УДК 342.1
DOI https://doi.org/10.24144/2788-6018.2023.06.101

ОБ'ЄКТ ТА ПРЕДМЕТ КРИМІНАЛЬНИХ ПРАВОПОРУШЕННЬ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Замахін А.Л.,
кандидат юридичних наук,
проректор з науково-педагогічної роботи
Національного університету «Полтавська політехніка
імені Юрія Кондратюка»
email: feup.zamakhin@nupp.edu.ua
ORCID 0009-0000-9270-6278

Замахін А.Л. Об'єкт та предмет кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Стаття присвячена розгляду об'єкта та предмета комп'ютерних кримінальних правопорушень. Мета статті – дослідити об'єкт та предмет комп'ютерних кримінальних правопорушень, проаналізувати сучасний стан правового регулювання комп'ютерних кримінальних правопорушень, надати пропозиції і зауваження до законодавства.

Доведено, що в зв'язку з розвитком науково-технічного прогресу наприкінці XX сторіччя в державі виник новий тип суспільних відносин в сфері обігу комп'ютерної інформації, які в подальшому були взяти під охорону кримінального закону. Інформаційна безпека (кібербезпека) держави стала однією з складових національної безпеки України. На відміну від інших науковців ми вважаємо, що безпосереднім об'єктом комп'ютерних кримінальних правопорушень є суспільні відносини щодо забезпечення цілісності та збереження комп'ютерної інформації та безпечного функціонування інформаційних систем. Фундаментом інформаційної системи є сукупність інформаційних ресурсів у вигляді комп'ютерної інформації, комп'ютерних технологій та обладнання, а також пов'язаної з ними комп'ютерної інфраструктури, включаючи мережі електрозв'язку. Не будь-яка комп'ютерна інформація потребує кримінально-правової охорони та відповідно виступати в якості предмета комп'ютерних кримінальних правопорушень, тому законодавцю потрібно внести зміни в диспозиції статей XVI розділу Особливої частини КК України та замінити термін «інформація» на «охоронювана законом інформація». Вбачається, що обмежив в законі способи впливу на комп'ютерну інформацію законодавець надав можливості уникнути кримінальної відповідальності особам, які в інший спосіб спричиняють шкоду власникам комп'ютерної інформації.

Складність захисту правовідносин у сфері комп'ютерної інформації полягає не лише в еволюції технологій її оформлення та передачі, а й у еволюції самих правовідносин та способів впливу на них. Відсталість статей Розділу XVI КК України та проблеми кваліфікації діянь за цими статтями, які виникають в сучасної судовій практиці, не можуть знайти вирішення лише зміною диспозицій вказаних складів.

Ключові слова: кіберзлочинність, комп'ютерна інформація, кримінальна відповідальність, інформаційна безпека.

Zamakhin A.L. Object and Subject of Criminal Offenses in the Field of Use of Electronic Computers, Systems and Computer Networks and Telecommunication Networks.

The article deals with the object and subject matter of computer criminal offenses. The purpose of the article is to study the object and subject matter of computer criminal offenses, to analyze the current state of legal regulation of computer criminal offenses, and to provide suggestions and comments to the legislation.

It is proved that due to the development of scientific and technological progress at the end of the twentieth century, a new type of social relations in the field of computer information circulation emerged in the State, which were subsequently taken under the protection of criminal law. The information security (cybersecurity) of the state has become one of the components of Ukraine's national security. Unlike other scholars, we believe that the direct object of computer criminal offenses is social relations to ensure the integrity and safety of computer information and the safe operation of information systems. The foundation of an information system is a set of information

resources in the form of computer information, computer technologies and equipment, as well as related computer infrastructure, including telecommunication networks. Not all computer information requires criminal legal protection and, accordingly, can be the subject of computer criminal offenses, so the legislator should amend the dispositions of Articles XVI of the Special Part of the Criminal Code of Ukraine and replace the term "information" with "information protected by law". It seems that by limiting the ways of influencing computer information in the law, the legislator has provided opportunities to avoid criminal liability to persons who otherwise cause damage to the owners of computer information.

