DOI: https://doi.org/10.32839/2304-5809/2020-6-82-53
УДК 343.9

Лугіна Н.А., Вартовнік А.М.
Університет державної фіскальної служби України

КРИМІНОГЕННА ДЕТЕРМІНАЦІЯ КІБЕРЗЛОЧИННОСТІ В БАНКІВСЬКІЙ СФЕРІ

Анотація. В статті досліджуються групи, на які поділяються детермінанти кібезлочинності. При аналізі правових детермінант виокремлено основні законодавчі недоліки, зокрема недостатня врегульованість таких нових технологій, як: інтернет-банкінг, Big data, кредитних електронних платформ, криптовалют, блокчейну та інше. Розкрито недоліки Стратегії кібербезпеки, як основного документа, що регулює кіберпростір. Серед політичних чинників виявлено головну проблему – а саме цілковите направлення державної політики на відбиття агресії з боку Російської Федераці, при чому у зв'язку з цим, обмежуються бюджетні фінансування робіт вітчизняних вчених щодо дослідження кіберпростору всередині країни. Досліджено, що соціальні чинники кіберзлочинності пов'язані із тим, що багато сфер суспільної активності переходить у віртуальний простір, що створило нові можливості для вчинення різноманітних злочинів за допомогою електронно-обчислюваної техніки. Встановлено, що кіберзлочинність виступає побічним продуктом так званої «техноревлюції».

Ключові слова: кіберзлочинність, кібербезпека, детермінанти кіберзлочинності, інноваціні технології, глобальнізація, техноревлюція.

Lygina Natalia, Vartovnik Anastasiia
University of the State Fiscal Service of Ukraine

CRIMINOGENIC DETERMINATION OF CYBERCRIME IN THE BANKING SECTOR

Summary. The article explores the groups into which the determinants of cybercrime are divided. When analyzing legal determinants, the main legislative shortcomings were highlighted, in particular, the lack of regulation of such new technologies as Internet banking, Big data, electronic credit platforms, cryptocurrencies, blockchain technologies and so on. Disclosed are the shortcomings of the Cybersecurity Strategy, as the main document regulating cyberspace. Among the political factors, the main problem was identified – namely, the full direction of state policy to repel aggression from the Russian Federation, and in this regard, budgetary funding for the work of domestic scientists on the study of cyberspace inside the country is limited. It has been proved that the social factors of cybercrime are related to the fact that many areas of social activity are moving into the virtual space, which has created new opportunities for committing various crimes using electronic computer technology. It has been established that cybercrime is a by-product of the so-called technological revolution. Cybercrime is inextricably linked to the development of information infrastructure. This is due to the fact that with the constant growth of society's dependence on the smooth operation of computer systems aimed at their destruction, cause more and more significant damage and cause a serious public response. Among the determinants of cybercrime, special attention is paid to corruption. Experts note that corruption and incompetence in regulating information security and cybersecurity in Ukraine are making the situation critical. After analyzing the opinions of various scholars, we can conclude that corruption is the most dangerous threat to national security. It exists as a norm in the relations of economic entities and in the economy as a whole, leading to the use of public goods in their own interests in the shadow trade. Corruption is becoming a major obstacle to building intellectual capacity in the fight against cybercrime. After all, corruption hinders the education of patriotism and the application of their knowledge for the benefit of their country, it is a determinant of cynicism. Many scientists and practitioners have proven that for our country, among other dangers, corruption risks pose the most serious threat to the stable and safe operation of many critical infrastructure facilities.

Keywords: cybercrime, cybersecurity, determinants of cybercrime, technology innovation, globalization, technological revolution.

Постановка проблеми. Якщо звернутися до загального кримінологічного поділу детермінант в теорії, то їх можна застосувати і до причини розповсюдження такого явища як кіберзлочинність. З урахуванням того, що зараз кіберзлочинці швидко пристосовуються, використовуючи найновітніші технології, кожен з нас може стати жертвою кіберзлочину і навіть не помітити. Хто знає, можливо саме ваш телефон вже є в загальній базі кіберзлочинців як один із ботів для використання в протизаконних діях. Тому все, це не викликає жодних сумнівів щодо актуальності та доцільності даних досліджень. Можна виділити наступні групи: політичні, економічні, соціальні, технологічні, психологічні, а також чинники пов'язані з діяльністю правоохоронних органів та віктимною поведінкою потерпілих.

