DOI 10.51369/2707-7276-2024-1(37)-1
УДК 343.233

ДЕНИСЕНКО Микола Миколайович

ПРОБЛЕМИ КРИМІНАЛЬНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА, ДЕРЖАВИ

У статті розглянуто проблемні питання у сфері охорони інформаційних відносин, перспективи виділення всіх злочинів проти інформаційної безпеки в окремий розділ Особливої частини Кримінального кодексу України, обґрунтовано необхідність створення чіткої несуперечливої концептуальної моделі кримінально-правового захисту інформаційної безпеки людини, суспільства та держави.

Проаналізовано проблему узагальнення складів злочинів, які посягають на інформаційну безпеку, та виокремлено їх у самостійний розділ Особливої частини; концептуально нові підходи до реформування кримінального законодавства, які запропонувала Робоча група з питань розвитку кримінального права, створена в межах роботи Комісії з питань правової реформи. Обґрунтовано необхідність визначення чіткого критерію, за яким буде включено певні діяння, що стосуються інформаційних відносин, до складу інформаційних кримінальних правопорушень.

На основі теоретичного підходу проведено аналіз статей Кримінального кодексу України, які стосуються охорони інформаційної безпеки. Запропоновано можливі шляхи вдосконалення цих статей, зміну назви розділу XVI і згрупування в ньому кримінальних правопорушень, передбачених статтями 360, 361, 361-1, 361-2, 362, 363, 363-1 КК (з відповідними змінами); введення поняття критично важливої інформаційної технічної інфраструктури, до якої належать технічні комунікаційні системи, що забезпечують інформаційні потреби та комунікацію державних органів і установ, а також комунікацію між регіонами країни.

На підставі проведеного дослідження зроблено висновок, що групування злочинів проти інформаційної безпеки в окремому розділі (або розділах) Особливої частини є доцільним лише при докорінній реформі системи вітчизняного кримінального права.

Ключові слова: *диспозиція кримінально-правової норми, злочини проти інформаційної безпеки, інформаційна безпека, інформаційні відносини, кримінальне право, кримінальне правопорушення в інформаційній сфері, кримінально-правова охорона, об'єкт злочину, суспільні відносини.*

Постановка проблеми. Для ефективної кримінально-правової охорони інформаційної безпеки людини, суспільства та держави потрібна система логічних, внутрішньо узгоджених правових норм. Війна поставила перед

правовою системою України нові виклики та загрози, вчасне реагування на які є першочерговим завданням державних органів. У кримінально-правовій сфері це завдання довгий час вирішувалося шляхом внесення змін і доповнень до чинних норм. Станом на 22 листопада 2022 року до чинного Кримінального кодексу (далі – КК) України було внесено 1 271 зміну та доповнення [3]. На думку багатьох науковців, це призвело до непослідовності, внутрішньої неузгодженості норм, зокрема й тих, які повинні забезпечувати кримінально-правову охорону інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Проблематику вдосконалення норм статей, що стосуються охорони інформаційної безпеки, вивчала низка вітчизняних правознавців, зокрема І. Арістова, О. Бантишев, Ю. Баулін, К. Бєляков, В. Борисов, В. Боровенко, В. Владіміров, М. Карпушин, М. Карчевський, В. Кузнецов, В. Ліпкан, Ю. Луценко, А. Марущак, Д. Олєйніков, М. Панов, Д. Прокоф'єва-Янчиленко, В. Рябчук, В. Тацій, В. Тихий, В. Шаблистий та інші. Вони розглядають різні можливі підходи до вирішення вказаних проблем, зокрема з урахуванням рівнів інформаційної безпеки [7], вирішення питання конкурування норм статей розділу XVI Особливої частини КК України [14], розширення його змісту та зміни назви [2].

Метою статті є визначення оптимальних напрямів удосконалення кримінально-правової охорони інформаційної безпеки людини, суспільства та держави на сучасному етапі розвитку національної правової системи.

Виклад основного матеріалу. Під інформаційною безпекою в широкому значенні розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [11]. Як і будь-яка важлива система суспільних відносин, інформаційна безпека потребує державної охорони, зокрема й кримінально-правової.

Слід зазначити, що термін «кримінально-правова охорона» не має законодавчого визначення і по-різному тлумачиться науковцями [6]. Під кримінально-правовою охороною певних суспільних відносин ми будемо розуміти криміналізацію діяння, яке на них посягає, тобто включення цього діяння до складу кримінально караних правопорушень.

Подібно до інших сфер суспільного життя, кримінально-правовій охороні підлягають найважливіші, найзначущіші для суспільства елементи інформаційної системи. Науковці виокремлюють три рівні інформаційної безпеки, які потребують кримінально-правової охорони: рівень особи, рівень суспільства та рівень держави [7]. На сьогодні одним із найбільш обговорюваних у науковому середовищі є питання вдосконалення системи кримінально-правових норм у сфері інформаційних відносин. Неодноразово висловлювалась пропозиція

щодо виділення всіх злочинів проти інформаційної безпеки в окремий розділ Особливої частини Кримінального кодексу. Вказана пропозиція не тільки обґрунтовується фахівцями теоретично, але й була подана до Верховної Ради у формі законопроєкту. Зокрема 9 грудня 2011 року до Верховної Ради України було внесено проєкт Закону України «Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки» (законопроєкт № 9575).

У вказаному законопроєкті передбачалося вилучення з Кримінального кодексу України таких статей: розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132), незаконне розголошення лікарської таємниці (ст. 145), порушення таємниці голосування (ст. 159), порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163), розголошення таємниці усиновлення (ст. 168), порушення недоторканності приватного життя (ст. 182), незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231), розголошення комерційної або банківської таємниці (ст. 232), розголошення державної таємниці (ст. 328), передача або збирання відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави (ст. 330).

Також було запропоновано вилучити положення статті 158 КК щодо втручання або інших несанкціонованих дій із базою даних, і положення статті 209-1 КК щодо розголошення в будь-якому вигляді інформації, яка відповідно до закону надається спеціально уповноваженому центральному органу виконавчої влади із спеціальним статусом з питань фінансового моніторингу, особою, якій ця інформація стала відома у зв'язку з професійною або службовою діяльністю.