The complexity of protecting legal relations in the field of computer information lies not only in the evolution of technologies for its registration and transfer, but also in the evolution of legal relations themselves and the ways of influencing them. The backwardness of the articles of Section XVI of the Criminal Code of Ukraine and the problems of qualification of acts under these articles which arise in modern judicial practice cannot be solved by changing the dispositions of these corpus delicti only.

Key words: cybercrime, computer information, criminal liability, information security.

Постановка проблеми. У зв'язку із соціально-економічними змінами, що відбулися в Україні наприкінці XX ст., переходом до інформаційного суспільства, з'явився новий вид суспільних відносин – відносини у сфері обігу інформації. Інформація стала одним із необхідних елементів життя суспільства. Різні її види проникли практично у всі сфери життя. Право не залишилося осторонь змін, що відбулися: почала розвиватися нова комплексна галузь права – інформаційне право. У міру формування та розвитку інформаційного права як самостійної галузі українського права розвиватиметься у самостійну галузь юридичної науки наука інформаційного права. Виникнення нового виду відносин неминуче призводить до того, що рано чи пізно виникає потреба у їх охороні, в тому числі з застосуванням заходів кримінально-правового впливу. Рішення Ради національної безпеки і оборони України «Про стратегію національної безпеки України» наголошує завершити створення національної системи кібербезпеки, сформувати сучасні спроможності суб'єктів забезпечення кібербезпеки і кібероборони та зміцнить систему їх координації. [1]

Існуючи реалії сучасного світу такі, що інформація, інформаційні технології, комп'ютерна та інформаційно-телекомунікаційна сфери є одним із важливих факторів формування суспільства у XXI століття. Поступове впровадження цих технологій веде до розвитку інформаційних систем як технічної основи для державних органів, науково-дослідних організацій, промислових підприємств, банків та кредитної та фінансової діяльності в цілому. До того ж життя сучасної людини неможливо уявити без смартфона, планшета та інших електронних пристроїв. Варто зрозуміти всю значущість цього процесу у сучасному світі, оскільки розвиток і застосування нових технологій тягне за собою появу способів несанкціонованого доступу до них, порушення інформаційної безпеки. На тлі широкомасштабного вторгнення рф на територію України слова «інформаційна безпека» ототожнюються з національною безпекою – ключовою умовою існування України як незалежної держави. Діджиталізація багатьох сторін суспільного життя полегшує це життя, але в той же час створює чималі можливості для ворога. Протиправні втручання до комп'ютерних мереж та мереж електрозв'язку можуть призвести не лише до колосальних фінансових витрат, а й вплинути на діяльність Збройних Сил України, що може призвести до загибелі людей. Не викликає сумнівів, що кіберзлочинність має високу ступень суспільної небезпечності.

Стан опрацювання. Питання кваліфікації комп'ютерних кримінальних правопорушень перебували в сфері наукових інтересів та знайшли своє відображення в наукових працях Д.С. Азарова [2], П.П. Андрушка [3], В.М. Бутузова [4], М.В. Карчевського [5], О.К. Мазуренка [6], С.О. Орлова [7], О.Є. Радутного [8], Н.А. Розенфельда [9] та інших. В той же час серед вказаних авторів не має єдиної точки зору щодо об'єкту комп'ютерних кримінальних правопорушень, також вони неоднаково трактують предмет цих правопорушень.

