаційного середовища, виділено складові системи інформаційної безпеки, які можуть бути ідентифіковані на рівні особи, суспільства чи держави, та в її складі виділено елементи системи забезпечення інформаційної безпеки. З погляду менеджменту виокремлено етапи процесу управління системою забезпечення інформаційної безпеки.



Концептуальна схема ідентифікації системи забезпечення інформаційної безпеки
Джерело: власна розробка авторів.

Щодо окремої складової процесу управління системою забезпечення інформаційної безпеки – аналізу системи забезпечення інформаційної безпеки – доцільне застосування, наприклад, такого інструменту, як SWOT-аналіз викликів і загроз безпеці в інформаційному просторі та можливостей щодо забезпечення безпеки цього простору (що розглядають як елементи зовнішнього середовища) та сили/слабкості суб'єктів інформаційного простору (як елементів внутрішнього середовища). Завдяки цьому уможливлюються ідентифікація, оцінювання та контроль ризиків відповідно до цифрових перетворень у суспільстві. Як результат окреслених дій очікується формування збалансованої системи інформаційної безпеки із урахуванням заходів щодо захищеності від інформаційних впливів, захисту даних, захисту інформаційних прав, відкритий доступ до інформації тощо, а також здатність до вдосконалення та розвитку, що є відображенням циклічності процесу забезпечення безпеки інформаційного простору.

У таблиці подано авторське бачення співвідношення ризиків, загроз та вразливостей, які домінують, на прикладі соціально-економічного простору України (див. таблицю).

Послідовність ідентифікації та оцінювання ризиків у кіберпросторі: безпековий зріз інформаційних та фінансових потоків

Послідовність ідентифікації ризику	Зміст
1	2
Ризик 1	Безпека систем, процесів та технологій, дезінформація, асиметрія інформації
Загроза	Підвищення рівня інформаційних загроз (тероризм, екстремізм, авторитарний режим, міграційні потоки, кібертероризм (інформаційні спецоперації, хакерські атаки, бойове використання соцмереж та інтернет-сервісів), цифрова нерівність, цифрова недбалість, втрата приватності та чистоти інформації тощо), зумовлене цифровізацією економіки
Вразливість	Порушення стійкості економічних систем, яке сформувалось через трансформацію значної кількості галузей промисловості та різке зниження затребуваності працівників одних галузей та зростання потреб у висококваліфікованих працівниках у інших. Крім того, формування нових процесів спричинило дематеріалізацію виробництва завдяки зростанню частки знань у створеній вартості та посилило міжгалузеву та внутрішньогалузеву конкуренцію серед груп компаній, які застосовують різні торговельні та інвестиційні стратегії на засадах цифровізації. Крім трансформації сфер виробництва та управління, нові вимоги постали перед системами охорони здоров'я, освіти, транспорту, зв'язку, безпеки тощо. Для підвищення суспільної довіри та відчуття населенням захищеності у цифровому середовищі потрібен перегляд глобальних норм, стандартів, політик та угод. Стійкість галузі ІКТ залежить від стану глобальної економіки, фінансових криз та пандемій, на які сектор реагує із певним часовим лагом. Настання пандемії (2019) у короткостроковому періоді суттєво не позначилось на рівні сервісів, які надавали у дистанційному режимі. Однак глобальні кризи з певним часовим лагом позначаться на проєктах компаній, передусім дрібних
Рівень ймовірності настання ризику (3 б.)	Галузь інформаційно-комунікаційних технологій (ІКТ), яка посідає чільне місце у генерації потенціалу цифрової економіки, демонструє швидкі темпи розвитку в Україні та займає третє місце за обсягом експорту послуг із часткою 20 % у структурі українського сервісного експорту. Експорт ІТ-послуг у 2019 р. становив 4,17 млрд дол США, а обсяг сплачених податків від ІТ-експорту – 16,7 млрд грн. Одночасно із розвитком галузі ІКТ підвищується небезпека систем, процесів та технологій [11]. Структура галузі (ІКТ) в країні фрагментована: є потужні суб'єкти ринку (асоціація IT Ukraine, 50 компаній, що генерують близько 50 % виручки галузі; EPAM, 7550 прац.; SoftServe, 5840 прац.;GlobalLogic, 4305 ос.; Luxoft, 3597 прац.), які працюють із великими клієнтами і складними end-to-end-рішеннями у власному портфоліо; середні компанії із обмеженою кількістю клієнтів; компанії із класичною аутсорсинговою та аутстафінговою моделями. **Можливість дистанційного режиму роботи (*remote work*), гнучкість оптимізації робочих процесів, здатність формувати нішові рішення, притаманні ІТ-індустрії, дають змогу підтримувати ефективність процесів у галузі та забезпечувати захист і безпеку проєктів.**

