DOI: 10.18372/2307-9061.54.14553
УДК 346.7(045)

В. П. Козирєва,
кандидат юридичних наук, доцент

А. П. Гаврилішин,
кандидат юридичних наук, доцент

КІБЕРПРАВОПОРУШЕННЯ ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ

Національний авіаційний університет
проспект Космонавта Комарова, 1, 03680, Київ, Україна
Університет державної фіскальної служби України
вул. Університетська, 31, 08201, Ірпінь, Київська область, Україна
E-mails: kozurevav@ukr.net, gavrilishinap@gmail.com

Мета: *розглядаються об'єктивні фактори, що випливають із специфіки кіберправопорушень, загрози та їх негативний вплив на економічну безпеку держави, характеризуються кримінальні правопорушення у сфері банківських платіжних карток, ознаки, які відрізняють кіберзлочини від інших кримінальних правопорушень, наводяться визначення «кіберзлочину», аналізується система кібернетичної безпеки, яка має ґрунтуватися на певних принципах, об'єктах і суб'єктах, які її забезпечують.* ***Методи:*** *дослідження проведене з використанням таких методів як аналіз, синтез, порівняння.* ***Результати:*** *зроблено висновок, що кіберправопорушення несуть загрози економічній безпеці України, тому на законодавчому рівні здійснюються заходи щодо запобігання та протидії таким проявам.* ***Обговорення:*** *проблеми забезпечення кібербезпеки та запобігання кіберпавопорушенням в економічній сфері.*

Ключові слова: *кібербезпека; економічна безпека; кіберправопорушення; кіберзлочин.*

Постановка проблеми та її актуальність. Сучасний стан глобалізаційних процесів у світі детермінує умови для переходу українського суспільства до нової стадії розвитку – інформаційної.

Широке використання сучасних інформаційних технологій у господарських відносинах висуває вирішення проблем економічної безпеки суспільства на перше місце. На даний час кількість правопорушень, що здійснюються в галузі господарювання, зростає пропорційно кількості користувачів комп'ютерних мереж. Таке зростання є неминучим процесом як розвитку інформаційних технологій, так і удосконаленням професіоналізму правопорушників у сфері економічних відносин.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», який вступив у дію з 05.04.2018 р., визначаються правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі.

Тому одним із пріоритетних завдань держави є вироблення та вдосконалення правових основ для дієвого запобігання та припинення правопорушень у сфері інформаційних технологій, захист електронної інформації в комп'ютерних системах та телекомунікаційних мережах для забезпечення економічної, політичної, військової та інших сфер життя суспільства.

У зв'язку з чим створення адекватних заходів протидії кіберправопорушенням є однією із найбільш актуальних проблем українського законодавства.

Аналіз останніх досліджень і публікацій.

Питанням правової відповідальності за вчинення правопорушення з використанням комп'ютерних технологій приділяється значна увага в сучасній правовій науці України. Серед науковців, які працюють у цьому напрямку, можна виділити праці Д.С. Азарова, А.А. Васильєва, В.О. Голуб'єва, О.П. Чорпинюка, О.Д. Довгань, О.О. Дудорова, М.В. Карчевського, Д.Ю. Кондратюка, В.В. Кузнєцова, А.А. Музики, С.О. Орлова, Н.А. Розенфельда, К.В. Юртаєва та інші.

Разом з тим питання безпеки держави у протидії кіберправопорушенням потребує подальшого наукового вивчення.

Мета статті. Аналіз правових засад запобігання та припинення правопорушень у сфері економічної безпеки з використанням комп'ютерних мереж та інформаційних технологій.

Виклад основного матеріалу. Втілення в життя комп'ютерних технологій з величезними можливостями призвело до комп'ютеризації господарської й управлінської діяльності, також інших сфер життя суспільства, в яких порушення нормальної роботи такої техніки може понести величезні економічні збитки. Загроза для користувачів у сфері комп'ютеризації детермінується тим, що «користувач не тільки одержує можливість доступу до різних інформаційних серверів цієї мережі, а й створює канал для доступу до свого комп'ютера» [1].

Конвенція Ради Європи про кіберзлочинність звертає увагу на те, що комп'ютерні мережі та електронна інформація можуть використовуватися для вчинення кримінальних правопорушень [2].