Натомість розробники законопроєкту пропонують запровадити відповідальність за такі суспільно небезпечні діяння в статтях КК України:

– незаконні дії з комп'ютерними даними – ст. 361;

– незаконні дії в сфері телекомунікаційних послуг – ст. 361-1;

– порушення правил здійснення масових розсилок електронних повідомлень – ст. 361-3;

– незаконне надання доступу до інформації – ст. 361-2;

– заподіяння необережної шкоди через незаконні дії з комп'ютерними даними – ст. 362;

– заподіяння необережної шкоди через незаконне створення перешкод для надання телекомунікаційних послуг або їх незаконне отримання – ст. 362-1;

– заподіяння необережної шкоди через незаконне надання доступу до інформації – ст. 362-2;

– заподіяння необережної шкоди через порушення правил здійснення масових розсилок електронних повідомлень – ст. 362-3;

– порушення вимог інформаційної безпеки – ст. 363;

– незаконне отримання доступу до інформації – ст. 363-1.

Також розробники пропонували змінити назву розділу зі «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на «Злочини у сфері інформаційної безпеки». Указаний законопроєкт був 4 вересня 2012 року направлений на доопрацювання, після чого відкликаний 12 грудня 2012 року.

Отже, необхідність узагальнення складів злочинів, які посягають на інформаційну безпеку, а також виокремлення їх у самостійний розділ Особливої частини КК України усвідомлюються давно. Водночас на сьогодні вказані зміни так і не відбулися, хоча продовжується їх обговорення в академічних колах. Це свідчить про складність проблеми й відсутність простих шляхів її вирішення.

Норми Особливої частини систематизовані, переважно, відповідно до родового об'єкта злочинів. Слід відзначити, що на сьогодні в науковому світі триває дискусія щодо того, що вважати об'єктом злочину. Традиційно у вітчизняній правовій доктрині об'єктом злочину вважають суспільні відносини [4, с. 105]. Деякі дослідники заперечують використання традиційного підходу, пропонуючи вважати об'єктом злочину порядок суспільних відносин [8]. На нашу думку, для досягнення мети цього дослідження цілком достатньо найпоширенішого розуміння об'єкта злочину як охоронюваних кримінальним законом суспільних відносин.

Відповідно до цього у вітчизняній правовій науці родовим об'єктом злочину визначають певну групу однорідних суспільних відносин, що знаходяться під кримінально-правовим захистом [5, с. 6]. Таке впорядкування не завжди є однозначним, оскільки часто один злочин посягає більше, ніж на один об'єкт. У цьому випадку науковці говорять про основний і додатковий об'єкти злочину. Класичними прикладами є розбій (ст. 187 КК) – злочин, який посягає як на майнові відносини, так і на відносини захисту життя і здоров'я особи, або незаконне заволодіння транспортним засобом (ст. 289 КК), що посягає як на безпеку руху та експлуатації транспортних засобів, так і на відносини власності. Завжди можна поставити питання, які саме суспільні відносини є основним, а які – додатковим об'єктом таких злочинів.

Тому, коли мова йде про виділення окремого розділу в Особливій частині або зміну назви розділу, або виключення певного злочинного діяння з одного розділу та включення до іншого, то фактично ставиться питання щодо оптимальної класифікації визначених законом злочинних діянь. Пропонуючи включити до Особливої частини новий розділ, необхідно довести, що нова класифікація є досконалішою, а групи однорідних суспільних відносин, які підлягають кримінально-правовій охороні, побудовані логічніше. Тому для вирішення питання щодо доцільності виділення злочинів проти інформаційної безпеки в окремий розділ необхідно, передусім, чітко визначити суспільні відносини, на які посягають указані злочини.

Закон України «Про інформацію» визначає поняття суб'єктів та

об'єкта інформаційних відносин, але не надає власне їх визначення. Водночас, спираючись на норми вказаного закону, можна визначити інформаційні відносини як урегульовані правом відносини між фізичними та юридичними особами, об'єднаннями громадян, суб'єктами владних повноважень із приводу створення, отримання, зберігання, поширення (розповсюдження) інформації.

Розглянувши це визначення, знову можемо помітити, що інформаційні відносини часто не є самоцінними для людини, суспільства або держави, зазвичай вони лише обслуговують інші важливі суспільні відносини, наприклад управлінські, господарські, охорони здоров'я чи довкілля тощо. Кримінальних правопорушень, де інформаційні відносини були б основним об'єктом, не так багато. Насамперед до кола таких правопорушень належать ті, що посягають на елементи інформаційної інфраструктури: телекомунікаційні мережі, інформаційно-комунікаційні системи та їхнє програмне забезпечення. Указані правопорушення виділені в розділ XVI Особливої частини КК України. Водночас було б нелогічно відносити до кримінальних правопорушень проти інформаційної безпеки тільки ті діяння, що посягають на інформацію, закріплену на певних носіях, а саме: в електронних інформаційно-комунікаційних системах та електронних комунікаційних мережах. Тому дослідники намагаються виробити загальні підходи, які дадуть можливість створити цілісну систему кримінально-правового захисту інформаційної безпеки.

Одне з ключових завдань, які необхідно вирішити на цьому шляху, – це визначення чіткого критерію, який дасть змогу обґрунтувати включення (або не включення) певного діяння, що стосується інформаційних відносин, до складу інформаційних кримінальних правопорушень. Без такого критерію важко обґрунтувати віднесення таких різних за кримінально-правовою природою діянь як, наприклад, шпигунство й незаконне розголошення лікарської таємниці до одного інституту, а тим більше – об'єднання їх в одному розділі Особливої частини. Інакше кажучи, те, що об'єднує злочинні діяння, уміщені в одному розділі, повинно бути більш суттєвим, ніж те, що їх відрізняє.

Пропонуємо визначати як інформаційне кримінальне правопорушення таке діяння, яке прямо посягає на інформаційні відносини або через посягання на стан захищеності в інформаційній сфері створює небезпеку для широкого, наперед невизначеного кола інших суспільних відносин. Якщо діяння посягає на певні, чітко визначені суспільні відносини (як-то: власності, господарські, управлінські), його, на нашу думку, не можна визначити як інформаційний злочин, навіть якщо інформаційні відносини також зазнають деструктивного впливу або ж інформація використовується як основне знаряддя злочину. За наявності вказаного критерію можна дати науково обґрунтоване визначення поняттю «інформаційне кримінальне правопорушення».