Продовження таблиці

1	2
	Причинами та умовами найбільшого сприяння проявам ризику є все те, що сприяє порушенню стійкості системи, за якого знижується рівень контролю, а відтак формуються сприятливі обставини для хакерських атак: фінансова та економічна кризи, дефолт, зростання курсів іноземних валют, пандемія тощо, прояви гібридної агресії, дія бізнес-стейкхолдерів, політичних та інших стейхолдерів. Наприклад, атаки перед проведенням аудиту державних реєстрів; перед президентськими та парламентськими виборами; з метою проведення референдуму тощо). Висока залежність інформаційної безпеки від воєнно-політичного середовища в країні підвищує рівень ймовірності настання ризику
Рівень наслідків прояву ризику (3 б.)	Глобалізація та інформатизація суспільства, поряд із поширенням баз даних, утворюють джерела виникнення ризиків кібератак, маніпулювання, втрат (комерційних, технологічних) та спотворення інформації. Наслідки порушення безпеки систем можуть відобразитися у будь-якій галузі, яка упроваджує цифровізацію процесів. Ризики і загрози інформаційної безпеки є хаотичними, множинними та непередбачуваними. Застосування інтернету, який можуть використовувати як вагоме середовище маніпуляцій суспільною свідомістю, домінантно у сегменті користувачів нового покоління Z, супроводжується труднощами розпізнавання, інтерпретації, запобігання дезінформаційному впливу та його подолання. Поряд із цим, дезінформація може бути спрямована на формування змішаних та гібридних норм поведінки громадянського суспільства. Кібератаки можуть поширюватися не тільки на організації-споживачів (об'єкти критичної інфраструктури, держпідприємства тощо), а і на кінцевих споживачів (лідерів громадянських партій та держав, "лідерів думок" тощо). В Україні персональні дані споживачів розміщені у 300 різних реєстрах, єдиного центру їх акумулювання немає. Поряд із цим у хакерських мережах можна віднайти бази персональних даних з найбільших оцифрованих державних і комерційних реєстрів за понад 20 років. У таких ресурсів із недоведеною безпекою неконтрольований трафік, невідомі клієнтам використовувані масиви, є приховані та інші функції
Загальний рівень ризику	9 б.
Складові та рівень ефективності пом'якшувальних заходів (2 б.)	Упорядкування суспільних інформаційних відносин потребує створення єдиної системи захисту даних, основаної на: · прогресивних принципах захисту даних: забезпечення контролю процесів оброблення даних, превентивність щодо ідентифікації, недопущення чи усунення шкідливого інформаційного впливу; оптимальне співвідношення "права доступу та захисту даних", захищеність від несанкціонованого витоку та оброблення даних тощо, а за мету поставлено підтримання оптимального балансу прав людини, суспільства та держави; · завданнях щодо забезпечення безпеки від інформаційних впливів, захищеності інформаційної інфраструктури, інформаційних прав, відритого доступу до інформації, публічності відкритої інформації тощо; · організаційно-правовому механізмі захисту даних, основаному на необхідності впорядкування відповідальності суб'єктів інформаційного ринку, державного контролю за допомогою ліцензування діяльності щодо збирання, передавання, оброблення, зберігання та інших маніпуляцій із даними, розроблення стандартів маніпуляцій із даними та сертифікування інформаційних систем з їх оброблення; · побудові реєстрів баз даних, а також реєструванні володільців/розпорядників даних, третіх осіб, яким передано дані для подальшої маніпуляції; · формування незалежного координаційного центру зі здійснення державної політики в частині нагляду за дотриманням вимог щодо захисту даних тощо
Рівень чистого ризику	6 б.
Ризик 2	Висока чутливість фінансових потоків щодо процесів реалізації шокових макроекономічних явищ (зокрема без істотної девальвації валют на тлі пандемії): у центрі безпека фінансових потоків
Загроза	Глобальні фінансові кризи в умовах розвитку фінансових технологій (на тлі поширення цифровізації), що є наслідками мегатрендів глобалізації, інформатизації та індивідуалізації споживчих потреб, посилені дією пандемій