Складність поставлених завдань обумовлюється об'єктивними факторами, що пов'язані зі специфікою кіберправопорушень. Як зазначає К.В. Юртаєва, до них відносяться:

– транскордонний характер комп'ютерних правопорушень;

– неузгодженість юрисдикційних актів протидії кіберправопорушенням (позитивні і негативні конфлікти кримінальних юрисдикцій);

– постійне вдосконалення злочинних засобів та методів вчинення кіберправопорушень;

– орієнтація кримінального і кримінального процесуального законодавства на традиційні моделі вчинення та поширення правопорушень;

– складність та суперечливість процесу кваліфікації правопорушень;

– недоліки кримінального процесуального законодавства щодо отримання, фіксації та дослідження електронних правопорушень [3, с. 221].

Інші автори виділяють внутрішні негативні фактори, які впливають на інформаційну безпеку України. До таких факторів відносять:

– неефективність державної інформаційної політики, в тому числі відсутність цілісної комунікативної політики як всередині держави, та і у зовнішніх зносинах;

– неналежний стан національного законодавства з питань інформаційної безпеки України, відсутність концептуальних правових засад її забезпечення, надто повільні темпи проведення відповідних реформ;

– відсутність належної координації діяльності суб'єктів забезпечення інформаційної безпеки, дублювання їх функцій, а також недостатньо ефективне співробітництво державних установ із громадянським суспільством;

– неефективне управління безпекою юридичної інфраструктури, уразливість до кібератак її об'єктів та державних інформаційних ресурсів, критична знаменність її основних фондів та недостатній рівень їх фізичного захисту;

– відсутність комплексної системи підготовки фахівців у закладах вищої освіти для сфери інформаційної безпеки України, зокрема, за напрямом протидії негативним інформаційним впливом [4].

Слід погодитися з поглядами тих авторів, які відмічають, що значимість проблеми захисту інформаційних ресурсів зумовлена такими чинниками:

– розвитком світових і національних відкритих ком'ютерних мереж та нових інформаційно-комунікаційних технологій, що забезпечують легкий доступ до інформаційних ресурсів;

– переведення усе більшої частини інформаційного ресурсу з паперових на електронні носії та концентрацію її у різних інформаційних системах;

– розробленням та постійним удосконаленням інформаційних технологій, що можуть ефективно

використовуватися для кримінального проникнення в комп'ютери, підключені до відкритих і навіть захищених мереж [5].

Н.А. Розенфельд виділяв такі загрози безпеці даних у комп'ютерній системі:

– розкриття змісту повідомлень, що передаються;

– аналіз трафіку, що дозволяє визначати належність відправника і одержувача даних до однієї з груп користувачів мережі, пов'язаних спільними завданнями;

– зміна потоку повідомлень, що може призвести до порушення режиму роботи будь-якого об'єкта, керованого з віддаленої ЕОМ;

– неправомірна відмова в наданні послуг;

– несанкціоновані з'єднання [6, с. 20].

Разом із тим, процеси глобалізації інформаційних технологій згладжують кордони між територіями держав та надають необмежені можливості для вчинення будь-якого впливу на особу та суспільство і як негативний наслідок стала поява нового виду правопорушень кіберзлочинності. Термін «кіберзлочинність» був уведений на десятому конгресі ООН з попередження злочинності та поводження із правопорушниками і охоплює будь-який злочин, учинений в електронному середовищі [7].

Ми підтримуємо тих авторів, які під кіберзлочинністю розуміють, що це сукупність злочинів, учинених у кіберпросторі за допомогою або опосередкованим використанням комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, у межах комп'ютерних систем або мереж, а також проти комп'ютерних мереж і комп'ютерних даних [8, с. 178].

Кіберзлочини у сучасному суспільстві набирають загрозливого характеру. Відтепер успішна атака хакерів може знеструмити цілу область чи державу, пограбувати банк чи знищити успішну організацію, проникнути в державну, військову чи комерційну таємницю, заблокувати комп'ютерні мережі.

Сучасні технології не тільки дали поштовх вільній торгівлі, глобалізації та віртуалізації економічної діяльності, а й стимулювали злочинну діяльність. У зв'язку з чим стратегія забезпечення кібербезпеки України потребує корегування відповідно до нових викликів та загроз, а також змін у геополітичному безпековому середовищі [9].