Методологічну основу дослідження становить сукупність загальнонаукові методи та підходи пізнання, на які спирається правова наука. Серед них були використані: діалектичний метод, історико-правовий (історичний), формально-логічний (догматичний), порівняльно-правовий (компаративний) та статистичний метод. Діалектичний метод надав можливості, використовуючи категоріальний апарат діалектики, дослідити складові суспільних відносин, як об'єкта кримінального правопорушення, історико-правовий (історичний) в сукупності з методом порівняльного правознавства дозволив прослідити еволюцію поняття предмет кримінального правопорушення від матеріалістичного розуміння до конструювання моделі в тому числі й з віртуальним предметом (інформацією). Формально-логічний (догматичний) метод дозволив зробити висновок, що інформація є не лише предметом кримінального правопорушення, а й складовою суспільних відносин, які взяти під охорону кримінальним законом. Порівняльно-правовий (компаративний) метод дав змогу виділити загальні способи впли-

ву на комп'ютерну інформацію. Опанування статистичного методу стало в нагоді при відслідковуванні росту числа комп'ютерних кримінальних правопорушень за останні шість років.

Мета статті – дослідити об'єкт та предмет комп'ютерних кримінальних правопорушень, проаналізувати сучасний стан правового регулювання комп'ютерних кримінальних правопорушень, надати пропозиції і зауваження до законодавства.

Виклад основного матеріалу. В даний час комп'ютерна злочинність (кіберзлочинність) стала реальністю життя. За статистичними даними Офісу Генерального прокурора України за останні шість років збільшується їх питома вага збільшується так у 2018 р. за розділом XVI КК України було відкрито 2031 кримінальних провадження, 2019 р. – 2204, 2020 р. - 2498, 2021 р. – 3310, 2022 р. – 3168, за січень – жовтень 2023 р. – 3495 [10]

Висока суспільна небезпека кіберзлочинності не викликає сумнівів і полягає в наступному:

- при використанні невеликих ресурсів для їх вчинення може бути завдано величезної шкоди різноманітним об'єктам кримінально-правової охорони;

– суспільно небезпечні наслідки можуть бути виявлені не відразу та не завжди;

– кримінальне правопорушення може бути вчинено в одній юрисдикції, а правопорушник може бути під іншою юрисдикцією (як правило, комп'ютерні кримінальні правопорушення носять транснаціональний, організований характер);

– вони мають високу латентність, тому що ймовірність їх виявлення досить низька;

– потрібні особливі заходи запобігання та профілактики вчинення цих кримінальних правопорушень, оскільки багато традиційних превентивних заходів не працюють.

На XI Конгресі ООН із запобігання злочинності та кримінальному правосуддю, що відбувся у квітні 2005 року, злочинності, пов'язаної з використанням комп'ютерів, було приділено особливу увагу. У рекомендаціях, підготовлених до Конгресу, експерти ООН говорять про особливий характер кіберзлочинності та необхідність застосування комплексних підходів у боротьбі з нею, а також про невідкладні заходи щодо оновлення кримінального законодавства держав-учасниць ООН, таких як уточнення або вилучення норм, що не відповідають ситуації, що склалася. або прийняття норм щодо нових видів кіберзлочинів. Результатом діяльності Конгресу стала Бангкокська декларація, [11] в якій наголошується, що в період глобалізації швидкий розвиток інформаційних технологій та нових систем телекомунікацій та комп'ютерних мереж супроводжується зловживаннями цими технологіями у злочинних цілях, а також наголошується на необхідності розробки національних заходів та розвитку міжнародного співробітництва з протидії кіберзлочинам.

Як відомо, єдиною підставою для притягнення особи до кримінальної відповідальності є вчинення особою суспільно небезпечного діяння, яке містить склад кримінального правопорушення. Склад кримінального правопорушення, як наукова логіко-юридична абстракція вищого рівня, [12, с. 637] що містить в собі чотири обов'язкових елемента (об'єкт, об'єктивна сторона, суб'єкт і суб'єктивна сторона) знаходиться в основі найголовнішого положення кримінального права - злочинність та караність діяння визнається лише чинним кримінальним законом тим самим реалізуючи принцип nullum crimen sine lege.