Продовження таблиці

1	2
Вразливість	Конфіденційність та кібербезпека, разом із питаннями керування інтернетом (безпека використання цифрової валюти, захист персональних даних споживачів; інші процеси та послуги в онлайн-просторі), якими можна скористатись для здійснення платіжного шахрайства та кібератак (відмивання грошей, фінансування тероризму, витоки персональних даних тощо). Наприклад, різновиди цифрової валюти: цифрова валюта центрального банку (потенційно *е*-гривня в Україні), цифрова валюта, віртуальна валюта, криптовалюта розширюють структуру фінансових потоків, які формуються за допомогою віртуальних валют. Також розширення асортименту послуг банками в системі онлайн (P2P-перекази, операції з депозитами, обмін валюти, онлайн-шопінг. онлайн-кредити, здебільшого споживчі тощо) стимулюють споживачів користуватися безготівковими розрахунками та іншими сервісами онлайн, що розширює проведення трансакцій у інтернет-мережах. Разом із тим упроваджуються нові напрями застосування шахрайських схем (для прикладу, в банківській сфері: банкоматне шахрайство; махінації в торговельно-сервісних мережах; махінації в онлайн-просторі; махінації у системах дистанційного банківського обслуговування; у соціальних мережах: маніпуляція; зловмисне програмне забезпечення; мережеві та комп'ютерні атаки; дезінформування; фармінг; фішинг), що потребує забезпечення більшої прозорості фінансових потоків
Рівень ймовірності настання ризику[1] (3 б.)	Причинами та умовами найбільшого сприяння проявам ризику є: розвиток цифрової економіки, розвиток фінансових технологій, зміна споживчих переваг щодо підвищення мобільності, зручності, швидкості, здешевлення вартості послуг і візуалізації інформації
Рівень наслідків прояву ризику (3 б.)	Розвиток цифрової економіки призвів до загострення ризиків, що супроводжують фінансову діяльнісь у кіберпросторі: розвитку кіберзлочинності, розширення банківських операцій, започаткування нових видів безготівкових розрахунків, упровадження криптовалют, появи електронних кредитних платформ тощо, що вимагає формування відповідної цифрової інформаційно-комунікативної інфраструктури банківської системи. Шокові макроекономічні явища, спричинені, наприклад, коронавірусом, фінансовими кризами тощо, спричиняють спад економічної активності та кон'юнктури ринку електронної торгівлі за рахунок зменшення обсягів операцій купівлі-продажу в інтернет-просторі, спричиняючи зменшення попиту споживачів та зниження доходів суб'єктів інтернет-простору. Наприклад, у споживчому секторі спостерігається зменшення обсягів операцій населення із банківськими рахунками, зокрема зарахування заробітної плати, отримання споживчих кредитів тощо, а відтак доходів банків від комісії за безготівкові розрахунки тощо [10]
Загальний рівень ризику	9 б.
Складові та рівень ефективності пом'якшувальних заходів (3 б.)	Цифровізація спричинила активне перенесення фінансових операцій в онлайн-формат. Здійснюється поетапна відмова від готівкових транзакцій, започатковуються нові види платежів і переказів, запроваджуються мобільні додатки, безконтактні платежі, онлайн-кредитування, електронні гроші тощо. Розвиток біткоїн-бізнесу в Україні, зокрема, засвідчує її належність до десятки лідерів країн світу за кількістю біткоінодів у всесвітній біткоін-мережі, отримання доходів українськими біткоін-бізнесменами близько – 15 % від усіх коштів за майнінг за рахунок надання обчислювальних потужностей під біткоін, високий рівень підготовки українських ІТ-спеціалістів. Автоматизація процесів та процедур із використанням великих даних та методів машинного навчання забезпечує значний потенціал підвищення ефективності та зменшення витрат на мережу. Одночасне посилення кіберзагроз, які визнають одним із найбільших джерел системного ризику, вимагає удосконалення систем захисту інформації та виявлення шахрайства, а також підвищення прозорості фінансових потоків. Для цього необхідна підтримка Групи з розроблення фінансових заходів боротьби із відмиванням грошей (FATF) та Держфінмоніторингу щодо ризик-орієнтованого моніторингу діяльності цифрових валютних бірж і ліцензування операцій у віртуальних валютах