Аналіз останніх досліджень і публікацій. Даній тематиці присвячено незначну кількість наукових досліджень. Варто відзначити, що дуже важливу роль у дослідженні кіберризиків та детермінантів кіберзлочинності відіграють страхові, консалтингові та інші приватні компанії. Дуже пильну увагу приділять і державні структури деяких країн, як наприклад, США, зокрема Федеральне Бюро розслідувань тощо.

Кіберризики розглядають як 1) систематичні ризики в діяльності фінансових установ; 2) складова ризиків компанії; 3) можливі злочини вчинені за допомогою Інтернет тощо.

Серед вчених, що займалися даним питанням слід виділити М. Елінга, В. Братюка, К. Семенової, К. Тарасової, Ю. Кожедуба.

Виділення невирішених раніше частин загальної проблеми. Не дивлячись на значні здобутки в даній сфері, відображено лише окремі аспекти кіберризиків, але поки є потреба в подальших повних та комплексних наукових дослідженнях. Можна сказати, що в науці, на даний момент, відсутнє повне дослідження кіберризиків з економічних проблем.

Формулювання цілей статті є дослідження детермінантів виникнення кіберризиків та їх негативного впливу на банківський сектор та фінансову систему національної економіки.

Виклад основного матеріалу дослідження. До правових детермінантів, зокрема, можна віднести окремі аспекти вітчизняної нормативної бази, зокрема теоретичне обґрунтування сутності фінансової безпеки та закріплення цього в законодавстві визначається як важлива складова частина економічної безпеки держави, її фінансового стану, що характеризується збалансованістю і якістю системної сукупності фінансових інструментів, технологій і послуг, стійкістю до внутрішніх і зовнішніх негативних чинників (загроз), здатністю цієї сфери забезпечувати захист національних фінансових інтересів, достатні обсяги фінансових ресурсів для всіх суб'єктів господарства та населення і в цілому – ефективне функціонування національної економічної системи і соціальний розвиток [1].

До ключових змін функціонування фінансового сектору під дією цифрової економіки відносять стрімкий розвиток інформаційних технологій, зокрема інтернет-банкінгу, алгоритмічної торгівлі, індустрії Big data, кредитних електронних платформ, блокчейну (Blockchain) та криптовалют із поступовою відмовою від готівкових розрахунків. Такі перетворення полягатимуть у поступовому перенесенні платіжних транзакцій в електронний вигляд, сприяють появі нових засобів платежу, новітніх платіжних інструментів і систем, що в свою чергу призводить до потреби постійного оновлення законодавства [2].

Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 5 березня 2016 року № 96/2016 передбачається створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Однак, цей документ хоча і називається стратегією, проте визначені в ньому основні засади кібербезпеки у світовій практиці не зовсім вважаються стратегічними. Варто додати, що головним атрибутом у закордонних стратегіях передбачається перелік конкретних проектів забезпечення кібербезпеки із кінцевим терміном їх реалізації, з виділеним фінансуванням і, що найголовніше, конкретними відповідальними. У нас це нагадує більше концепцію – напрями, куди треба рухатися зі своїми тактиками дій, власним, а не державним, фінансуванням і без будь-якої відповідальності [3].

Політичні чинники – це перш за все концентрація всіх і вся на агресії Російської Федерації. Так, не можна не відзначити зумовлені агресією хакерські атаки на Україну, одначе не слід залишати поза увагою значну кількість інцидентів, що відбуваються всередині країни. Також, вони виявляються у недостатньому усвідомленні урядом можливих соціальних наслідків кіберзлочинності. У зв'язку з цим, обмежуються бюджетні фінансування робіт зі створення правової, організаційної, технічної бази інформаційної безпеки держави та захисту прав і свобод громадян в віртуальному просторі. Фактично не виділяються кошти на фундаментальні та прикладні вітчизняні дослідження у сфері запобігання кіберзлочинності.

Соціальні чинники виступають своєрідними передумовами функціонування та розвитку кіберзлочинності. В першу чергу, це зміни в соціальному житті, породжені сучасним науково-технічним прогресом, пов'язані з всебічною комп'ютерізацією суспільства, а також формуванням інформаційного простору, заснованого на використанні ЕОМ, та зумовленого цим створенням і розвитком нових суспільних відносин у сфері комп'ютерної інформації. У зв'язку з цим, багато сфер суспільної активності переходить у віртуальний простір, що не залишилось без уваги кримінального середовища та створило нові можливості для вчинення різноманітних злочинів за допомогою електронно-обчислюваної техніки.

Отже, кіберзлочинність виступає побічним продуктом так званої «техноревалюції».

