ISSN 2072–8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2021.3(53)
Issue 3(53) 2021

УДК 351.86:004

Користін Олександр Євгенійович,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
головний науковий співробітник ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0001-9056-5475
Веселова Лілія Юріївна,
доктор юридичних наук, доцент,
Одеський державний університет внутрішніх справ, м. Одеса, Україна
ORCID ID 0000-0001-6665-0426

РИЗИКОРІЄНТОВАНІСТЬ КІБЕРБЕЗПЕКИ

Статтю присвячено аналізу проблем упровадження ризик-менеджменту у сфері кібербезпеки. Методологічно зосереджується увага на усвідомленні феномену ризику. Акцентовано увагу на питаннях, які формують чітку уяву щодо гібридності кіберзагроз та основних напрямів правового та організаційного забезпечення кібербезпеки. Проаналізовано низку документів Європейського Союзу у частині протидії гібридним кіберзагрозам. Зроблено висновки, що вітчизняна нормативна база має суттєві недоліки та потребує упровадження відповідних норм щодо запровадження ризик-орієнтованого підходу у діяльності щодо забезпечення кібербезпеки в Україні.

Ключові слова: *кібербезпека, ризик, загроза, ризик-орієнтований підхід, стійкість, уразливість, гібридні загрози.*

У сучасному суспільстві проблематика кібербезпеки привертає все більше уваги. Розвиток інформаційного суспільства та сформовані правові інструменти забезпечують реалізацію інформаційних прав і обов'язків громадян, визначають ступінь розвитку інформаційної сфери України, стан інформаційного правопорядку, рівень забезпечення правової охорони і захисту соціальних цінностей. За умови гібридизації кіберзагроз, національна безпека загалом, зокрема її інформаційна складова – кібербезпека, потребують формування безпекового кіберпростору та системного упровадження правових інструментів превентивного характеру. Одним із ключових світових трендів кібербезпеки базується на ризик-орієнтованому підході.

Сьогодні в умовах гібридної війни, яка з весни 2014 року активно нав'язується Україні, забезпечення кібербезпеки має надзвичайно важливе значення, так як кібератаки, які є фактично ескалацією бойових дій у кіберпросторі, поширюють технологічно новітні форми агресії та підвищують загрози інтересам громадян та суспільства, а в окремих випадках завдають реальних збитків державі.

У НАТО та ЄС є чітке розуміння того, що гібридним загрозам потрібно запобігати, з-поміж іншого, і "пасивними" елементами, такими як посилення стійкості до потрясінь чи несподіванок. У цьому контексті неможливо перебільшити важли-

DOI (Article): https: //doi.org/10.36486/np.2021.3(53).17

вість активних дій з посиленням цивільної готовності, вільної преси, освіченого населення і дієвої правової структури тощо [1].

У розвиток зазначеного, Європейська комісія разом з Європейською службою зовнішніх зв'язків (англ. *European External Action Service*, EEAS) у 2016 році розробили Об'єднану структуру протидії гібридним загрозам [2], що складається із 22 заходів для країн-учасниць та інституцій, які визначають підходи до виявлення гібридних загроз, покращувати інформованість про них і здійснювати кроки з розвитку стійкості. Зазначені заходи підвищують спроможність протистояти гібридним загрозам, починаючи від обміну інформацією і до захисту критичної інфраструктури, кібербезпеки, стійкості суспільства до радикалізму та екстремізму, зокрема [3]:

створення гібридної ланки ЄС для збору інформації та інформування осіб, що приймають рішення у закладах ЄС та державах-членах;

створення Європейського центру передового досвіду з протидії гібридним загрозам;

забезпечення проактивної стратегічної комунікації та оптимізації моніторингу ЗМІ щодо протидії дезінформації;

підвищення стійкості;

посилення кібербезпеки у Європі за допомогою широкомасштабних конкретних заходів, спрямованих на значне посилення структур кібербезпеки ЄС та можливостей реагування;

боротьба з онлайн-дезінформацією для забезпечення більш безпечного Інтернету, запобігання втручанням у вибори тощо.

Виділення окремих заходів за напрямом протидії саме гібридним загрозам яскраво демонструє пріоритет, що сформувався в ЄС.