[1] Ймовірність настання та наслідків прояву ризику запропоновано встановити на рівні: 1 бал – низький, 2 бали –середній, 3 бали – високий.

Продовження таблиці

1	2
Рівень чистого ризику	9 б.
Ризик 3	Технічна, технологічна, особиста тощо уразливість в інформаційній сфері, спричинена зростанням кіберзлочинності: у центрі уваги безпека інформаційних потоків
Загроза	Нестабільна безпекова ситуація в інформаційній сфері, пандемія
Вразливість	Кіберпростір, зокрема персональні дані, економічна стабільність, інформаційна безпека, національна безпека
Рівень ймовірності настання ризику[2] (3 б.)	Причини та умови найбільшого сприяння проявам ризику такі: нестабільна соціально-політична й економічна ситуація в Україні, що перебуває в стані економічної та політичної трансформації; поширення гібридної агресії з боку РФ проти України; розвиток цифрових технологій (ураховуючи великі дані й аналітику, штучний інтелект та автоматизацію), викликаний Четвертою індустріальною революцією; недосконаліть законодавства у кібернетичній сфері; посилення зв'язку між кіберзлочинністю, що набула ознак бізнесу, та організованою злочинністю. Крім того, цифрова трансформація в умовах пандемії прискорила зростання частки безготівкових операцій у різних секторах економіки та операцій, здійснюваних населенням. Запровадження зручних дистанційних сервісів є вагомою конкурентною перевагою та сприяє зниженню операційних витрат, однак підвищує ризики кібершахрайства
Рівень наслідків прояву ризику (3 б.)	**Істотне зростання кількості облікованих кіберзлочинів (2005 р. – 39 од.; 2010 р. – 190 од.; 2015 р. – 598 од.; 2019 р. – 4263 од.), темпи зростання у 2019–2005 рр. – 109,31, які радше характеризують статистику розпізнавання злочинів, а не їх ранньої ідентифікації. Найпоширенішими видами кіберзлочинів є: камкординг; кардшаринг; фальшиві інтернет-аукціони; розсилання листів (спам); азартні онлайн-ігри на гроші; створення вірусів; крадіжка персональних даних та особистої інформації; сексуальна експлуатація дітей в інтернеті; наскрізні чинники злочинів (зловживання криптовалютами, відмивання брудних коштів, отриманих злочинним шляхом, компрометація корпоративної електронної пошти) тощо. Високий рівень зв'язку кібер- та організованої злочинності на теренах України та поза нею призвів до позиціонування України на міжнародній арені як вагомого центра хакерства, поряд із Бразилією, Китаєм та меншою мірою – Індією, яке набуває транснаціональних ознак і становить загрозу національній та міжнародній безпеці. У 2018 р. в Україні нейтралізовано поширення чотирьох масових кібератак, припинено діяльність понад 40 піратських сайтів. У частині міжнародної співпраці викрито вісім транснаціональних хакерських угруповань та взято участь у понад 30 міжнародних операціях.** Поширення кіберзлочинності є наслідком розвитку цифрової економіки, яку характеризують такі індекси та показники у міжнародних рейтингах: - *Global Innovation Index* (GII), глобальний індекс інновацій, за яким Україна в 2019 р. посіла 47-ме місце серед 129 економік, увійшовши до ТОП-3 країн економічної групи *lower-middle income* (у 2018 р. – 43-тє місце); - *ICT Development Index* (ITU), індекс розвитку інформаційно-комунікаційних технологій, за яким у 2017 р. Україна посіла 79-те місце [18]; - *Global Competitiveness Index* (GCI), індекс глобальної конкурентоспроможності, згідно з яким Україна в 2019 р. зайняла 85-те місце зі 141 країни (у 2018 р. – 83-тє місце). Регрес зафіксовано, зокрема, у сфері впровадження ІКТ – із 77-го на 78-ме місце, макроекономічної стабільності – із 131-го на 133-тє місце та інноваційних можливостей – із 58-го на 60-те місце [13]; - ***E-Government Development Index*, рейтинг *e*-урядування, згідно із яким Україна зайняла 82-ге місце щодо розвитку електронного урядування [14; 15];** - ***Open Data Barometer*, рейтинг у сфері відкритих даних, за яким у 2018 р. Україна посіла 17-те місце та друге місце – за темпами розвитку за чотири роки [16];** - ***Global Open Data Index*, рейтинг відкритих даних, за яким Україна посіла 31-ше місце у 2018 р. [19]**