Економічний чинник. В Україні, як і в усьому світі економічні фактори детермінації пов'язані, перш за все, з процесом глобалізації світової економіки. Модернізація сучасного соціуму шляхом впровадження у життя продуктів комп'ютерної техніки та технологій несе з собою цілу низку новоутворень в соціальному бутті. Доступ все більшої кількості користувачів до глобальних інформаційних мереж, розвиток електронної торгівлі, можливість відкриття банківських рахунків через Інтернет і здійснення онлайн-операцій, що не вимагають безпосереднього контакту з контрагентом, поява електронних грошей обумовлюють зростання кіберзлочинів в сфері торгівлі і операцій з кредитними картками, крадіжок персональних даних, паролів доступу.

Психологічні детермінанти. Особа злочинця почуває необмежену свободу, здатність сховатися і при цьому діяти в нечуваних масштабах. Також, вони зумовлені особливостями кібепростору. У реальності існують певні перешкоди, а у віртуальності злочинець не бачить та не відчуває своїх жертв. Звичайно, що так легше красти гроші, наприклад, немає ризиків небезпеки, завдання комусь фізичної шкоди чи смерті та всіх інших аспектів. Злочини у мережі – це злочини на відстані. У зв'язку з цим, у винних осіб є певне усвідомлення анонімності та вони не бояться бути виявленим та притягнутим до кримінальної відповідальності.

Технологічні чинники. Кіберзлочинність нерозривно пов'язана із розвитком інформаційної інфраструктури. Це пояснюється тим, що при постійному зростанні залежності суспільства від безперебійного функціонування обчислювальних систем дії, спрямованих на їх руйнування, наносять все більш значної шкоди і викликають серйозний громадський резонанс [4].

Глобальна мережа привертає увагу кібертерористів такими своїми характерними особливостями: 1) оперативністю; 2) економічністю; 3) доступ-

ністю; 4) відсутністю контролю з боку держави; 5) наявністю величезної кількості потенційної користувачів; 6) легке і дешеве розміщення інформації; 7) конфіденційність та анонімність; 8) використання ботів; 8) складність відстежування та зібрання доказів; 9) просторово-часова віддаленість від об'єкта або суб'єкта кібератаки; 10) завжди існуватимуть вразливості в системах, які можна експлуатувати та зламати; 11) низький рівень формування ефективних правоохоронних структур.

Існують внутрішні і зовнішні загрози безпеці як окремого об'єкта так і держави. За характером впливу вони поділяються на: 1) економічні загрози – корупція, недобросовісна конкуренція, шахрайство, використання неефективних, застарілих технологій; 2) фізичні загрози – пошкодження або знищення обладнання, неефективна експлуатація технічних засобів, що призводить до їх швидкого зношування; 3) інтелектуальні загрози – дискредитація суб'єкту, розголошення чи неправомірне використання конфіденційної інформації, зокрема банківської, соціальне напруження та конфлікти навколо фінансових установ [5].

На наш погляд особливої уваги серед детермінантів кіберзлочинності посідає корупція. Експерти відзначають, що корупція та некомпетентність у сфері регулювання галузі інформаційної безпеки та кібербезпеки набувають в Україні роблять ситуацію критичною. На думку З. Варналія, корупція є найнебезпечнішою загрозою національній безпеці. Вона існує як норма в стосунках господарюючих суб'єктів та в економіці в цілому наштовхуючи на використання суспільних благ у власних інтересах в тіньовому обороті. Ф. Ціммерман – це людина, яка створила програмне забезпечення фільтрації електронної пошти. Він вважає, що корупція стає головною перешкодою до формування інтелектуального потенціалу у боротьбі з кіберзлочинністю. Адже корупція заважає вихованню патріотизму та застосування своїх знань на благо своєї країни, вона є детермінантом цинізму.

Багатьма науковцями та практиками доведено, що для нашої держави серед інших небезпек корупційні ризики створюють найсерйознішу загрозу стабільній і безпечній діяльності багатьох об'єктів критичної інфраструктури.

Значний вплив на рівень кіберзлочинності поряд з корупцією, на нашу думку, мають економічна і політична ситуації в країні, рівень еволюції суспільства, його розвитку та освіченості, доступність до технологій та мереж [6].