Подальший розвиток системи забезпечення кібербезпеки в ЄС достатньо ґрунтовно характеризується у підсумкових документах, що вийшли у вигляді:

спільних комюніке Європейського парламенту та Європейської ради щодо реалізації заходів протидії гібридним загрозам в Європейському Союзі (06.04.2016 р. [4]; 19.07.2017 р. [5]; 13.06.2018 р. [6]) та звіту про імплементацію плану заходів 2016 року щодо протидії гібридним загрозам, а також Спільного повідомлення 2018 року про підвищення стійкості та посилення можливостей для подолання гібридних загроз від 28.05.2019 [7].

Основною метою зазначених звітних щорічних документів є представлення для європейської спільноти звіту щодо прогресу та наступних кроках щодо виконання дій у чотирьох сферах запропонованих у Спільних заходах: підвищення поінформованості щодо ситуації: стійкість суспільства; посилення здатності щодо запобігання кризи та реагування на них, а також координація відновлення та розширення співробітництва з НАТО для забезпечення взаємного доповнення у заходах.

Розвиваючи питання підвищення обізнаності щодо гібридних кіберзагроз, акценти ставляться на визначенні вразливості суспільства щодо них та скоординованої діяльності щодо оцінювання зазначених загроз. Для виявлення ключових вразливостей, враховуючи конкретні гібридні показники, здійснюється аналіз ризиків, що впливають на інститути та мережі.

DOI (Article): https: //doi.org/10.36486/np.2021.3(53).17

З приводу ризик-орієнтованого підходу, доречним є звернути увагу на ухвалення 20 грудня 2002 року Генеральною асамблею ООН резолюції 57/239 "Елементи для створення глобальної культури кібербезпеки" [8], згідно з якою термін "кібербезпека" почав активно використовуватись у правовій термінології. Показовим є те, що ще у 2002 році документи ООН вказували на необхідність оцінювання ризиків з метою виявлення загроз та факторів уразливості.

Зі свого боку глобальна культура кібербезпеки передбачає врахування дев'яти взаємопов'язаних елементів, зокрема:

– *обізнаність* (тобто учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що саме вони можуть здійснити для підвищення безпеки);

– *відповідальність* (учасники відповідають за безпеку мереж відповідно до власної ролі);

– *реагування* (учасники мають вживати своєчасних та спільних заходів щодо попередження інцидентів, які стосуються безпеки, їх виявлення та реагування, у тому числі обмінюватись інформацією і вводити процедури, які передбачають оперативне та ефективне співробітництво з попередження, виявлення та реагування таких інцидентів);

– *етика* (врахування законних інтересів інших);

– *демократія* (безпека повинна забезпечуватись так, щоб це відповідало демократичним цінностям, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації, належний захист приватної інформації; відкритість та гласність);

– *оцінка ризиків* (учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації, яка захищається);

– *проектування та впровадження засобів забезпечення безпеки*;

– *переоцінка* (належні та своєчасні заходи з внесення змін у політику, практику забезпечення безпеки з врахуванням нових та зміни існуючих загроз) [9, с. 72–73].

Резолюція ООН – не єдиний міжнародний правовий документ, що акцентує увагу на необхідності оцінювання ризиків у системі забезпечення кібербезпеки. Зокрема, Директива ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (Директива NIS) [10] закладає єдині правила та вимоги в сфері кібербезпеки для всіх країн ЄС, але залишає за кожною країною-членом право вжити власних заходів щодо імплементації норм цієї Директиви в національне законодавство. Більше того, Директива вимагала від країн-членів упровадження цих правил ще до 9 травня 2018 року.

Зазначене передбачає, що для підвищення спроможності забезпечення кібербезпеки на національному рівні держави-члени ЄС повинні розробити національну стратегію мережевої та інформаційної безпеки, яка має включати в себе:

стратегічні цілі, пріоритети та державне підґрунтя,

заходи з підготовки до кіберінцидентів, реагування на них та відновлення після них,

DOI (Article): https: //doi.org/10.36486/np.2021.3(53).17

засади державно-приватного партнерства,
програму освітніх, тренувальних заходів та заходів з підвищення обізнаності,
план науково-дослідницьких робіт,
план оцінки та управління ризиками,
список стейкголдерів, відповідальних за реалізацію стратегії,
визначити один чи більше державних органів, що будуть відповідати за виконання Директиви,
створити одну чи більше команд реагування на комп'ютерні надзвичайні події.