[2] Рівень ризику запропоновано встановити як: 1–3 бали – низький, 4–6 балів – середній, 7–9 балів – високий.

Закінчення таблиці

1	2
Загальний рівень ризику	9 б.
Складові та рівень ефективності пом'якшувальних заходів (2 б.)	**Упорядкування процесів, які відбуваються у сферах цифрових технологій, потребує (потенційно): визнання цифрової складової невід'ємним компонентом процесу формування економічної вартості; інституціональне формування на основі телекомунікаційної сфери ринків (цифрового ринку, ринку персональних даних тощо) із наданням відповідних кодів видів економічної діяльності за КВЕД; формування відкритої конкуренції (зокрема упорядкування надмірної концентрації на ринку онлайн-платформ завдяки удосконаленню нормативного регулювання тощо); формування політики безпеки (ураховуючи положення захисту персональних даних, конфіденційності та кібербезпеки і керуванням інтернетом тощо); розроблення проактивних заходів для створення нових робочих місць (зокрема підвищенням професійної підготовки, переорієнтацією ринку праці на високотехнологічні галузі тощо); удосконалення заходів щодо соціального захисту населення (підвищення цифрової культури вразливих груп клієнтів, насамперед старшого покоління тощо)**
Рівень чистого ризику	6 б.

Джерело: власна розробка автора.

У таблиці проаналізовано домінантні ризики зовнішнього і внутрішнього середовищ для безпеки інформаційного віртуального простору України. До таких зараховано безпеку систем, процесів та технологій, дезінформацію та асиметрію інформації; високу чутливість фінансових потоків щодо процесів реалізації шокових макроекономічних явищ (зокрема без істотної девальвації валют на тлі пандемії) в частині безпеки фінансових потоків; підвищення технічної, технологічної та особистої уразливості в інформаційній сфері через зростання кіберзлочинності в частині безпеки інформаційних потоків.

Висновки

1. Інформатизація суспільства поряд із загальновизнаними перевагами загострила питання вразливості суспільних процесів; викликала напруження та дезорганізацію державного управління, стала чинником сприяння виникненню техногенних аварій, гібридних конфліктів тощо, а відтак актуалізувала необхідність ідентифікації, оцінювання та контролю загроз інформаційній безпеці. Розгортання гібридної війни РФ проти України декларується як домінантний чинник розвитку кібершпигунства в частині порушення бізнес-процесів та політично мотивованих кібератак у загальній структурі кіберзлочинності в Україні (на противагу світовим трендам у цій царині, за якими цілі отримання матеріальних вигод ідентифікуються в чотири рази рідше ніж в інших країнах (за даними PwC)).

2. Науковий інтерес до проблематики соціально-економічної складової безпеки в інформаційній сфері пояснюється необхідністю формування моделі забезпечення безпеки в інформаційній віртуальній сфері, до складу якої входять ідентифікація та управління ризиками, загрозами та вразливостями інформаційного простору, що з'являються внаслідок складностей моніторингу та контролювання тенденцій і процесів інформаційно-технологічного та соціально-економічного розвитку, займає вагоме місце і спирається на концептуальну схему ідентифікації системи забезпечення інформаційної безпеки, яку сформували автори.