Важливу роль в складі кримінального правопорушення займає об'єкт. [13, с. 91-97] Науковці по різному трактують це поняття: цінність, благо, інтерес, навіть людина але найбільш усталеною точкою зору є визначення об'єкта в якості суспільних відносин, що охороняються кримінальним законом та яким кримінальне правопорушення спричиняє шкоди або ставить в реальну загрозу спричинення шкоди. [14, с. 262-269] Враховуючи, що найменування розділів Особливої частини КК України містять у собі перелік однорідних суспільних відносин, що захищаються кримінальним законом – об'єктів кримінальних правопорушень, то відносини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є одним із них. Досвід правозастосовної практики у сфері захисту цих відносин та їх об'єкта налічує вже понад двадцять років. Тим не менш, під час проведення кримінально-правової експертизи матеріалів кримінальних проваджень і вироків часто можна спостерігати помилкову кваліфікацію діянь, під час яких використовувалися ті чи інші комп'ютерні технології. Ми вважаємо, що це явище пов'язане не з кваліфікацією правозастосовника, як іноді прийнято стверджувати, але викликане наявною в законі дефініцією самого об'єкта злочину, способами опису складів діянь і тим, як це співвідноситься з іншими нормами вітчизняного законодавства, регулюванням правовідносин, що захищаються, і технічними. злочини. Розглянемо докладніше, на чому ми ґрунтуємо цю нашу позицію.

Розділ XVI КК України містить в собі шість складів кримінальних правопорушень:

1) стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж;

2) стаття 361-1. Створення з метою протиправного використання, розповсюдження або

збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

3) стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

4) стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

5) стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;

6) стаття 361-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

У науковців не має єдиної точки зору щодо родового об'єкту вищезгаданої групи кримінальних правопорушень. Так на думку М. В. Карчевського родовим об'єктом виступає частина інформаційних суспільних відносин, яку можна визначити як інформаційні відносини, засобом реалізації яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку. Далі автор підкреслює, що кримінальні правопорушення, передбачені розділом XVI КК України, посягають на певну частину інформаційних відносин – інформаційні відносини, пов'язані із застосуванням спеціальних технічних засобів: електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, телекомунікаційних мереж (мереж електрозвязку) [5, с. 105-106]. Автори науково-практичного коментарю до КК України за загальною редакцією професора В. Я. Тація більш широко трактують родовий об'єкт – інформаційна безпека України (стан її захищеності), при цьому безпосереднім об'єктом є нормальне функціонування електронно-обчислювальних машини, автоматизованих систем, комп'ютерних мереж, комп'ютерної інформації та мережі електрозв'язку [15, с. 768]. На наш погляд безпосереднім об'єктом є суспільні відносини щодо забезпечення цілісності та збереження комп'ютерної інформації та безпечного функціонування інформаційних систем.

Як відомо, будь-які суспільні відносини складаються з трьох обов'язкових елементів (суб'єктів відносин, предмету відносин та соціального зв'язку між суб'єктами відносно предмета), суспільні відносини в сфері інформаційної безпеки держави не є виключенням. В нашому випадку предметом суспільних відносин та одночасно предметом кримінальних правопорушень виступає інформація, яка міститься на електронних носіях, інакше кажучи – комп'ютерна інформація.

Слід зазначити, що зовсім недавно класична теорія кримінального права використовувала матеріалістичний підхід до визначення предмета кримінального правопорушення. М. І. Панов, вказуючи, що предмети злочину – речі матеріального світу, впливаючи на які особа зазіхає на цінності (благу), що належать суб'єктам суспільних відносин, а також наполягаючи на тому, що засоби скоєння злочину – це предмети матеріального світу, які застосовуються злочинцем під час вчинення суспільно-небезпечного діяння [16, с. 292-297]. Проте модернізація характеру суспільних відносин, яка пов'язана з використанням високих технологій та інформаційного розвитку суспільства перенесли деякі суспільні відносини у віртуальну площину, що дозволило науковцям виділити новий різновид предмету кримінального правопорушення – віртуальний предмет [6, с. 80-83] (інформацію). Під віртуальним предметом кримінального правопорушення слід розуміти такий предмет об'єктивного світу, який створений за допомогою спеціальних методів та (або) способів, не має зовнішнього уявлення, проте може його придбати за допомогою спеціальних методів та способів впливу [9, с. 9].