Загалом, для досягнення мети Директиви, забезпечення більш високого рівня мережевої та інформаційної безпеки в межах Європейського Союзу, визначено у якості необхідних заходів три основних напрями:
підвищення спроможності системи кібербезпеки на національному рівні;
підвищення рівня пан-європейського співробітництва;
запровадження управління ризиками та зобов'язання сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових послуг.

Таким чином, управління ризиками міжнародними правовими актами визначається не лише у якості рекомендацій, а й як обов'язковий елемент, що підвищує обізнаність щодо вразливості системи у сфері забезпечення кібербезпеки.

Для розуміння проблем, що мають місце у сфері забезпечення кібербезпеки, а також знаходження шляхів їх вирішення важливим, є дослідження питань історії і логіки походження поняття "ризик", його сутності, змісту та місця у системі сучасного суспільного розвитку.

Загалом, потрібно зазначити, що розвиток суспільства у досить тривалий історичний період певним чином відзначався ризиковим характером. Поряд з тим, порівняно новітнім продуктом розвитку наукової думки стало усвідомлення ризикогенності людської діяльності та атрибутивність ризику у процесах сучасного суспільного розвитку.

Як свідчить практичний досвід, для більшості осіб, що приймають управлінські рішення, психологічно важко адекватно сприймати атрибутивність ризику. Особливо нерозуміння важливості зазначеного мало місце за радянських часів, коли головним постулатом було притаманність ризиків лише капіталістичному суспільству через дію ринкових законів, стихійність та відсутності планування. Ментальне несприйняття феномену ризику мало місце не лише у радянських державних діячів. Американський правознавець Т. Лоуві зазначає, що у цей же, фактично, час в американській державній політиці, попри старі традиції лібералізму, які високу цінність надавали праву на ризик, домінувала доктрина захисту від ризику і декларацій побудови у Сполучених Штатах "суспільства, вільного від ризику" [11, с. 254]. Лише з приходом до влади уряду Р. Рейгана розпочалася переоцінка проблеми ризику в політичній ідеології у бік деміфологізації ідеї "суспільства, вільного від ризику" на користь пошуку конструктивних підходів до державного управління ризиками суспільного життя [11].

Обґрунтований погляд на проблему ризику базується на усвідомленні феномену ризику, що є сталим атрибутом людської життєдіяльності, з широким спектром прояву та масштабами, що пов'язані із соціально-історичним розвитком

DOI (Article): https: //doi.org/10.36486/np.2021.3(53).17

суспільства, і є певним чином віддзеркаленням його інтенсивності. Для сучасного сприйняття важливим є розуміння того, що в інформаційному суспільстві за рахунок поширення інфогенних ризиків, посилюються характерні для індустріальної стадії суспільного розвитку соціальні ризики.

Гідденс Е. зазначає, що жити в епоху "пізньої сучасності", під якою він, по суті, розуміє інформаційне суспільство, значить жити в світі випадковостей і ризику, незмінних супутників соціальної системи, що прагне до встановлення владарювання над природою та рефлексивного творіння історії. На його думку, поняття ризику стає центральним у суспільстві, яке прощається з минулим та традиційним і відкривається для незвіданого майбутнього, а в самому суспільстві з'являється таке явище, як прагнення контролювати час і колонізувати майбутнє [12, с. 107].

Так, Штомпка П., розвиваючи погляди щодо зростання ризикогенності суспільного розвитку зазначає, що феномен ризику набуває нових якостей, пов'язаних із виникненням нових некерованих ситуацій, які приховують загрозу не лише окремим індивідам, а й соціальним системам, і в тому числі державам, наражаючи на небезпеку мільйони людей, а то й людство в цілому. Такі нові якості ризику вирізняють його як з об'єктивної, так і з суб'єктивного погляду, бо не лише посилюються й урізноманітнюються фактори ризику самі по собі, але й стає більш гострим, ніж коли-небудь раніше, їх сприйняття [13].