3. Дотримуючись загальновизнаного означення загроз інформаційній безпеці як сукупності умов і чинників, що створюють небезпеку для життєво важливих інтересів особистості, суспільства і держави в інформаційній сфері та складаються із загроз безпеці інформації та інформаційній

інфраструктурі, безпеці суб'єктам інформаційного середовища та безпеці соціальним зв'язкам між ними, у статті з'ясовано домінантні ризики зовнішнього і внутрішнього середовищ для безпеки інформаційного віртуального простору України. До таких зараховано недостатню безпеку систем, процесів та технологій, дезінформацію та асиметрію інформації; високу чутливість фінансових потоків щодо процесів реалізації шокових макроекономічних явищ (зокрема без істотної девальвації валют на тлі пандемії) в частині безпеки фінансових потоків; підвищення технічної, технологічної та особистої уразливості в інформаційній сфері через зростання кіберзлочинності в частині безпеки інформаційних потоків.

Перспективи подальших досліджень

Надалі наукові праці авторів стосуватимуться поглиблення проблематики дослідження впливу цифровізації економіки на інші соціально-економічні ризики в частині забезпечення безпеки соціально-економічних явищ.

1. Бек У. (2000). Общество риска. На пути к другому модерну. М.: Прогрес-Традиция. Available at: http://royallib.com/book/bek_ulrih/obshchestvo_riska_na_puti_k_drugomu_modernu.html.

2. Верченко П. І. (2006). Багатокритеріальність і динаміка економічного ризику (моделі та методи). К.: КНЕУ, 272 с.

3. Вітлінський В. В., Наконечний С. І. (1996). Ризик у менеджменті. К.: ТОВ "Борисфен-М", 336 с.

4. Глобалізація і сучасний міжнародний процес (2009). За заг ред. Б. Гуменюка, С. Шергіна. К.: Університет "Україна", С. 42–45.

5. Івченко І. Ю. (2004). Економічний ризики: навч. посіб. К.: Центр навчальної літератури, 304 с., С. 21.

6. Інтеграція України в глобальний соціально-економічний простір (2019). [О. Г. Білорус та ін.]; НАН України [та ін.]. К.: КНЕУ, 287 с.

7. Горбулін В. П., Додонов О. Г., Ланде Д. В. (2009). Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 164 с.

8. Машина Н. І. (2003). Економічний ризик і методи його вимірювання: навч. посіб. для студ. ВУЗів. К.: Центр навчальної літератури, 188 с.

9. Мур А., Хиарнден К. (1998). Руководство по безопасности бизнеса: практ. пособ. по управлению рисками. М.: Филинъ, 328 с.

10. Національний банк України. Звіт про фінансову стабільність. Червень 2020 року. Available at: https://bank.gov.ua/admin_uploads/article/FSR_2020-H1.pdf?v=4.

11. Некрасов В. ІТ-галузь України проти "коронакризи": скорочень персоналу та урізання зарплат не буде, поки що. *Економічна правда*. Available at: https://www.epravda.com.ua/publications/2020/04/6/658983/.

12. Семенютіна Т. В. (2012) Економічні ризики, небезпеки, загрози: сутність та взаємозв'язок. Економічний простір: зб. наук. праць. Дніпропетровськ: ПДАБА, № 68, С. 106–113.

13. Україна опустилася на 85-те місце в щорічному рейтингу конкурентоспроможності WEF / Інтерфакс-Україна. Available at: https://ua.interfax.com.ua/news/economic/617843.html.

14. Україна в міжнародних рейтингах. E-Ukraine. Available at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey2018?fbclid=IwAR0ROie7FQWA-o7F3USIMIS5ePu2YMA40NLQ2rA52uUAUX6QCZJdtXtT2k8.

15. Україна в міжнародних рейтингах. E-Ukraine. Available at: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine.

16.Україна в міжнародних рейтингах. E-Ukraine. Available at: https://opendatabarometer.org/?_year=2017&indicator=ODB&fbclid=IwAR3N3W052by0j_QkJest6gM5bZ2c GDKGtGXV6K7dNPWrc88Qa4bFLf-xvJg.