Чинники пов'язані з віктимною поведінкою потерпілих виявляються в відсутності у більшості населення належної культури поведінки в поводжені з комп'ютерною технікою. Це проявляється в економії потерпілих на системах програмного і технічного захисту інформації (відсутність антивірусних програм, брандмауерів; недооцінка оновлення програм захисту; використання неліцензійного програмного забезпечення), порушенні загальних правил роботи з інформацією в мережі (відсутність резервних копій важливої інформації, порушення своєї анонімності, застосування виробничого комп'ютера для невідповідних цілей), ігнорування вимог, направлених на збереження конфіденційної інформації (відсутність локальних нормативних актів поводження з комп'ютерною технікою на підприємстві, відсутність нагляду за персоналом, що має доступ до важливої інформації, недосконаліть парольної системи захисту від несанкціонованого доступу до робочої станції та її програмного забезпечення, яка не передбачає достовірної ідентифікації користувача за індивідуальними біометричними параметрами), порушення інших правил (ведення публічного особистого життя), а також неповідомлення потерпілими про вчинення кіберзлочинів [7].

Що стосується причин кіберзлочинів саме в банківській сфері. Початок цифрової економіки несе в собі стрімкий розвиток інформаційних та комунікаційних технологій, нових викликів зі сторони FinTech-компаній, а також глобалізаційних процесів. Під Fintech розуміється програмне або технологічне нововведення у фінансових послугах. Компанії, що працюють в цій сфері, зазвичай намагаються поліпшити існуючу фінансову інфраструктуру або створити нову. Банківський сектор активно впроваджує нові інновації та передові технології, що орієнтовані на комфортність користування послугами їх клієнтами. Серед нових тенденцій можна виокремити використання електронних платежів, перехід на хмарні технології, нові способи аутентифікації, автоматизація процесів для виявлення проблем та мінімізації збитків від шахрайств тощо [8].

Всі банки вимушені бути в курсі всіх актуальних останніх подій та інновацій в цифровому банкінгу для якісного обслуговування клієнтів. Це в свою чергу стимулює покращення кібербезпеки для оптимізації введених технологій. Використання предиктивної аналітики дозволяє проводити кредитний скоринг більш точно й ефективніше управляти ризиками, знижуючи витрати і підвищуючи прибутковість кредитування. Перехід даних, інфраструктури та процесів у гібридну хмару забезпечує безпеку даних із застосуванням firewall – це задовольняє виконання вимог конфіденційності та локального законодавства. Використання гібридної моделі хмарного сервісу (поєднання публічної хмари і приватної хмари з розмежуванням доступу до даних і додатків) надає банкам більше можливостей для оптимізації бюджетів, скорочуючи витрати на обслуговування, дозволяючи проводити швидкі зміни в продуктах і сервісах, дотримуючись при цьому високих стандартів безпеки. Конкретне рішення має ґрунтуватися на існуючих компетенціях банку, баченні акціонерів та менеджменту та глибокому аналізі перспектив ринку та конкурентного середовища [9].

Одна з головних проблем при впровадженні цифрових технологій в банківському секторі – вимагає значних інвестицій. Окрім кадрових проблем існує і зовнішня проблема кібербезпеки банківських систем – фінансова та інформаційна неграмотність населення, недовіра до нововведень через помилки в їх використанні.

Загроза кібербезпеки полягає в тому, що зниження контролю з боку користувачів може спричинити за собою загрозу шахрайства при розширенні цифрового сервісу та індивідуалізації безлічі видів послуг.

Ризики витоку інформації вимагають підвищення рівня захисту електронних систем. За останніми тенденціями такі злочини спрямовані на крадіжку даних з мобільних пристроїв і фінансових додатків. Чим більше буде велика сума грошових транзакції, тим вигіднішою стає крадіжка для зловмисників. Внутрішня стабільність банку включає в себе, серед іншого, достатність капіталу банку, якість активів, професіоналізм керівництва та його моральні якості, прибутковість банку, ліквідність, а також систему управління ризиками, внутрішній контроль та систему стратегічного і тактичного планування. Хоча інформаційна безпека є основою конкурентоспроможності сучасного бізнесу, за підсумками обстеження 248 українських фірм компанією PwC виявилося, що 40 % українських компаній не має стратегії інформаційної безпеки, а в 50 % компаній відсутній план реагування на інциденти інформаційної безпеки, при цьому у 48 % компаній немає програм навчання співробітників [10].

Негативна сторона полягає ще втому, що при введенні інновацій інтерес організованих злочинних угруповань до нових технологій і відсутність кордонів у кіберпросторі сприяли формуванню транснаціональної організованої кіберзлочинності. Дії зловмисників орієнтовані на отримання довгострокового доходу. Вони вже не обмежуються простим спамом або шахрайством – вони посягають на здоров'я, фінанси та базові права людини як в онлайні, так і за межами цифрового простору [11].