Практика свідчить, що за останній час виникли нові способи вчинення економічних правопорушень з використанням інформаційних технологій. За даними досліджень міжнародної аудиторської компанії Price waterhouse Coope з 2011 року кіберзлочинність стала одним із п'яти найпоширеніших економічних злочинів в Україні. Потенційні хакери мають можливість за декілька хвилин зняти готівку з рахунків у банках на сотні тисяч гривень за допомогою платіжних систем Visa та Master Card [10].

Залежно від того, як відбуваються злочини у сфері платіжних карток (за критерієм об'єктивної сторони) їх можна класифікувати на три групи:

– злочини, які пов'язані з незаконним зберіганням інформації про платіжні картки. До них належать:

– створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут (скіммінг, використання шкідливих програмних засобів у банкоматах, зокрема комп'ютерних вірусів, програм, призначених для нейтралізації паролів, програм – шпигунів) – ст. 361-1 КК України;

– несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислюваних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (службові злочини уповноважених осіб банківських установ та інших осіб, що мають доступ до такої інформації при вступ ними у злочинну змову із зловмисником) – ст. 361-2 КК України;

– незаконне збирання з метою використання відомостей, що становлять комерційну або банківську таємницю (так званий фітинг інтернет-шахрайство, спрямоване на отримання конфіденційних даних шляхом проведення масових розсилок від імені банків або інших установ. У листах часто є посилання на сайт із редиректом, на якому пропонується ввести свої персональні дані, які відкривають шлях злочинцям до

банківських рахунків;

– злочини, пов'язані з підробленими платіжними картками:

– незаконні дії з документами на переказ платіжними картками та іншими засобами доступу до банківських рахунків, обладнання для їх виготовлення (ст. 200 КК України).

Під незаконними діями в цій статті розуміється підробка документів на переказ платіжних карток чи інших засобів доступу до банківських рахунків, а так само їх придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ чи платіжних карток або їх використання чи збут.

Необхідно зазначити, що 18.09.2012 р. вступив у дію Закон України «Про внесення змін до деяких законодавчих актів України» щодо гуманізації відповідальності за правопорушення в сфері господарської діяльності. Відповідно до закону за вчинення злочинів, передбачених статтями 200, 231 КК України, встановлений один вид покарання – штраф. Альтернативні покарання, такі як обмеження волі, позбавлення волі на певний строк, відсутні, хоча у старих редакціях зазначених статей вони були достатньо дієвими.

У зв'язку з чим, територія України стала привабливою для іноземних правопорушників, так як у державах Європи передбачені більш суворі види покарання. Наприклад, стаття 310 КК Польщі – 25 років позбавлення волі, статті 396, 387 КК Іспанії – 8 років позбавлення волі.

Виникає цікава ситуація – іноземний правопорушник, сплативши штраф на суму 51 тисяча гривень, зможе спустошувати українські банкомати на сотні тисяч гривень;

злочини із використанням платіжних карток (їх реквізитів). До них належать: використання викраденої, втраченої картки, використання незаконно отриманих реквізитів справжньої картки. Такі протиправні дії за українським законодавством є корисливими, носять матеріальний склад та залежно від обставин справи кваліфікуються за двома статтями КК України як крадіжка (ст. 185) та шахрайство (ч. 2, 3 ст. 190).

Кіберзлочини не знають державних кордонів, мають організований, транскордонний характер, що ускладнює проведення як розшукових, так і процесуальних заходів. Все це вимагає уніфікації національного законодавства, на що спрямована конвенція Ради Європи про кіберзлочинність 2001 року та ратифікована Верховною Радою України в 2005 році.

Іноземні науковці виділяють такі ознаки кіберзлочинів, які відрізняють їх від традиційних кримінальних правопорушень та значно підвищують суспільну небезпечність. До них належать:

– по-перше, не мають фізичного зближення між жертвою та суб'єктом злочину в момент вчинення правопорушення;

– по-друге, кіберзлочини є «автоматизованими злочинами», що дає можливість злочинцю вчинити від декількох до безлічі протиправних дій;

– по-третє, суб'єкт кіберзлочину не має обмежень, які існують у реальному фізичному світі. Кіберзлочини можуть вчинятися раптово, а тому потребують швидкої реакції у відповідь;

– по-четверте, кіберзлочини і на сьогодення залишаються феноменом, тому наука ще не взмозі зреагувати належним чином на ті чи інші моделі кіберзлочинів [11, с. 33].