Тобто можемо стверджувати, що феномен ризику набуває більш універсальної форми, що несе певні загрози суспільству незалежно від етнічної чи класової належності. Крім того, ризики глобалізуються, торкаючись все більшої кількості людей, та розповсюджуються на все більш широкі території. У сучасних умовах окремі несприятливі події в різних країнах і регіонах світу трансформуються в цілісну глобальну проблему – проблему виживання людства в ускладнених природних і суспільно-політичних умовах, висувають на порядок денний питання про існування глобального ризику [14]. Тотальність і всеосяжність ризику на сучасному етапі розвитку суспільства сформували підстави щодо утвердження стійкого сприйняття проблеми ризику як одного з утворюючих факторів сучасного і особливо майбутнього суспільства, що також набуває все більшого загально-соціального значення.

Різні автори вбачають у цьому навіть зміну політико-суспільних акцентів і початок процесу формування новітньої фази розвитку суспільства – "суспільства ризику". Більше того, як стверджує німецький учений Ульріх Бек (Beck U.), людство вже вступило в цю нову фазу свого розвитку [15]. Цієї думки дотримується також Роберт Швеблер (Schwebler R.) [16].

Причиною таких змін є характерні особливості більшості сучасних загроз та породжуваних ними ризиків, які виходять за межі локального значення та набувають глобального. Такий підхід достатньою мірою відображено в наступному визначенні суспільства ризику – це постіндустріальна формація, яка відрізняється від індустріального суспільства низкою особливостей, головною з яких є те, що якщо для індустріального суспільства характерним був розподіл благ, то для суспільства ризику – розподіл загроз і зумовлений цим ризик [17, с. 281–282].

DOI (Article): https: //doi.org/10.36486/np.2021.3(53).17

Більше того, низка фахівців у галузі теорії ризику висувають припущення про те, що в найближчій перспективі світове співтовариство чекає ще більш суттєва трансформація. На їх думку, логічним й історично природним продовженням "суспільства ризику" буде суспільство більш високого рівня – побудоване на управлінні ризиком. Тобто суспільство будуватиме свою стратегію розвитку не тільки з урахуванням ризику, але навіть на базі управління ризиком [18].

Бехман Г. зазначає, що в ментальності індустріального суспільства різного роду деструктивні наслідки нерідко звужуються до залишкового ризику, який у зв'язку з величезними прибутками трактується як соціально адекватні втрати, свого роду допустима ціна за добробут [19, с. 27]. Тому ризик не стільки є властивістю техніки, скільки зумовлений потенційною діяльністю суспільства, в якому майбутнє не може бути розмитим і повинно вже сьогодні бути усвідомленим і прорахованим [19, с. 42].

Важливим, на нашу думку, є узагальнення Бека У., який зазначає, що стабільність у суспільстві ризику виявляється стабільністю відмови від продумування наслідків та необхідності усвідомлення ризикогенного характеру сучасного суспільного розвитку як на рівні пересічних громадян, так і на рівні суспільства та державної влади [17, с. 287].

З погляду Лумана Н., слід розмежовувати ризик і небезпеку, бо небезпека є завжди, оскільки немає абсолютної надійності, а ризик має місце там, де є рішення або відмова від нього. При цьому вчений наголошує, що вільної від ризику поведінки не існує, як і не існує абсолютної надійності. Якщо рішення не приймається і суб'єкт утримується від дій, то все одно ризику він не уникає [20]. Так, Луман Н. вважає, що усвідомлення, оцінка ризику і прийняття ризику – проблема не лише ментальна (психологічна), а й соціальна, бо сам по собі зовнішній світ не знає ніякого ризику, оскільки йому, на відміну від людини й суспільства, не відомі ніякі очікування, цінності та калькулювання імовірностей [17, с. 274].