Чинне законодавство України під інформацією розуміє будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [17]. На думку О. Є. Радутного інформація – це нові відомості, які прийняті, зрозумілі і оцінені її користувачем як корисна [8, с. 458]. Інформація є системним явищем і складається принаймні з двох підсистем [18, с. 12]: інформація з відкритим доступом та інформація з обмеженим доступом, яка в свою чергу за ступенем секретності (важливості для її власників (держави, юридичних та фізичних осіб)) поділяється на конфіденційну, таємну та службову. Комп'ютерною інформацією є положення об'єктивної дійсності, здатні змінювати характер суспільних відносин, які є результатом людської діяльності та закріплені на машинному носії, електронно-обчислювальній машині, системі ЕОМ, їх мережах, тобто інформація, подана в електронному вигляді. Сфера комп'ютерної інформації, будучи складовою інформаційної сфери, є багаторівневою і в найзагальнішому вигляді включає відносини, що виникають з приводу 1) виробництва, збору, обробки, накопичення, зберігання, пошуку, передачі, поширення та споживання комп'ютерної інформації, 2) створення та використання інфор-

маційних комп'ютерних технологій та засобів їх забезпечення; 3) захисту комп'ютерної інформації та прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації з використанням комп'ютерів, їх систем та мереж. Її фундаментом є сукупність інформаційних ресурсів у вигляді комп'ютерної інформації, комп'ютерних технологій та обладнання, а також пов'язаної з ними комп'ютерної інфраструктури, включаючи мережі електрозв'язку.

Глобальна комп'ютерна мережа Інтернет містить велику кількість інформації, в тому числі й кримінально протиправну (заклики до міжнаціональної ворожнечі, порнографію тощо) і вся вона обробляється за допомогою електронно-обчислювальних машин (комп'ютерів). Вбачається, що такого виду інформація не може виступати предметом кримінального правопорушення. Виходячи з цього при побудові складів кримінальних правопорушень, предметом яких є інформація, законодавець повинен зробити деякі уточнення, а саме: інформація, що охороняється законом. Способом її обмеження є не лише її внутрішній зміст, а й зовнішнє оформлення, об'єктивізація. Вичерпний перелік та відмежування видів інформації, що охороняється, від неохоронюваної визначаються спеціальними нормативно-правовими актами, а інколи й правозастосовником. Мова йде про деталі особистого життя осіб, які є учасниками судового процесу. Суд може прийняти рішення про здійснення кримінального провадження у закритому судовому засіданні впродовж усього судового провадження або його окремої частини, якщо, наприклад, необхідно запобігти розголошенню відомостей про особисте та сімейне життя чи обставин, які принижують гідність особи (ст. 27 КПК України) [19]. У цьому випадку інформація стає такою, що охороняється законом, за рішенням суду, яке конкретизує її із загального обсягу всієї подібної інформації. Звідси ми можемо зробити висновок, що під інформацією, що охороняється законом, слід розуміти не лише інформацію, яку законодавець цілеспрямовано наділив ознаками конфіденційності та щодо якої встановив режим охорони. Інформація, що охороняється законом – це будь-яка інформація, визнана законом, визначена законом, якщо в її відношенні встановлено будь-який правовий режим, тобто якщо вона визнана об'єктом правовідносини.