Слід погодитися з думкою про те, що найбільш суттєвою характеристикою Інтернету з точки зору юрисдикційної політики є те, що він стирає межу між внутрішньодержавною та міжнародною передачею інформації [12, с. 434].

У науковій літературі виділяють наступні підстави, відповідно до яких суди різних держав світу встановлюють свою територіальну юрисдикцію щодо злочинів із використанням комп'ютерних мереж:

– місце вчинення злочинного діяння;

– місце знаходження комп'ютера (діяння залежить від того, на території якої держави він знаходиться);

– місце знаходження осіб (суб'єкт злочину або потерпіла особа знаходяться на території якої держави);

– місце настання суспільно небезпечного наслідку (істотний шкідливий наслідок діяння настає на території держави) – принцип об'єктивної територіальності;

– місце знаходження будь-якої з перерахованих підстав, у тому числі й транзит інформації через територію держави [13, с. 10-21].

А яка ситуація із кіберправопорушеннями в Україні? Слід зазначити, що в КК України відсутнє визначення поняття «кіберправопорушення». В Особливій частині КК України міститься розділ XVI, який має назву «Злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Певною мірою зміст цього розділу КК України відповідає положенням Конвенції Ради Європи про кіберзлочинність 2001 року. Разом із тим до останнього часу в законодавчому плані визначення поняття «кіберзлочин» не було наведено.

З метою усунення цієї прогалини Верховною Радою України 05.10.2017 р. був прийнятий Закон «Про основні засади забезпечення кібербезпеки України», який вступив у дію 05.04.2018 р. У п. 8 ст. 1 цього закону наведено наступне визначення кіберзлочину: «кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачено законом України про кримінальну відповідальність та/або яке визначено злочином міжнародними договорами України», а у п. 9. кіберзлочинність визначається як сукупність кіберзлочинів.

Виходячи із вище зазначеного визначення можна говорити про те, що комп'ютерні злочини – це не тільки злочини, передбачені розділом XVI Особливої частини КК України (п'ять складів), а й інші злочини, при вчиненні яких використовувалися комп'ютери та комп'ютерні системи. Зауважимо також про те, що в п. 14 Доповіді комітету II Десятого Конгресу ООН 2000 року по попередженню злочинності і поводженню з правопорушниками було виділено два види кіберзлочинів:

– кіберзлочини у вузькому розумінні (комп'ютерні злочини): будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і обчислюваних ними даних;

– кіберзлочини у широкому розумінні (злочини з використанням комп'ютерів) – будь-яке протиправне діяння, яке вчиняться шляхом або у зв'язку з комп'ютерною системою або у зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [14, с. 338].

У науковій літературі є і таке визначення кіберзлочинності – це сукупність злочинів, учинених у кіберпросторі за допомогою або опосередкованим використанням комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору в межах комп'ютерних систем або мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [15, с. 178].

Ми підтримуємо думку авторів і зазначаємо, що їх визначення кіберзлочинності значно ширше, ніж це зазначено в законі.

Для успішної протидії кіберзлочинам в Україні відбувається процес формування системи кібернетичної безпеки, і як будь-яка система вона ґрунтується на певних принципах та має відповідні об'єкти та суб'єкти, які її забезпечують. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень здійснюється на наступних принципах: мінімально необхідного регулювання; об'єктивності та правової визначеності; максимально позитивного застосування національного та міжнародного права; забезпечення захисту прав користувачів комунікаційних систем та споживачів послуг електронних комунікацій; прозорості, згідно з яким рішення суб'єктів владних повноважень мають бути належним чином обґрунтовані; збалансованості вимог та відповідальності; недискримінації, тощо [16, ст. 2].

Об'єктами кібербезпеки та кіберзахисту є: конституційні права та свободи людини і громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканість; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; комунікаційні системи всіх форм власності, які використовуються для задоволення суспільних потреб та реалізації правовідносин у сфері електронного урядування, електронних державних послуг, еле-

ктронної комерції, електронного документообігу [16, ст. 4].