Інформаційним кримінальним правопорушенням слід уважати про-

типравне, кримінально каране, вчинене суб'єктом злочину, винне діяння, яке прямо посягає на інформаційну безпеку людини, суспільства чи держави або шляхом порушення захищеності відносин з приводу створення, отримання, зберігання, передачі, поширення інформації створює небезпеку для широкого, наперед невизначеного кола інших суспільних відносин (надалі в цій статті для простоти викладення матеріалу будемо застосовувати термін «злочин» для позначення кримінального правопорушення будь-якої тяжкості).

Відповідно до наведеного визначення для визнання інформаційним злочину з матеріальним складом є необхідною реалізація однієї з двох можливостей:

1) злочинне діяння має будь-який характер, але його наслідки спричиняють шкоду відносинам із приводу створення, отримання, зберігання, передачі, поширення інформації (як приклад можна навести ч. 1 ст. 360 КК України – умисне пошкодження або руйнування телекомунікаційної мережі чи технічних засобів телекомунікації, чи споруд електрозв'язку, що входять до складу телекомунікаційної мережі, якщо такі дії спричинили припинення надання телекомунікаційних послуг);

2) злочинне діяння стосується інформаційної сфери, а суспільні відносини, яким завдано шкоду, чітко законодавцем не визначені (наприклад, ч. 2 ст. 330 КК України – передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам відомостей, що становлять службову інформацію, що спричинили тяжкі наслідки для інтересів держави).

Інша ситуація характерна для злочинів із формальним складом, оскільки питання про їхні суспільно небезпечні наслідки виходить за межі диспозиції статті. Тому для цих злочинів необхідно аналізувати характер і спрямованість злочинного діяння. Якщо діяння має інформаційний характер і може бути спрямоване на спричинення шкоди невизначеному колу суспільних відносин, такий злочин слід віднести до інформаційних. Якщо ж діяння злочину з формальним складом стосується інформаційної та інших сфер суспільного життя, доцільність віднесення такого злочину до інформаційних повинна визначатися в кожному випадку окремо.

Зауважимо, що під діянням інформаційного характеру розуміємо таку поведінку (дію або бездіяльність) суб'єкта злочину, яка спрямована на створення, отримання, зберігання, передачу, розголошення, поширення (розповсюдження), знищення, приховування, зміну інформації. Далі проаналізуємо ті конкретні визначення, які законодавець використовує в диспозиціях статей чинного КК України для опису таких діянь.

Виходячи з наведеного вище визначення, інформаційні злочини – це група злочинів, родовим об'єктом яких є суспільні відносини, що забезпечують інформаційну безпеку людини, суспільства і держави. На запитання, чи є необхідність виділяти ці злочини в окремий розділ Особливої частини або оптимальнішим було б вивчення інформаційних злочинів як інституту кримінального права без тако-

го об'єднання, ми спробуємо відповісти в процесі нашого дослідження.

Які ж діяння відповідно до запропонованого критерію можна визначити як інформаційні злочини? Наприклад, розголошення державної таємниці (ст. 328 КК) посягає на інформаційні відносини й може створювати небезпеку в економічній, військовій сферах, сфері громадського порядку тощо. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 КК), порушує інформаційну захищеність особи, створює неприйнятний для нормальної життєдіяльності дискомфорт, навіть якщо життю, здоров'ю або майновим правам потерпілого не завдано жодної шкоди. Цілком логічно об'єктом цих злочинів визначити саме інформаційні відносини. В обох із наведених прикладів злочинним діянням притаманні обидві визначені вище ознаки – інформаційна спрямованість діяння й універсальність негативних наслідків, тому їх слід віднести до інформаційних злочинів.

Іншим за характером діяння прикладом може бути виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436-1 КК). Ці діяння можуть мати наслідком терористичний акт, масові заворушення або інші, наперед не визначені наслідки, а можуть просто створювати небезпеку та дискомфорт для певних осіб або соціальних груп. Тому відповідно до запропонованого вище критерію ці діяння також належать до інформаційних злочинів.

Протилежний приклад становить незаконна діяльність з організації або проведення азартних ігор, лотерей, які проводяться в мережі Інтернет (ч. 1 ст. 203-2 КК). Хоча саме діяння з організації онлайн-казино, без сумніву, має інформаційний характер, більше того, потребує певної кваліфікації саме у сфері інформаційних технологій. Однак, оскільки в цьому випадку всі маніпуляції суб'єкта злочину з інформацією та інформаційними технологіями мають чітко визначену законодавцем мету – створення незаконного грального бізнесу, злочин у цілому не є інформаційним.

Те саме стосується такого злочину як надання неправдивих відомостей до органу ведення Державного реєстру виборців або інше несанкціоноване втручання в роботу Державного реєстру виборців (ст. 158 КК), для якого посягання на інформаційні відносини хоч і є необхідною ознакою, але лише опосередковує посягання на суспільні відносини іншого виду, а саме – ті, що забезпечують виборчі права громадян. Вилучати цей злочин із відповідного розділу Особливої частини для того, щоб включити до окремого розділу Особливої частини, як це пропонують деякі дослідники [2], убачається недоречним. Тим більше необґрунтованим є включення до складу інформаційних тих злочинів, у яких інформація або маніпулювання інформацією є предметом, знаряддям або способом вчинення злочину.

Отже, необхідно ретельно проаналізувати наявні в Кримінальному кодексі України склади злочинів, що

стосуються інформаційних відносин, і визначити, які з них можуть бути злочинами інформаційного характеру. Для цього доцільно провести класифікацію таких складів відповідно до того, яким елементом складу злочину є інформація: об'єктом, предметом чи знаряддям злочину, з урахуванням того, чи є інформація (інформаційні відносини) обов'язковим або факультативним елементом певного складу. Відповідно до загального принципу формування Особливої частини можливо розглядати включення до інформаційних тільки злочинів, для яких інформаційні відносини є основним або додатковим об'єктом. Указані злочини можна класифікувати таким чином:

1) злочини, що спрямовані проти інформаційної безпеки держави або її органів;

2) злочини, що спрямовані проти інформаційної безпеки суспільства;

3) злочини, що порушують інформаційну безпеку приватних суб'єктів – фізичних осіб або юридичних осіб приватного права.