17. Appadurai A. (1996). Modernity at Large: Cultural Dimensions of Globalization. Minneapolis.

18. Global ICT Development Index – ITU. 2017. Available at: https://www.itu.int/net4/ITU-D/idi/2017/index.html

19. Global Open Data Index. Отслеживание состояния открытых государственных данных. Available at: https://index.okfn.org/place/?fbclid=IwAR1jXf7Wo_XqfwW8TT6f2XT9QP5-o0umpV2HSmCsJ3nuZgeYQjkOz_a2Cbo/

20. Puschaver L., Eccles R. G. (1996). Input of the upside: Opportunity in Risk management. PW Rewiew, Dec., p. 25.

21. Robertson R. (1992). Globalization: Social Theory and Global Culture. London.

22. Sklair L. (1991). Sociology of the Global System. Hemel Hempstead.

1. Bek U. (2000). Obshchestvo ryska. Na puty k druhomu modernu. M.: Prohres-Tradytsyia. Retrieved from: http://royallib.com/book/bek_ulrih/obshchestvo_riska_na_puti_k_drugomu_modernu.html (in Russian).

2. Verchenko P. I. (2006). Bahatokryterialnist i dynamika ekonomichnoho ryzyku (modeli ta metody). K.: KNEU, 272 p. (in Ukrainian).

3. Vitlinskyi V. V., Nakonechnyi S . I. (1996). Ryzyk u menedzhmenti. K.: TOV "Borysfen-M", 336 p. (in Ukrainian).

4. Hlobalizatsiia i suchasnyi mizhnarodnyi protses (2009). Za zah red. B. Humeniuka, S. Sherhina. K.: Universytet Ukraina, pp. 42–45 (in Ukrainian).

5. Ivchenko I. Iu. (2004). Ekonomichnyi ryzyky: navchalnyi posibnyk. K.: Tsentr navchalnoi literatury, 304 p. (in Ukrainian).

6. Intehratsiia Ukrainy v hlobalnyi sotsialno-ekonomichnyi prostir (2019). [O. H. Bilorus ta in.]; NAN Ukrainy [ta in.]. K.: KNEU, 287 p. (in Ukrainian).

7. Horbulin V. P., Dodonov O. H., Lande D. V. (2009). Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia: monohrafiia. K.: Intertekhnolohiia, 164 p. (in Ukrainian).

8. Mashyna N. I. (2003). Ekonomichnyi ryzyk i metody yoho vymiriuvannia: navch. posib. dlia stud. VUZiv. K.: Tsentr navchalnoi literatury, 188 p. (in Ukrainian).

9. Mur A., Khyarnden K. (1998). Rukovodstvo po bezopastnosty byznesa: praktycheskoe posobye po upravlenyiu ryskamy. M.: Fylynъ, 328 p. (in Russian).

10. Natsionalnyi bank Ukrainy. Zvit pro finansovu stabilnist. Cherven 2020 roku. Available at: https://bank.gov.ua/admin_uploads/article/FSR_2020-H1.pdf?v=4 (in Ukrainian).

11. Nekrasov V. IT-haluz Ukrainy proty "koronakryzy": skorochen personalu ta urizannia zarplat ne bude, poky shcho. *Ekonomichna pravda*. Retrieved from: https://www.epravda.com.ua/publications/2020/04/6/658983/ (in Ukrainian).

12. Semeniutina T. V. (2012). Ekonomichni ryzyky, nebezpeky, zahrozy: sutnist ta vzaiemozviazok. *Ekonomichnyi prostir*: zbirnyk nauk. prats. Dnipropetrovsk: PDABA, No. 68, pp. 106–113 (in Ukrainian).

13. Ukraina opustylasia na 85-te mistse v shchorichnomu reitynhu konkurentospromozhnosti WEF / Interfaks-Ukraina. Retrieved from: https://ua.interfax.com.ua/news/economic/617843.html (in Ukrainian).