Суб'єктами, які безпосередньо здійснюють у межах своїх повноважень заходи із забезпечення кібербезпеки, виступають: центральні виконавчі органи та органи місцевого самоврядування; правоохоронні, розвідувальні і контрозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Національний банк України, суб'єкти господарювання тощо [16, ст. 5].

Висновки. Таким чином в Україні на законодавчому рівні встановлені заходи щодо забезпечення кібербезпеки у всіх сферах життя суспільства, в тому числі в економічній сфері. Прояви кримінального використання високих інформаційних технологій у економічній безпеці суспільства є одним із головних напрямів протидії прояву кіберзлочинності в державі.

Кібербезпека має бути постійним процесом діяльності відповідних державних органів із запобігання та протидії загрозам кіберпростору України. Вона має ґрунтуватися на принципах: верховенства права; забезпечення балансу прав та інтересів людини, громадянина, держави; взаємодії державних органів та громадськості. На підставі викладеного пропонуємо визначити кіберправопорушення у сфері економічної безпеки як систему кіберправопорушень, які посягають на життєво важливі суспільні відносини в економічній сфері з використанням комп'ютерних систем та комп'ютерних технологій.

Література

1. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности. URL: http://www.ztb.

2. Про кіберзлочинність: Конвенція Ради Європи. *Офіційний вісник України*. 2007. № 65. Ст. 2535. С. 107.

3. Юртаєва К.В. Проблеми криміналізації незалежного використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем чи їх частин. *Ф. П.* 2017. № 3. С. 221-227.

4. Довгань О.Д. Інформаційна безпека: стан, проблеми, тенденції. URL: http:fsp.kpi.ua › faculty › dovhan.

5. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности. URL: http://www.ztb.

6. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж): дис. … канд. юрид. наук: 12.00.08. Київ, 2003. 20 с.

7. Преступления, связанные с использованием компьютерной сети. Десятый конгресс ООН по предупреждению преступности и обращения с правонарушителями. URL: http://www.un.org/russian/topics/crime/

8. Пивоваров В.В., Лисенко С.Ю. Кіберзлочинність: кримінально логічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. Харків, 2015. № 3. С. 177-182.

9. Національний інститут стратегічних досліджень. 05 лип. 2018 р. URL: http://www.niss.gov.ua/artiecles/1919/.

10. Всесвітній огляд економічних злочинів. Кіберзлочини в центрі уваги. URL: https://www.pwc.com/ua/uk/press-room/ assets/gecs_ukraine_ua.pdf.

11. Brenner S.W. Toward a Criminal law Enforcement? 30 Rutgers Computer Tech. L./. 1 (2004).

12. Stein A.R. Sumposium: Persenal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision. 98. Nw U. L. Rew. 411 (2004).

13. Brenner S.W., Koops B.J. Approaches to Cybercrime Jurisdiction. 4. G. High Tech L. I. (2004).

14. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: ООО «Издво «Юрлитинформ». 2002. 496 с.

15. Пивоваров В.В., Лисенко С.Ю. Кіберзлочинність: кримінально логічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. 2016. № 3. С. 177-181.

16. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

References

1. Smolyan G.L. Setevye informacionnye tehnologii i problemy bezopasnosti. URL: http://www.ztb.

2. Pro kiberzlochinnist: Konvenciya Radi Yevropi. *Oficijnij visnik Ukrayini*. 2007. № 65. St. 2535. S. 107.

3. Yurtayeva K.V. Problemi kriminalizaciyi nezalezhnogo vikoristannya komp'yuternih paroliv, kodiv dostupu abo podibnih danih, yaki nadayut dostup do komp'yuternih sistem chi yih chastin. F. P. 2017. № 3. S. 221-227.

4. Dovgan O.D. Informacijna bezpeka: stan, problemi, tendenciyi. URL: http:fsp.kpi.ua › faculty › dovhan.

5. Smolyan G.L. Setevye informacionnye tehnologii i problemy bezopasnosti. URL: http://www.ztb.

6. Rozenfeld N.A. Kriminalno-pravova harakteristika nezakonnogo vtruchannya v robotu elektronno-obchislyuvalnih mashin (komp'yuteriv, sistem ta komp'yuternih merezh): dis. … kand. yurid. nauk: 12.00.08. Kiyiv, 2003. 20 s.