Еволюційні перетворення, що мають місце з утвердженням інформаційного суспільства, потребують упровадження науково обґрунтованої системи заходів прогнозування суспільного розвитку у будь-якій сфері життєдіяльності. Як зазначав відомий американський футуролог Ф. Фукуяма, зрушення у бік інформаційного суспільства віталося практично всіма, хто про нього писав або говорив. Усі зміни, які принесе розвиток інформаційного суспільства, розглядалися виключно як сприяючі процвітанню суспільства в цілому, а також благотворні для демократії та свободи особистості [21]. Саме в такому аспекті розглядаються й наслідки розбудови інформаційного суспільства в Україні у низці відповідних законодавчих та урядових документів, а також у більшості українських наукових досліджень.

Тому важливим елементом подальшої розбудови системи забезпечення кібербезпеки України, особливо в умовах гібридної війни, є необхідність імплементації положень Директиви Європейського Парламенту І Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (далі – Директива NIS) [10]. Положення зазначеної Директиви NIS містять низку вимог щодо покращання рівня кібербезпеки. Зокрема, національні стратегії кібербезпеки, стосується і визначення ризиків.

Крім того, у ст.ст. 14 та 16 першою вимогою щодо безпеки й повідомлення про інциденти зазначено, що держави-члени повинні забезпечити умови операторам основних послуг, а також надавачам цифрових послуг, для вжиття ними відповідних та пропорційних технічних та організаційних заходів для управління ризиками, пов'язаними із безпекою мережевих та інформаційних систем, які вони використовують у своїх операціях.

Загалом у тексті Директиви NIS 17 разів використовується термін "ризик", який у ст. 4 "Терміни та означення" визначено так: "ризик" означає будь-яку обставину чи подію, яку можна розумно виявити, що має потенційний негативний вплив на безпеку мережевих та інформаційних систем [10].

Потрібно зазначити, що у зв'язку з імплементацією Україною європейського законодавства, ми змушені будемо зазначені норми Директиви NIS також імплементувати до вітчизняного законодавства. Водночас чинний Закон України "Про основні засади забезпечення кібербезпеки України" будь-якої діяльності щодо оцінювання ризиків у сфері забезпечення кібербезпеки не передбачає.

На нашу думку, зазначене є суттєвим недоліком чинного вітчизняного законодавства, що мотивується нами з декількох точок зору:

об'єктивно сучасні процеси суспільного розвитку потребують запровадження інституту наукового прогнозу у прийнятті управлінських рішень, забезпечення якого методологічно лежить у безпекознавчій площині та базується на ризик-орієнтованому підході до прогнозування;

оцінювання ризиків у сфері забезпечення кібербезпеки України є не лише необхідністю сучасного етапу розвитку суспільства, а й вимогою формальною та юридичною міжнародного законодавства, зокрема, європейського, подальша імплементація якого в Україні зобов'язує до виконання та впровадження;

з методологічного погляду, оцінювання ризиків передбачає не лише інформування щодо величини тієї чи іншої загрози у кіберсфері, а й з'ясування питань стійкості суспільства у протидії цим загрозам, що зі свого боку формує підґрунтя для визначення пріоритетних напрямів підвищення стійкості вітчизняної системи у сфері забезпечення кібербезпеки України;

з огляду на місце інституту ризик-орієнтованого підходу (оцінювання ризиків, управління ризиками) у механізмі державного регулювання, об'єктивним є упровадження його у чинному законодавстві та визначення важливим інструментом у механізмі адміністративно-правового регулювання у якості заходів попереджувального характеру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Співпраця заради протидії гібридним загрозам. URL: https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html (дата звернення: 02.07.2021).

2. A Europe that Protects: Countering Hybrid Threats. URL: https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en (дата звернення: 02.07.2021).

3. A Europe that protects: good progress on tackling hybrid threats. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788 (дата звернення: 02.07.2021).

4. Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018(дата звернення: 02.07.2021).

5. Joint Report to The European Parliament and the Council on the Implementation of the Joint Framework on countering hybrid threats - a European Union response. 2017. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017JC0030 (дата звернення: 02.07.2021).

6. Joint Report to the European Parliament, the European Council and the Council on the Implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2018:014:FIN (дата звернення: 02.07.2021).

7. Joint Staff Working Document Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. URL: https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf (дата звернення: 02.07.2021).