Законодавець обмежив способи впливу на комп'ютерну інформацію: збут або розповсюдження інформації; знищення або блокування інформації; перехоплення або копіювання інформації. При цьому під збутом або розповсюдженням інформації слід розуміти будь-які дії наслідком яких є те, що інформація стала відома невизначеному колу осіб. Знищення інформації – приведення інформації або її частини до непридатного для використання стану незалежно від можливості її відновлення. Блокування інформації - неможливість протягом деякого часу або постійно здійснювати необхідні операції над комп'ютерною інформацією повністю або в необхідному режимі, тобто вчинення дій, що призводять до обмеження або закриття доступу до комп'ютерного обладнання та ресурсів, що перебувають на ньому, цілеспрямоване утруднення доступу законних користувачів до комп'ютерної інформації, не пов'язане з її знищенням. Копіювання інформації - створення копії наявної інформації на іншому носії, тобто перенесення інформації на відокремлений носій при збереженні незмінної початкової інформації, або відтворення інформації в будь-якій матеріальній формі - від руки, фотографуванням тексту з екрана дисплея, а також зчитування інформації шляхом будь-якого перехоплення інформації тощо.

Висновки. На нашу думку, штучне обмеження способів протиправного впливу на комп'ютерну інформацію може призвести до ухилення від кримінальної відповідальності за деякі дії. Наприклад, за модифікацію комп'ютерної інформації – протиправне внесення змін в комп'ютерну інформацію. Складність захисту правовідносин у сфері комп'ютерної інформації полягає не лише в еволюції технологій її оформлення та передачі, а й у еволюції самих правовідносин та способів впливу на них. Відсталість статей Розділу XVI КК України та проблеми кваліфікації діянь за цими статтями, які виникають в сучасної судовій практиці, не можуть знайти вирішення лише зміною диспозицій вказаних складів. Враховуючи, який законодавчий і правозастосовний пласт ховається за простими на вигляд термінами, проблема вимагає іншого, набагато більш комплексного рішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України» https://www.president.gov.ua/documents/3922020-35037.
2. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінальноправове дослідження). Київ : Атіка, 2007. 304 с.
3. Андрушко, П.П. Коментар до розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку» Особливої частини Кримінального кодексу України. Законодавство України. 2006. № 1. С. 32–54.
4. Бутузов, В.М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Нау-

ково-практичний коментар. В.М. Бутузов. К.: Друкарня МВС України, 2005. 86 с.
5. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України. монограф. М.В. Карчевський; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 528 с.
6. Мазуренко О., Розенфельд Н. Комп'ютерна інформація як предмет злочинів, передбачених Розділом XVI КК України. Право України. 2004. № 6.
7. Орлов, Ю.Ю. Реалізація вимог міжнародної Конвенції про кіберзлочинність у законодавстві України. Науковий вісник Національної академії внутрішніх справ. 2011. № 6. С. 3–9.
8. Радутний О. Є. Інформація як універсальний предмет злочинів. Держава і право 2009, вип. 46.
9. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: Автореф. дис. … к. ю. н.: Київ, 2003.
10. Сайт Офісу Генерального Прокурора України https://www.gp.gov.ua/.
11. Бангкокська декларація «Взаємодія та заходи у відповідь: стратегічні спільки в галузі попередження злочинності та кримінального правосуддя» https://www.un.org/ru/documents/decl_conv/declarations/bangkok_declaration.shtml.
12. Панов М.І. Вибрані праці з проблем правознавства. Харків: Право, 2020. 1160 с.
13. Основи кваліфікації кримінальних правопорушень: навч. посіб. Київ: Норма права, 2023. 460 с.
14. Mykola I. Panov, Sergiy O. Kharytonov, Victoria V. Haltsova. Object of criminal offense: current interpretations. Journal of the national academy of legal sciences of Ukraine, 2021 №4.
15. Кримінальний кодекс України. Науково-практичний коментар: у 2 т. 5-те вид., допов., т.2 : Особлива частина. Х.: Право, 2013. 1040 с.
16. Панов М.І. Вибрані наукові праці з правознавства. К.: Ін Юре, 2010. 812 с.
17. Закон України «Про інформацію» https://zakon.rada.gov.ua/laws/show/2657-12#Text.
18. Прокоф'єва Д. Інформація як предмет злочину. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2001 р., вип. 2.
19. Кримінально-процесуальний кодекс України https://zakon.rada.gov.ua/laws/show/4651-17#Text.