7. Prestupleniya, svyazannye s ispolzovaniem kompyuternoj seti. Desyatyj kongress OON po preduprezhdeniyu prestupnosti i obrasheniya s pravonarushitelyami. URL: http://www.un.org/ russian/ topics/crime/

8. Pivovarov V.V., Lisenko S.Yu. Kiberzlochinnist: kriminalno logichnij poglyad na genezis yavisha ta shlyahi zapobigannya. *Pravo i suspilstvo*. Harkiv, 2015. № 3. S. 177-182.

9. Nacionalnij institut strategichnih doslidzhen. 05 lip. 2018 r. URL: http://www.niss. gov.ua/ articles/1919/.

10. Vsesvitnij oglyad ekonomichnih zlochiniv. Kiberzlochini v centri uvagi. URL: https://www.pwc.com/ua/uk/press-room/assets/gecs_ ukraine_ua.pdf.

11. Brenner S.W. Toward a Criminal law Enforcement? 30 Rutgers Computer Tech. L./. 1 (2004).

12. Stein A.R. Sumposium: Persenal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision. 98. Nw U. L. Rew. 411 (2004).

13. Brenner S.W., Koops B.J. Approaches to Cybercrime Jurisdiction. 4. G. High Tech L. I. (2004).

14. Volevodz A.G. Protivodejstvie kompyuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva. Moskva: OOO «Izd-vo «Yurlitinform». 2002. 496 s.

15. Pivovarov V.V., Lisenko S.Yu. Kiberzlochinnist: kriminalno logichnij poglyad na genezis yavisha ta shlyahi zapobigannya. *Pravo i suspilstvo*. 2016. № 3. S. 177-181.

16. Pro osnovni zasadi zabezpechennya kiberbezpeki Ukrayini: Zakon Ukrayini vid 05 zhovt. 2017 r. *Vidomosti Verhovnoyi Radi Ukrayini*. 2017. № 45. St. 403.

V. Kozireva, A. Gavrilishin

CYBER OFFENSE AS A THREAT TO ECONOMIC SECURITY OF UKRAINE

National Aviation University
Kosmonavta Komarova Avenue, 1, 03680, Kyiv, Ukraine
University of the State Fiscal Service of Ukraine
Universitetska str., 31, 08200, Irpin', Kyiv region, Ukraine
E-mails: kozurevav@ukr.net, gavrilishinap@gmail.com

***Purpose**: the objective factors arising from the specificity of cybercrime, threats and their negative impact on the economic security of the state are considered, criminal offenses in the field of bank payment cards are characterized, features that distinguish cybercrime from other criminal offenses, the definition of «cybercrime» a cyber security system that must be based on certain principles, objects and entities that provide it. **Methods:** the study was conducted using methods such as analysis, synthesis, comparison. **Results**: it is concluded that cybercrime poses a threat to Ukraine's economic security, so measures are taken at the legislative level to prevent and counteract such manifestations. **Discussion**: cybersecurity issues and prevention of cybercrime in the economic sphere.*

The widespread use of modern information technology in economic relations puts the solution of problems of economic security of society in the first place. Currently, the number of offenses committed in the industry is increasing in proportion to the number of users of computer networks. Such growth is an inevitable process for both the development of information technology and the improvement of the professionalism of offenders in the sphere of economic relations.

In Ukraine, measures are being put in place at the legislative level to ensure cybersecurity in all spheres of society, including in the economic sphere. The manifestations of criminal use of high information technologies in the economic security of society is one of the main directions of counteracting cybercrime in the country.

Cybersecurity should be an ongoing process for the activities of relevant government agencies to prevent and counteract cyberspace threats to Ukraine. It should be based on the principles of: the rule of law; ensuring the balance of rights and interests of a person, citizen, state; interaction between government agencies and the public. On the basis of the foregoing, we propose to identify cybercrime in the field of economic security as a system of cybercrime that encroaches on vital public relations in the economic sphere using computer systems and computer technologies.

***Keywords**: cybersecurity; economic security; cybercrime; cybercrime.*