Обсяг даних про людину, що потребують автоматизованої обробки, буде постійно розширюватися, роблячи людину прозорою в інформаційному середовищі. Персональні дані – це новий товар, що пропонується кіберзлочинністю. Вони стали основним предметом торгівлі для шахраїв у всьому світі. Кіберзлочинні угруповання наймають талановитих програмістів для створення програмних продуктів і пропонують платні послуги, отримуючи прибутки. На думку фахівців, соціальні мережі, Інтернет-платежі, Інтернетбанкінг, віддалені сховища даних, онлайнові ігри, онлайнові біржові агенції знаходяться в числі найбільш уразливих для атак, що робить персональні дані привабливим об'єктом для злочинних посягань з боку організованої кіберзлочинності. У той же час приватні структури (особливо кредитно-фінансові) неохоче надають інформацію про кількість витоку конфіденційної інформації з їх телекомунікаційних систем та наслідки і збитки від їх використання. В результаті спостерігається надвисока латентність правопорушень в інформаційному просторі, що є одним із вагомих детермінантів зростання кіберзлочинності.

Анонімне використання Інтернету та вразливих аспектів серверів унеможливлюють виявлення злочинця, оскільки він може використовувати точки загального доступу в кафе, або ж зовсім «зламати» чужу мережу Wi-Fi тощо. Можуть бути вчинені множинні злочини, при чому злочинець здійснює їх без особливих фінансових і часових затрат. Ви можете стати однією із тисячі користувачів, у яких викрали незначні для вас кошти та просто цього не помітити, а отже і кримінального переслідування не відбудеться [12].

Висновки з даного дослідження. Отже, серед головних детермінантів можна виділити: 1) стрімкий розвиток глобальної мережі, що вже налічує сотні мільярдів документів, десятки мільйонів серверів і мільярди користувачів; 2) небувалий рівень та кількість злоякісного програмного забезпечення; 3) поява нових видів атак, їх вдосконалення (фішинг, смс-шахрайство, лже-антивіруси, кібер-шантаж, фальшиве розсилання інформації від «друзів», електронні листи з «цікавими» вкладеннями, створення бот-мереж); 4) відсутність належної державної фінансової підтримки фундаментальних і прикладних вітчизняних досліджень у сфері запобігання та боротьби з кіберзлочинністю; 5) складність організації захисту; 6) відсутність адекватного захисту даних у більшості випадків; 7) неправильне адміністрування систем; 8) наявність помилок у засобах забезпечення безпеки, а іноді й повне ігнорування необхідності їх упровадження; 9) відсутність моніторингу та аудиту; 10) складність підтримання належного стану в умовах постійних змін стандартів.

Список літератури:

1. Кочетков В.М. Забезпечення фінансової стійкості сучасного комерційного банку: теоретико-методологічні аспекти : монографія. Київ : КНЕУ, 2002. 238 с.
2. Фіщук В. Цифрова економіка – це реально. URL: http://biz.nv.ua/ukr/ (дата звернення: 17.06.2020).
3. Стратегія кібербезпеки України затверджена Указом Президента України від 5 березня 2016 року № 96. URL: http://zakon2.rada.gov.ua/laws/show/96/2016 (дата звернення: 18.06.2020).
4. Кривцова М.О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії. *Юридичний науковий електронний журнал*. 2014. № 5. С. 113–116.
5. Орлов О.В. Попередження кіберзлочинності – складова частина державної політики в Україні. *Теорія та практика державного управління*. 2014. № 1(44). С. 9–16.
6. Варналій З.С. Корупція як інституціональна загроза національній безпеці України. *Реалізація державної антикорупційної політики в міжнародному вимірі*. Матеріали II міжнар. наук.-практ. конф. Київ, 8 груд. 2017 р.
7. Бессонов Владимир Анатольевич. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации : диссертация кандидата юридических наук : 12.00.08. Нижний Новгород, 2000. С. 249.
8. Золотарьова О.В. Інноваційні банківські продукти та специфіка їх впровадження в Україні. *Науковий вісник Херсонського державного університету*. URL: http://www.ej.kherson.ua/journal/economic_16/1/29.pdf (дата звернення: 17.06.2020).
9. Васильчишин О.Б. Фінансова безпека банківської системи України: філософські детермінанти. Монографія URL: http://library.tneu.edu.ua/ (дата звернення: 17.06.2020).
10. Лисяк Л.В. Сучасний стан та основні проблем фінансової безпеки України. *Ефективна економіка*. 2017. № 4. URL: http://www.economy.nayka.com.ua/ (дата звернення: 17.06.2020).
11. Орлов О.В. Попередження кіберзлочинності – складова частина державної політики в Україні. *Теорія та практика державного управління : зб. наук. пр. ХРІДУ НАДУ*. Харків, 2014. № 1. С. 9–15.