Крім того, окремо слід виділити злочини, які спрямовані на завдання шкоди інформаційній технічній інфраструктурі або на спотворення інформації, що міститься на електронних чи інших матеріальних носіях. Останні, залежно від обставин конкретного злочинного діяння, можуть бути спрямовані проти інформаційної безпеки як держави або суспільства, так і фізичної або юридичної особи.

Аналіз чинної на сьогодні Особливої частини КК України дає можливість виділити понад 70 складів злочинів, що спрямовані проти інформаційної безпеки держави та її органів, інформаційної безпеки суспільства, інформаційної безпеки людини або юридичної особи приватного права, а також ті, які спрямовані на завдання шкоди інформаційній технічній інфраструктурі та спотворення інформації, що міститься на електронних або інших матеріальних носіях, і які можуть бути визначені як інформаційні. Згрупуємо їх у відповідності до запропонованої вище класифікації.

1. Злочини, які посягають на інформаційну безпеку держави або її органів: ч. 1, 2 ст. 111; ч. 1, 3, 6 ст. 111-1; ч. 1 ст. 114; ч. 1, 2, 3 ст. 114-2; ч. 2 ст. 163; ч. 1, 2 ст. 328; ч. 1, 2 ст. 329; ч. 1, 2 ст. 330; ч. 1, 2, 3 ст. 359; ч. 1, 2, 3 ст. 387; ч. 1, 3 ст. 422; ч. 1, 2, 3 ст. 436-2.

2. Злочини, які посягають на інформаційну безпеку суспільства: ч. 1 (*у частині розпалювання ворожнечі, ненависті*), ч. 2, 3 ст. 161; ч. 1, 2 ст. 238; ч. 1, 2, 3 ст. 300; ч. 1, 2 ст. 436-1.

3. Злочини, які посягають на інформаційну безпеку людини або юридичних осіб приватного права: ст. 132; ст. 145; ч. 1 ст. 163; ч. 1, 2 ст. 168; ч. 1, 2 ст. 182; ст. 231; ст. 232; ч. 1, 2 ст. 232-2.

4. Злочини, які посягають на безпеку інформаційної технічної інфраструктури або на достовірність інформації, що міститься на матеріальних носіях: ч. 1, 2, 3 ст. 360; ч. 1, 2, 3, 4 ст. 361; ч. 1, 2 ст. 361-1; ч. 1, 2, 3 ст. 362; ст. 363; ч. 1, 2 ст. 363-1.

Проаналізуємо злочини останньої групи детальніше. Слід зазначити, що на сьогодні серед науковців не існує спільного підходу до розуміння категорії «інформаційна інфраструктура». У науковій літературі можна знайти багато визначень цього понят-

тя, які суттєво відрізняються за обсягом [1, с. 18–20]. У межах цього дослідження під інформаційною технічною інфраструктурою будемо розуміти технічні системи, що забезпечують накопичення, зберігання, обробку та передачу інформації.

Першим зі злочинів указаного виду є умисне пошкодження або руйнування телекомунікаційної мережі (ст. 360 КК). Об'єкт цього злочину в різних науково-практичних коментарях визначається як встановлений порядок забезпечення інформаційного обміну за допомогою засобів електрозв'язку [10, с. 1033] або суспільні відносини, що забезпечують додержання нормативно визначеного порядку користування лініями та обладнанням мереж електрозв'язку [9, с. 843]. У будь-якому разі йдеться про злочин проти інформаційної безпеки.

Якщо спробувати відповісти на питання: проти інформаційної безпеки якого з виділених нами суб'єктів (людини, суспільства чи держави) спрямовано цей злочин, відповідь не є наперед визначеною і буде залежати від конкретних обставин вчиненого. Наприклад, унаслідок злочинних дій може бути пошкоджена телекомунікаційна мережа мікрорайону або районного міста, яка налічує десятки тисяч абонентів, тож скоєне може навіть підпадати під ч. 3 ст. 360 КК України, однак це навряд чи можна вважати злочином проти інформаційної безпеки суспільства або держави. Водночас унаслідок аналогічних за характером дій може бути пошкоджена мережа, що забезпечує критично важливий зв'язок між регіонами держави, державними органами й установами, військовими частинами тощо. В останньому випадку вчинене не завжди може бути кваліфіковане як диверсія з огляду на мету як необхідну ознаку злочину, передбаченого ст. 113 КК України. Проте не викликає сумніву, що останнє діяння є більше суспільно небезпечним і повинно кваліфікуватися як більш тяжкий злочин.

Ураховуючи це, уважаємо за доцільне ввести поняття критично важливої інфраструктури, до якої віднести технічні комунікаційні системи, що забезпечують інформаційні потреби та комунікацію державних органів і установ, а також комунікацію між регіонами країни. До відповідних статей Особливої частини КК України можна включити як окремі частини кваліфіковані склади, що передбачають відповідальність за посягання на критично важливу інформаційну інфраструктуру.

Крім того, оскільки предметом злочину, передбаченого ст. 360 КК України, є лінії, обладнання та споруди електрозв'язку, уважаємо логічнішим віднести вказаний злочин до розділу XVI Особливої частини КК, який містить інші кримінальні правопорушення у сфері використання мереж електрозв'язку, а також включити до предмета злочинного посягання ст. 360 КК системи оптоволоконного зв'язку, споруди й обладнання, призначене для обробки та зберігання інформації (так звані «data-центри»).

Ще шість статей, які є предметом нашого аналізу, містяться в розділі XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж

електрозв'язку». Стосовно цих статей у дослідників не виникає спорів щодо віднесення їх до злочинів проти інформаційної безпеки, однак до диспозицій цього розділу в науковців чи не найбільше зауважень щодо законодавчої техніки й організації правового матеріалу.