8. Резолюция Генеральной Ассамблеи ООН 57/329, принятая на 78 пленарном заседании 57-й сессии. 20 декабря 2002 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата звернення: 02.07.2021).

9. *Довгань О.Д., Доронін І.М.* Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки: монографія. Київ: Видавничий дім "АртЕк", 2017. 107 с.

10. Директива Європейського Парламенту І Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA (дата звернення: 02.07.2021).

11. *Лоуви Т.* Риск и право в истории американского государства. THESIS, 1994. № 5. С. 253–267.

12. *Гидденс Э.* Судьба, риск и безопасность. THESIS, 1994. № 5. С. 107–134.

13. *Шутаева Е.А.* Формирование глобального информационного общества: перспективы Украины. Ученые записки. Симферополь, 2008. Т. 21, № 1 (60): Экономика. С. 139–145.

14. *Альгин А.П.* Риск и его роль в общественной жизни. Москва: Мысль, 1989. 188 с.

15. *Beck U.* Risk Society. Towards a New Moderning. London, 1992. 260 p.

16. *Schwebler Robert.* Individualversicherung in Wirtschaft und Gesellschaft. Versicherungswirtschaft, 1990. № 1.

17. *Єфименко Т.І., Гасанов С.С., Користін О.Є.* та ін. Розвиток національної системи фінансового моніторингу. Київ: ДННУ "Акад. фін. управління", 2013. 380 с.

18. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Матеріал для обговорення. URL: https://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf (дата звернення: 02.07.2021).

19. *Бехман Г.* Современное общество как общество риска. Вопросы философии, 2007. № 1. С. 26–46.

20. *Луман Н.* Понятие риска. THESIS, 1994. Вып. 5. С. 135–160.

21. *Фукуяма Ф.* Великий разрыв. Москва: PHILOSOPHY, 2004. 480 с.

REFERENCES

1. Spivpratsia zarady protydii hibrydnym zahrozam. Cooperation to counter hybrid threats. URL: https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html (Date of Application: 02.07.2021) [in Ukrainian].

2. A Europe that Protects: Countering Hybrid Threats. URL: https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en (Date of Application: 02.07.2021) [in English].

3. A Europe that protects: good progress on tackling hybrid threats. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788 (Date of Application: 02.07.2021) [in English].

4. Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (Date of Application: 02.07.2021) [in English].

5. Joint Report to The European Parliament and the Council on the Implementation of the Joint Framework on countering hybrid threats – a European Union response. 2017. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017JC0030 (Date of Application: 02.07.2021) [in English].

6. Joint Report to the European Parliament, the European Council and the Council on the Implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2018:014:FIN (Date of Application: 02.07.2021) [in English].

7. Joint Staff Working Document Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. URL: https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf (Date of Application: 02.07.2021) [in English].

8. Rezoliutsyia Heneral'noj Assambley OON 57/329, pryniataia na 78 plenarnom zasedanyy 57-j sessyy. 20 dekabria 2002 hoda. UN General Assembly resolution 57/329, adopted at the 78th plenary session of the 57th session. December 20, 2002. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (Date of Application: 02.07.2021) [in Russian].

9. *Dovhan,' O.D., Doronin, I.M.* (2017) Eskalatsiia kiberzahroz natsional'nym interesam Ukrainy ta pravovi aspekty kiberzakhystu. "Escalation of Cyber Threats to the National Interests of Ukraine and Legal Aspects of Cyber Defense": monograph. Kyiv: ArtEk Publishing House. 107 p. [in Ukrainian].

10. Directive of the European Parliament and of the Council (EU) 2016/1148 of 6 July 2016 on Measures for a High Common Level of Security of Network and Information Systems in the Union. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA (Date of Application: 02.07.2021) [in Ukrainian].

11. *Louvi, T.* (1994) Risk i pravo v istorii amerikanskogo gosudarstva. Risk and Law in the History of the American State. No 5. P. 253–267 [in Russian].

12. *Giddens, Je.* (1994) Sud'ba, risk i bezopasnost'. "Risk and Law in the History of the American State". THESIS. No 5. P. 107–134 [in Russian].