12. Мовчан А.В. Кібернетична безпека України в умовах глобальної нестабільності. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2015. № 1(34). С. 159–163.

References:

1. Kochetkov, V.M. (2002). Zabezpechennya finansovoyi stiykosti suchasnoho komertsiynoho banku: teoretyko-metodolohichni aspekty [Ensuring the financial stability of a modern commercial bank: theoretical and methodological aspects]. Kyiv: KNEU. (in Ukrainian)
2. Fishchuk, V. Tsyfrova ekonomika – tse real'no [The digital economy is real]. URL: http://biz.nv.ua/ukr/ (accessed 17.06.2020).
3. Stratehiya kiberbezpeky Ukrayiny vid 5 bereznya 2016 roku № 96. URL: http://zakon2.rada.gov.ua/laws/show/96/2016 (accessed 18.06.2020).
4. Kryvtsova, M.O. (2014). Faktory determinatsiyi kiberzlochynnosti v suchasniy kryminolohichniy teoriyi [Factors in determining cybercrime in modern criminological theory]. *Yurydychnyy naukovyy elektronnyy zhurnal* [Legal scientific electronic journal], no. 5, pp. 113–116.
5. Orlov, O.V. (2014). Poperedzhennya kiberzlochynnosti – skladova chastyna derzhavnoyi polityky v Ukrayini [Cybercrime prevention is an integral part of public policy in Ukraine]. *Teoriya ta praktyka derzhavnoho upravlinnya* [Theory and practice of public administration], no. 1(44), pp. 9–16.
6. Varnaliy, Z.S. (2017). Koruptsiya yak instytutsional'na zahroza natsional'niy bezpetsi Ukrayiny [Corruption as an institutional threat to Ukraine's national security]. *Proceedings of the realizatsiya derzhavnoyi antykoruptsiynoyi polityky v mizhnarodnomu vymiri Ukraine*. Kyiv, 8 December 2017 r.
7. Bessonov, V.A. (2000). Vyktymolohycheskye aspekty preduprezhdenyya prestuplenyy v sfere komp'yuternoy ynformatsyy [Victimological aspects of computer crime prevention] dyssertatsyya kandydata yurydycheskykh nauk [PhD thesis]. Nyzhnyy Novhorod.
8. Zolotar'ova, O.V. (2016). Innovatsiyni bankivs'ki produkty ta spetsyfika yikh vprovadzhennya v Ukrayini [Innovative banking products and the specifics of their implementation in Ukraine]. *Naukovyy visnyk Khersons'koho derzhavnoho universytetu* [Scientific Bulletin of Kherson State University]. URL: http://www.ej.kherson.ua/journal/economic_16/1/29.pdf (accessed 17.06.2020).
9. Vasyl'chyshyn, O.B. (2017). Finansova bezpeka bankivs'koyi systemy Ukrayiny: filosofs'ki determinant [Financial security of the banking system of Ukraine: philosophical determinants]. URL: http://library.tneu.edu.ua/ (accessed 17.06.2020).
10. Lysyak, L.V. (2017). Suchasnyy stan ta osnovni problem finansovoyi bezpeky Ukrayiny [Current state and main problems of financial security of Ukraine]. *Efektyvna ekonomika* [An efficient economy], no. 4. URL: http://www.economy.nayka.com.ua/ (accessed 17.06.2020).
11. Orlov, O.V. (2014). Poperedzhennya kiberzlochynnosti – skladova chastyna derzhavnoyi polityky v Ukrayini [Cybercrime prevention is an integral part of public policy in Ukraine]. *Proceedings of the Teoriya ta praktyka derzhavnoho upravlinnya.* Kharkiv: KhRIDU NADU, no. 1, pp. 9–15.
12. Movchan, A.V. (2015). Kibernetychna bezpeka Ukrayiny v umovakh hlobal'noyi nestabil'nosti [Cyber security of Ukraine in the conditions of global instability]. *Borot'ba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka)* [Fight against organized crime and corruption (theory and practice)], no. 1(34), pp. 159–163.