Як головні недоліки цього розділу науковці визначають такі:

1. Відсутність чітких і прозорих критеріїв суспільної небезпечності посягань у сфері використання комп'ютерної техніки та мереж електрозв'язку. Наприклад, диспозиція ч. 1 ст. 361 КК України (несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж) не містить вказівки ні на наслідки втручання, ні на характеристики об'єкта втручання, що дає змогу притягти до кримінальної відповідальності за діяння, масштаб якого не має ознак суспільної небезпечності. Те саме стосується інших діянь: витік, втрата, підробка, блокування інформації, порушення встановленого порядку її маршрутизації або спотворення процесу її обробки (ст. 361, 362 КК) визнаються суспільно небезпечними самі по собі, безвідносно до їхніх масштабу і наслідків. Так само, на думку законодавця, суспільно небезпечними є просте розповсюдження або збут шкідливого програмного або технічного забезпечення (ст. 361-1 КК), розповсюдження або збут комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК) тощо. Лише на рівні кваліфікуючих ознак установлено залежність кримінальної відповідальності від настання істотної шкоди [12]. Фактично для обґрунтованого застосування більшості статей розділу XVI необхідне серйозне доктринальне тлумачення.

2. Норми статей розділу XVI конкурують із багатьма іншими нормами КК України, оскільки після комп'ютеризації багатьох сфер людської діяльності кожен із перерахованих злочинів може бути вчинений шляхом втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж або несанкціонованих дій з інформацією, яка оброблюється в електронно-обчислювальних машинах [14, с. 414]. Зокрема норми статей 361-2 та 362 КК фактично конкурують з усіма нормами, що охороняють режим обмеженого доступу до інформації, оскільки така інформація може бути розміщена на електронному носії. До їхнього складу входять статті 111, 114, 132, 145, 158, 159, 163, 168, 182, 209-1, 231, 232, 328, 330, 357, 376-1, 381, 387, 422 КК України. Головною причиною цієї конкуренції, на наш погляд, є те, що при визначенні предмета злочину за статтями 361-2 та 362 КК як критерій використано носій інформації, тоді як в інших розділах для визначення предмета використано зміст інформації або інші її характеристики. Однак ці критерії не є взаємовиключними: інформація, що становить предмет злочину, передбаченого ст. 330 КК, також може бути предметом злочину, передбаченого ст. 361-2 КК, оскільки може зберігатися в електронно-обчислювальних машинах. Вважаємо, що предметом

злочину статей 361-2 та 362 КК України слід визначити тільки таку інформацію, яка не може існувати в іншому вигляді, ніж електронний, або не може бути використана інакше, ніж за допомогою комп'ютерів, як-то: програмне забезпечення, бази даних (їхні дампи), великі масиви персональних даних користувачів тощо.

3. Через недоліки диспозицій відповідних статей наявні у КК України засоби не забезпечують захист від найбільш розповсюджених і суспільно небезпечних діянь у сфері використання інформаційних технологій, як, наприклад, незаконної торгівлі даними про кредитні картки, банківські реквізити, реквізити в електронних платіжних системах тощо.

4. Надмірне використання в диспозиціях статей розділу XVI технічних термінів, зокрема переліку технічних засобів оброблення інформації, створює небезпеку «технологічної залежності» законодавства та швидкого «старіння» правових норм із розвитком технічних систем. Як приклад можна навести ст. 363-1 КК України, що встановлює відповідальність за перешкоджання роботі електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. На сьогодні вказаний у диспозиції статті спосіб перешкоджання – розповсюдження повідомлень електрозв'язку, або так званий «SPAM», уже не створює таких незручностей, як на початку розвитку мережі Інтернет. По-перше, уже давно були запроваджені програмні засоби, які дають можливість користувачу ефективно запобігти отриманню небажаних повідомлень електрозв'язку. По-друге, сучасні комп'ютери та канали зв'язку мають таку потужність, що їм неможливо зашкодити розповсюдженням повідомлень електрозв'язку. Зараз для перевантаження систем зв'язку зловмисники використовують набагато потужніші й небезпечніші інструменти: так звані dos- та ddos-атаки. Однак, оскільки диспозиція ст. 363-1 чітко вказує спосіб впливу (розповсюдження електронних повідомлень), фактично стаття втратила актуальність і не виконує функції кримінально-правової норми.

5. Фахівці також відзначають недостатню визначеність та єдність термінології статей розділу XVI як на рівні законодавства, так і наукового тлумачення, що звужує можливості використання цих статей для охорони відповідних суспільних відносин. Так, неоднозначними є терміни, що використовуються у відповідних нормах КК України та Кодексу України про адміністративні правопорушення [12].

Як бачимо, вирішення проблем змісту розділу XVI є досить складним. Не вдаючись зараз до аналізу тих причин, які призвели до такого стану речей, звернемо увагу на шляхи їх вирішення, які пропонують вітчизняні правники. Більшість дослідників, які пропонують зміни до розділу XVI, уважають за необхідне розширити його зміст і ввести до нього не тільки злочини, пов'язані з використанням комп'ютерної техніки, але й інші злочини проти інформаційної безпеки. Відповідно, пропонується змінити його назву. Наприклад, у згаданому законопроєкті № 9575 пропонується назва

«Злочини у сфері інформаційної безпеки». В. С. Батиргареєва пропонує для вказаного розділу назву «Злочини проти інформаційної безпеки особи, суспільства, держави» [2, с. 116], у проєкті Робочої групи з питань розвитку кримінального права пропонується назва «Кримінальні правопорушення проти інформаційної безпеки» [13].

Не заперечуючи проти можливості такого підходу, слід звернути увагу на те, що визначені вище проблеми можна вирішити й іншим шляхом, а саме: звузити зміст розділу XVI до захисту безпеки інформаційної технічної інфраструктури, а також безпеки тих інформаційних об'єктів, які не можуть існувати або використовуватись інакше, як в електронному вигляді. Як свідчить проведений вище огляд, вмістити до єдиного розділу Особливої частини КК України всі злочини, що посягають на інформаційну безпеку, буде досить важко. Більше того, із розвитком інформатизації людського суспільства до такого розділу необхідно буде включати все більше статей Особливої частини КК. Тому доцільніше назвати розділ XVI ***«Кримінальні правопорушення проти інформаційної технічної інфраструктури та безпеки інформації, що міститься на електронних носіях»*** і згрупувати в ньому кримінальні правопорушення, передбачені статтями 360, 361, 361-1, 361-2, 362, 363, 363-1 КК, а також визначити в цьому розділі як самостійний злочин внесення завідомо неправдивих відомостей до державних електронних реєстрів. Усунення зазначених вище недоліків можливе шляхом удосконалення диспозицій цих статей, що потребує подальшого їх дослідження як правниками, так і спеціалістами у сфері інформаційних технологій.