13. *Shutaeva, E.A.* (2008) Formirovanie global'nogo informacionnogo obshhestva: perspektivy Ukrainy. "Formation of a Global Information Society: Prospects for Ukraine". Scientific Notes. Simferopol. Vol. 21. No 1 (60): Economics. P. 139–145 [in Russian].

14. *Al'gin, A.P.* (1989) Risk i ego rol' v obshhestvennoj zhizni. "Risk and Its Role in Public Life". Moscow: Mysl.188 p. [in Russian].

15. *Beck, U.* (1992) Risk Society. Towards a New Moderning. London. 260 p. [in English].

16. *Schwebler Robert* (1990) Individualversicherung in Wirtschaft und Gesellschaft. Versicherungswirtschaft. No 1 [in German].

17. *Yefymenko, T.I., Hasanov, S.S., O.Ye. Korystin, J.Ye.* and others (2013) Rozvytok natsional'noi systemy finansovoho monitorynhu. "Development of the National System of Financial Monitoring". Kyiv: DNNU "Acad. Financial Management". 380 p. [in Ukrainian].

18. Propozytsii do polityky schodo reformuvannia sfery kiberbezpeky v Ukraini. "Proposals for a Policy on Cybersecurity Reform in Ukraine". Material for discussion. URL: https://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf (Date of Application: 02.07.2021) [in Ukrainian].

19. *Behman, G.* (2007) Sovremennoe obshhestvo kak obshhestvo riska. "Modern Society as a Society of Risk". Issues of Philosophy 1, 26–46 [in Russian].

20. *Luman, N.* (1994) Ponjatie riska. "The Concept of Risk". THESIS. Issue 5. P. 135–160 [in Russian].

21. *Fukujama, F.* (2004) Velikij razryv. "Great Break". Moscow: PHILOSOPHY, 2004. 480 p. [in Russian].

DOI (Issue): https: //doi.org/10.36486/np.2021.3(53) Issue 3(53) 2021

UDC 351.86:004

Korystin Oleksandr,
Doctor of Law, Professor, Honored Academic of Science and Technology of Ukraine, State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-9056-5475
Veselova Liliia,
Doctor of Law, Associate Professor, Odessa State University of Internal Affairs, Odesa, Ukraine,
ORCID ID 0000-0001-6665-0426

RISK ORIENTATION OF CYBER SECURITY

Research article is devoted to the analysis of the problems of risk management implementation in the field of cybersecurity. Methodologically, the focus is on understanding of the phenomenon of risk. Emphasis is placed on the issues that form a clear idea of the hybridity of cyber threats and the main directions of legal and organizational support of cybersecurity.

Paper analyzes a number of EU documents that form a clear idea of the hybridity of cyber threats and the main directions of legal and organizational support of cybersecurity, in particular, on combating hybrid cyber threats in the European Union. The opinion on risk problems, awareness of the phenomenon of risk, which is a permanent attribute of human life, with a wide range of manifestations and scales related to the socio-historical development of society, and is in some way a reflection of its intensity, is revealed and substantiated. Emphasis is placed on the fact that for modern perception it is important to understand that in the information society due to the spread of infogenic risks, the social risks characteristic of the industrial stage of social development are intensifying. Based on the analysis, it is concluded that at the present stage of development of society formed the basis for the establishment of a stable perception of risk as one of the factors of modern and especially future society, which is also becoming increasingly important. Risk occurs in the activities of management entities in a situation of uncertainty, and therefore is a constant attribute of management activities. At the same time, the evolutionary transformations that take place with the establishment of the information society require the introduction of a scientifically sound system of measures for forecasting social development in any sphere of life. In developing awareness of hybrid cyber threats, emphasis has been placed on identifying societal vulnerabilities to them and coordinated action to assess these threats. To identify key vulnerabilities, taking into account specific hybrid indicators, it is necessary to analyze the risks affecting institutions and networks.

Keywords: cybersecurity, risk, threat, risk-oriented approach, resilience, vulnerability, hybrid threats.

Отримано 18.10.2021

DOI (Article): https: //doi.org/10.36486/np.2021.3(53).17