14. Ukraina v mizhnarodnykh reitynhakh. Retrieved from: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey2018?fbclid=IwAR0ROie7FQWA-o7F3USIMIS5ePu2YMA40NLQ2rA52uUAUX6QCZJdtXtT2k8 (in Ukrainian).

15. Ukraina v mizhnarodnykh reitynhakh // E-Ukraine. Retrieved from: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine (in Ukrainian).

16. Ukraina v mizhnarodnykh reitynhakh. E-Ukraine. Retrieved from: https://opendatabarometer.org/?_year=2017&indicator=ODB&fbclid=IwAR3N3W052by0j_QkJest6gM5bZ2c GDKGtGXV6K7dNPWrc88Qa4bFLf-xvJg (in Ukrainian).

17. Appadurai A. (1996). Modernity at Large: Cultural Dimensions of Globalization. Minneapolis.

18. Global ICT Development Index – ITU. 2017. Retrieved from: https://www.itu.int/net4/ITU-D/idi/2017/index.html

19. Global Open Data Index. Otslezhyvanye sostoianyia otkrыtыkh hosudarstvennыkh dannыkh. Retrieved from: https://index.okfn.org/place/?fbclid=IwAR1jXf7Wo_XqfwW8TT6f2XT9QP5-o0umpV2HSmCsJ3nuZgeYQjkOz_a2Cbo/

20. Puschaver L., Eccles R. G. (1996). Input of the upside: Opportunity in Risk management. ***PW Rewiew***, Dec., p. 25.

21. Robertson R. (1992). Globalization: Social Theory and Global Culture. London.

22. Klair L. (1991). Sociology of the Global System. Hemel Hempstead.

O. Shandrivska[1], N. Shynkarenko[2]
[1] Lviv Politechnik National University,
Department of marketing and logistic,
[2] National Technical University "Dnipro Politechnik",
Department of marketing

APPLIED RISK ASSESSMENT IN THE SYSTEM OF SOCIO-ECONOMIC PROCESSES IN CYBERSPACE

In the paper investigated safety of socio-economic processes in the virtual space. Studied the main trends influence on formation of preventive and adaptive mechanisms for ensuring information and cyber security enterprises. Key trends of the modern business and social environment include:

globalization, informatization and individualization of consumer needs; mediatization, territorialization and universalization of social phenomena.

Presented an original ensuring security model for the virtual information sphere. In this model was invented a conceptual scheme for identifying the information security system: given the identification sequence and risks assessment in cyberspace by stages; risk identification; a description of the threats it poses; identification of vulnerable market segments; analysis and assessment of the risk occurrence probability level; analysis and assessment of the risk manifestation consequences level; score determination of the general rick level; proposal to eliminate the development environment risks of the study object; net risk identification; risks in cyberspace have been identified and assessed in terms of security and financial flows.

Among the dominant risks of the external and internal security environment in the information virtual Ukrainian space the following are highlighted: insufficient system security, processes and technologies, disinformation and information asymmetry; high sensitivity of financial flows to the processes of the implementation of shock macroeconomic phenomena (including almost unsignificant currencies devaluation against the pandemic background) in terms of the safety of financial flows; technical, technological and personal vulnerability growth in the information sphere, due to the increasing cybercrime in terms of the information flow security.

Among the mitigation measures and neutralization of the general risk level, was proposed the creation of a single protection system. The single data protection system should be based on: data protection progressive principles, tasks to ensure security from information influences, information infrastructure security, information rights, open access to information, publicity of open information, etc.; organizational and right mechanism of data protection. This mechanism is based on the need to streamline the responsibilities of information marked actors; state control over data manipulation; data manipulation standards development; information systems certification for their processing.

Construction of database registers, as well as registration of owners and/or data administrators, third parties to whom the data was transferred for further manipulation; an independent coordination center formation for the state policy implementation in terms of monitoring compliance with data protection requirements, etc.; increasing the financial flow transparency, namely risk-oriented monitoring in digital currency exchanges and licensing of transactions in virtual currencies requires support from the Financial Action Task Force on Money Laundering and the Financial Intelligence Unit.

Key words: globalization; informatization; risks; dangers; threats; cyberspace; information security; ensuring information security.