Наприкінці нашого огляду слід звернути увагу на діяння, які посягають на достовірність інформації, що міститься на матеріальних носіях, крім електронних. До них належать такі два злочини як підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів (ст. 358 КК) і службове підроблення (ст. 366 КК). Відповідно до запропонованого нами критерію вказані діяння є інформаційними злочинами, оскільки вони шляхом порушення захищеності відносин із приводу створення, отримання, збереження, поширення інформації створюють небезпеку порушення широкого, наперед невизначеного кола інших прав і свобод.

Отже, злочини, що можуть належати до інформаційних, на сьогодні вміщені в одинадцяти розділах Особливої частини КК України (I, V, VIII, XII, XIV, XV, XVI, XVII, XVIII, XIX, XX), і, ураховуючи визначені вище недоліки, диспозиції відповідних статей потребують подальшого вдосконалення. Однак підходи до такого вдосконалення можуть бути різні. Консервативний підхід передбачає внесення змін до існуючих статей Особливої частини без зміни її структури й організації правового матеріалу. Натомість радикальний підхід передбачає не тільки зміну структури Особливої частини, але й самої системи кримінального права, яка склалася у 20–30-х роках минулого століття завдяки зусиллям радянських правників (А. А. Піонтковського,

А. Н. Трайніна й інших) і зберігається дотепер (вчення про склад злочину, визначення злочину як суспільно небезпечного діяння, визначення міри покарання в кожній частині статті Особливої частини тощо).

На сьогодні в науковому середовищі триває пошук найоптимальніших шляхів реформування вітчизняної системи кримінального права. Один із найрадикальніших підходів до реформування кримінального законодавства запропонувала Робоча група з питань розвитку кримінального права, створена в межах роботи Комісії з питань правової реформи. Вказана Робоча група підготувала проєкт нового КК (далі – Проєкт), презентувала його на численних конференціях, вебінарах, в офісі Генерального прокурора, адвокатам, суддям, опублікувала й постійно оновлює Проєкт на своєму сайті (URL: https://newcriminalcode.org.ua). Цей Проєкт [13] містить багато новітніх підходів у сфері кримінального права, зокрема й щодо інформаційних злочинів. Не вдаючись до аналізу змін, які виходять за межі предмета нашого дослідження, розглянемо, як автори Проєкту вирішили питання щодо кримінально-правового захисту інформаційної безпеки.

Позитивним є те, що в Проєкті окремо виділені розділи, присвячені захисту інформаційного простору особи й інформаційній безпеці держави, при цьому перший містить 9 складів злочинів (5 з яких – проступки), а другий містить 7 складів злочинів (3 з яких – проступки).

Зокрема захисту інформаційного простору особи присвячено розділ 4.7 «Кримінальні правопорушення проти приватності людини», який містить такі склади:

стаття 4.7.4 «Дії щодо інформації про особисте чи сімейне життя»;

стаття 4.7.5 «Порушення недоторканності житла чи іншого володіння»;

стаття 4.7.6 «Розголошення таємниці кореспонденції»;

стаття 4.7.7 «Обмеження інформаційних прав людини»;

стаття 4.7.8 «Обмеження права на інформацію»;

стаття 4.7.9 «Порушення права на особисті папери та зображення»;

стаття 4.7.10 «Розголошення таємниці інформації про стан здоров'я»;

стаття 4.7.11 «Порушення права на використання імені»;

стаття 4.7.12 «Перешкоджання законній професійній діяльності журналістів».

Запропоновані формулювання свідчать, що автори Проєкту намагаються в одному розділі узагальнити всі можливі посягання на інформаційну безпеку людини. Водночас систематизація злочинів проти інформаційної безпеки не проведена послідовно. Так, знищення, приховування або спотворення інформації про забруднення довкілля автори Проєкту пропонують розмістити в розділі 5.3 «Кримінальні правопорушення проти безпеки довкілля», хоча основним об'єктом злочину тут, очевидно, є безпека саме людини та/або суспільства, а не довкілля, шкода якому на момент приховування або спотворення інформації вже завдана. Розголошення інсайдерської інформації, що спричинило майнову шкоду, яке, на наш погляд, є

злочином проти приватності юридичної особи приватного права, вміщено авторами в розділі 6.3 «Кримінальні правопорушення проти фінансів».

Не цілком послідовним, на нашу думку, є внесення до розділу, присвяченого захисту інформаційного простору особи, такого правопорушення як перешкоджання законній професійній діяльності журналістів. Указаний недолік зумовлений тим, що автори Проєкту не розглядають інформаційну безпеку суспільства як категорію, окрему s від інформаційної безпеки людини, і від інформаційної безпеки держави.

Злочини проти інформаційної безпеки держави пропонується виділити в розділ 9.2 «Кримінальні правопорушення проти таємниці інформації, що належить державі», де передбачено покарання за діяння у статтях:

стаття 9.2.3 «Розголошення державної таємниці»;

стаття 9.2.4 «Збирання або передавання службової інформації у сфері оборони країни»;

стаття 9.2.5 «Несанкціоноване поширення інформації про направлення чи переміщення товарів військового призначення»;

стаття 9.2.6 «Несанкціоноване поширення інформації про переміщення або розміщення військових формувань України»;

стаття 9.2.7 «Необережне розголошення державної таємниці»;

стаття 9.2.8 «Необережна втрата носія інформації, що містить державну таємницю»;

стаття 9.2.9 «Розголошення службової інформації у сфері оборони країни».

Отже, автори Проєкту цілком слушно зібрали всі злочини проти держави, що мають інформаційну складову, в одному розділі (на сьогодні вказані діяння вміщені в чотирьох розділах Особливої частини КК України).

Цікавим і раціональним, на нашу думку, є виділення в Проєкті окремого розділу, присвяченого кримінальним правопорушенням проти достовірності інформації, що міститься на матеріальних носіях, крім електронних (розділ 7.8 Проєкту).

Правопорушення, які в чинному КК України вміщені в розділі XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», автори Проєкту пропонують зосередити в розділі 7.7 «Кримінальні правопорушення проти інформаційної безпеки». Зокрема пропонується в статтях установити кримінальну відповідальність за протиправні діяння (перші сім – злочини, інші – проступки):

стаття 7.7.4 «Діяння щодо комп'ютерних даних»;

стаття 7.7.5 «Діяння щодо комп'ютерних даних, що з необережності спричинили тяжку майнову шкоду»;

стаття 7.7.6 «Діяння в сфері телекомунікаційних послуг»;

стаття 7.7.7 «Діяння щодо інформації з обмеженим доступом»;

стаття 7.7.8 «Порушення вимог безпеки комп'ютерних даних з необережності»;

стаття 7.7.9 «Несанкціоноване використання чужого цифрового образу»;

стаття 7.7.10 «Поширення неправдивої новини»;

стаття 7.7.11 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»;

стаття 7.7.12 «Діяння щодо комп'ютерних даних, що з необережності спричинили значну майнову шкоду»;

стаття 7.7.13 «Діяння зі шкідливим програмним чи технічним засобом»;

стаття 7.7.14 «Порушення вимог безпеки комп'ютерних даних, що з необережності спричинило значну майнову шкоду».

Не торкаючись питання юридичної техніки та використаних авторами конкретних формулювань, спробуємо оцінити, наскільки оптимальною є запропонована класифікація інформаційних злочинів.

Назва розділу свідчить, що автори Проєкту ототожнюють інформаційну безпеку суспільства та безпеку інформаційної інфраструктури різних форм власності. Нелогічним є вміщення в цьому розділі такого правопорушення як незаконне отримання телекомунікаційних послуг, яке, фактично, є злочином проти власності (аналогічний за характером діяння і мотивами злочин «безоплатне використання електричної чи теплової енергії» автори Проєкту віднесли до розділу 6.1 «Кримінальні правопорушення проти власності на речі»). Таке діяння як несанкціоноване використання чужого цифрового образу було б логічно віднести до злочинів проти інформаційної безпеки людини або юридичної особи приватного права, які автори Проєкту згрупували в розділі 4.7.

Позитивним у Проєкті (у сфері кримінально-правової охорони інформаційної безпеки) є усунення дисбалансу між захистом інформаційної безпеки людини та держави, раціональніша класифікація інформаційних злочинів, виділення в окремий розділ правопорушень проти достовірності інформації, що міститься на матеріальних носіях, крім електронних. Недоліками Проєкту є непослідовність у класифікації злочинних діянь, відсутність розділу, присвяченого злочинам проти інформаційної безпеки суспільства, вміщення в одному розділі злочинів проти інформаційної безпеки суспільства й безпеки інформаційної технічної інфраструктури та комп'ютерних даних.

Отже, при радикальному оновленні системи кримінального права вбачається доцільним згрупувати правопорушення проти інформаційної безпеки в такі розділи (підрозділи) Особливої частини КК України:

1. Кримінальні правопорушення проти інформаційної безпеки особи. Розділ має вміщати діяння, які протиправно посягають на приватність особистого чи сімейного життя; спрямовані на незаконне отримання чи розголошення інформації особистого характеру; надання особі недостовірних даних, протиправне приховування або ненадання інформації, що має важливе значення для особи, тощо. У цьому ж розділі можливо визначити кримінальні правопорушення проти інформаційної безпеки юридичних осіб приватного права.

2. Кримінальні правопорушення проти інформаційної безпеки суспільства. Розділ повинен вміщати діяння, спрямовані на перешкоджання законній професійній діяльності журналістів; приховування або перекручення інформації, яка має важливе суспільне значення, зокрема інформації про стан довкілля, події або явища, що становлять суспільну небезпеку; пропаганду ненависті та ворожнечі; заклики до протиправних дій; поширення тоталітарних, фундаменталістських та інших небезпечних ідей; поширення матеріалів неприйнятного змісту тощо.

3. Кримінальні правопорушення проти інформаційної безпеки держави. Розділ має вміщати діяння, спрямовані на збирання та передачу відомостей, що містять державну або військову таємницю; розголошення державної або військової таємниці; порушення режиму роботи з таємною інформацією; поширення інформації, що містить відомості, заборонені до поширення, тощо.

4. Кримінальні правопорушення проти безпеки технічних інформаційних систем (інформаційної технічної інфраструктури). Розділ повинен вміщати діяння, спрямовані на пошкодження, перешкоджання в роботі, порушення захищеності технічних систем, що забезпечують накопичення, зберігання, обробку та передачу інформації, а також протиправні маніпуляції з інформацією в цих системах.

5. Кримінальні правопорушення проти достовірності інформації, що міститься на матеріальних носіях. Розділ має вміщати діяння, спрямовані на підроблення, пошкодження або знищення офіційних документів; видачу або використання завідомо неправдивого офіційного документа; підроблення або неправомірне використання засобів маркування, ідентифікації або нанесення реквізитів на офіційні документи тощо.

Узагальнюючи викладене, можна дійти висновку, що групування злочинів проти інформаційної безпеки в окремому розділі (або розділах) Особливої частини є доцільним лише при докорінній реформі системи вітчизняного кримінального права. ***Зведення до одного розділу всіх злочинів, спрямованих проти інформаційної безпеки, за збереження існуючої структури Особливої частини є недоцільним і неможливим.*** Більше того, навіть при радикальних змінах кримінального законодавства навряд чи доцільно об'єднувати в одному розділі злочини проти інформаційної безпеки людини, суспільства та держави.

Висновки. Інформаційна безпека є важливою складовою безпеки людини, суспільства та держави й підлягає кримінально-правовій охороні. Злочином проти інформаційної безпеки слід уважати протиправне, кримінально каране, вчинене суб'єктом злочину, винне діяння, яке прямо посягає на інформаційну безпеку людини, суспільства чи держави або шляхом порушення захищеності відносин з приводу створення, отримання, зберігання, передачі, поширення інформації створює небезпеку для широкого, наперед не визначеного кола інших суспільних відносин.

Вітчизняна система кримінально-правової охорони інформаційної безпеки людини, суспільства та держави

потребує реформування. Можливі два підходи до такого реформування: консервативний і радикальний.

Консервативний підхід передбачає збереження існуючої структури Особливої частини з певними вдосконаленнями, які усувають виявлені на сьогодні проблеми у сфері кримінально-правової охорони інформаційних відносин. Вбачається за доцільне змінити назву розділу XVI на таку: «Кримінальні правопорушення проти інформаційної технічної інфраструктури та безпеки інформації, що міститься на електронних носіях» і згрупувати в ньому кримінальні правопорушення, передбачені статтями 360, 361, 361-1, 361-2, 362, 363, 363-1 КК (з відповідними змінами). Доцільно ввести поняття критично важливої інформаційної технічної інфраструктури, до якої віднести технічні комунікаційні системи, які забезпечують інформаційні потреби та комунікацію державних органів і установ, а також комунікацію між регіонами країни. У результаті таких змін можливо до відповідних статей Особливої частини КК України включити як окремі частини кваліфіковані склади, що передбачають відповідальність за посягання на критично важливу інформаційну технічну інфраструктуру.

Також, ураховуючи підвищення ролі електронних реєстрів (Державного реєстру речових прав на нерухоме майно, Єдиного державного реєстру судових рішень та інших) і поширення практики отримання державних послуг в електронному режимі, зокрема через систему «Дія», убачається за доцільне визначити внесення завідомо неправдивих відомостей до державних електронних реєстрів як самостійний склад злочину розділу XVI Особливої частини КК.

Радикальний підхід до реформування системи кримінально-правової охорони інформаційної безпеки передбачає перехід до нової концептуальної моделі організації правового матеріалу. У такому разі доцільно згрупувати кримінальні правопорушення проти інформаційної безпеки в такі розділи:

1. Кримінальні правопорушення проти інформаційної безпеки особи.

2. Кримінальні правопорушення проти інформаційної безпеки суспільства.

3. Кримінальні правопорушення проти інформаційної безпеки держави.

4. Кримінальні правопорушення проти безпеки технічних інформаційних систем (інформаційної інфраструктури).

5. Кримінальні правопорушення проти достовірності інформації, що міститься на матеріальних носіях.

Зведення до одного розділу всіх злочинів, спрямованих проти інформаційної безпеки, як за збереження існуючої структури Особливої частини, так і за умови її кардинального реформування, є недоцільним і неможливим. Пошук оптимальних визначень діянь, які підлягають криміналізації, формулювань диспозицій відповідних статей Кримінального кодексу України має стати метою подальших досліджень.

Список використаних джерел

1. Арістова І. В., Баранов О. А., Дзьобань О. П. та ін. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології : монографія / за заг. ред. проф. К. І. Бєлякова. Київ : КВІЦ, 2019. 344 с.

2. Батиргареєва В. С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право.* 2020. № 1 (32). С. 110–119.

3. Баулін Ю. В. Виклики сучасності й проект нового КК України. *Кримінальне право України перед викликами сучасності і майбуття: яким воно є і яким йому бути* : матеріали міжнародної наукової конференції, (Харків, 21–22 жовт. 2022 р.) / редкол.: В. Я. Тацій, Ю. А. Пономаренко, Ю. В. Баулін та ін. Харків : Право, 2022. С. 219.

4. Кримінальне право України: Загальна частина : підручник / за заг. ред. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. Київ : Юрінком Інтер, 2003. 512 с.

5. Кримінальне право України: Особлива частина : підручник / за заг. ред. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. Київ : Юрінком Інтер, 2003. 672 с.

6. Кузнецов В. В. Кримінально-правова охорона: проблеми визначення поняття. *Науковий вісник Ужгородського національного університету*. 2015. Серія ПРАВО. Вип. 30. Т. 2. С. 107–110.

7. Кузьменко А. М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства. *Часопис Київського університету права*. 2010. № 4. С. 317–321.

8. Ландіна А. В. Інформаційна безпека як об'єкт злочину. *Правова держава*. 2016. Вип. 27. С. 354–361.

9. Науково-практичний коментар Кримінального кодексу України / за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернєя. 2-ге вид. Київ : Юрінком Інтер, 2018. 1104 с.

10. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. Київ : Юридична думка, 2010. 1288 с.

11. Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 р. : Закон України від 09.01.2007 № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E (дата звернення: 20.11.2023).

12. Пояснювальна записка до законопроекту «Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки» № 9575 від 09.12.2011. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=42065&pf35401=209124.t (дата звернення: 20.08.2023).

13. Проєкт нового Кримінального кодексу України станом на 14 липня 2022 р. URL: https://newcriminalcode.org.ua/upload/media/2022/07/14/1-kontrolnyj-tekst-proektu-kk-14-07-2022.pdf (дата звернення: 23.08.2023).

14. Хавронюк М. І. Довідник з Особливої частини Кримінального кодексу України. Київ : Істина, 2004. 504 с.

Стаття надійшла до редакції 24.01.2024

UDC 343.233

Denysenko M. M.

ISSUES OF THE CRIMINAL AND LEGAL PROVISION OF INFORMATION SECURITY OF AN INDIVIDUAL, SOCIETY AND THE STATE

The article provides an overview of problematic issues in the field of information relations protection considering the prospects of allocating all crimes against information security into a separate section of the Special Part of the Criminal Code of Ukraine, and substantiates the need to create a clear and consistent conceptual model of criminal law protection of information security of an individual, society and the State.

The author analyzes the problem of generalization of corpus delicti of crimes encroaching on information security and distinguishes them into an independent section of the Special Part as well as conceptually new approaches to reforming criminal law proposed by the Working Group on the Development of Criminal Law established within the framework of activities of the Legal Reform Commission. The author substantiates the need to define a clear criterion by which certain acts relating to information relations will be included into the scope of criminal offences relating to the field of information.

Based on the theoretical approach, the article analyzes relevant articles of the Criminal Code of Ukraine relating to information security protection. The author suggests possible ways of improving these articles, changing the title of Section XVI and grouping criminal offences under Articles 360, 361, 361-1, 361-2, 362, 363, 363-1 of the CC (with relevant amendments); by means of introducing the concept of critical information technical infrastructure, which includes technical communication systems that ensure information needs and communication between state bodies and institutions, as well as communication between the regions of the country.

On the basis of the study, the author concludes that grouping information security offences in a separate section (or sections) of the Special Part is appropriate only in case of a radical reform of the national criminal law system.

Key words: *disposition of the criminal and law provision, crimes against information security, information security, information relations, criminal law, criminal offence in the field of information, criminal law protection, object of the crime, public relations.*