УДК 343.3/.7:004

БОНДАРЕНКО Іван Дмитрович

РОЗМЕЖУВАННЯ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО СТ. 361-2 КК УКРАЇНИ, ІЗ СУМІЖНИМИ СКЛАДАМИ ЗЛОЧИНІВ

Постановка проблеми. Серед науковців, які досліджували проблеми кримінально-правової охорони інформації з обмеженим доступом в Україні, поширена думка, що поява ст. 361-2 у КК України, яка передбачає відповідальність за збут або розповсюдження будь-якого виду інформації з обмеженим доступом за умови її зберігання в «комп'ютерній» формі, створеної та захищеної відповідно до законодавства, призвела до нестабільності положень кримінального закону. Дійсно, відповідальність за посягання на конфіденційність цілої низки видів інформації з обмеженим доступом уже передбачена іншими статтями КК України, розміщеними в кодексі відповідно до родового об'єкта їхніх злочинів – тих суспільних відносин, у сфері яких і виникає та здійснюється обробка кожного із видів інформації (статті 111 (ч. 1), 114 (ч. 1), 132, 145, 158, 159, 163, 168, 182, 231, 232, 232-1, 232-2, 328, 330, 381, 387, 422 КК України).

Цілком обґрунтованим є твердження низки дослідників, що поява ст. 361-2 КК України призвела до виникнення невиправданої конкуренції кримінально-правових норм. На практиці проблема відобразилася в складнощах кримінально-правового оцінювання матеріалів правоохоронних органів і, відповідно, подальшої кваліфікації. Деякі вчені навіть аргументували позицію щодо необхідності виключення ст. 361-2 із КК України. Зазначене свідчить про потребу детальнішого розгляду питання специфіки розмежування злочину, передбаченого ст. 361-2 КК України, із суміжними складами злочину.

Аналіз останніх досліджень і публікацій. Проблему розмежування злочину, передбаченого ст. 361-2 КК України, із суміжними складами злочинів досліджували Д. Азаров, В. Голубєв, С. Дрьомов, М. Карчевський, Д. Музика, Д. Прокоф'єва-Янчиленко, Л. Паламарчук, Н. Розенфельд, М. Рудик, О. Самойлова, О. Шамсутдінов та інші. Але у їхніх наукових роботах це питання висвітлено фрагментарно, без комплексного, системного підходу.

Метою статті є визначення особливостей розмежування злочину, передбаченого ст. 361-2 КК України, із суміжними складами злочинів.

Виклад основного матеріалу. Стаття 361-2 КК України видається такою, що розроблена як спеціальна до наведених вище, оскільки «комп'ютерність» інформації є її додатковою характеристикою, а певний вид інформації з обмеженим доступом у зазначеній формі є вужчим поняттям,

ніж цей вид інформації сам по собі. Це означає, що відповідно до загальних правил кваліфікації у випадку збуту або розповсюдження збереженого в «комп'ютерній» формі із застосуванням певної системи захисту виду інформації з обмеженим доступом, який уже охороняється іншою статтею КК України, діяння має визначатися саме як злочин, передбачений ст. 361-2 КК України. Але детальніший аналіз свідчить про неприпустимість практичного застосування такої логіки.

По-перше, санкція низки зазначених вище кримінально-правових норм є суттєво більшою, ніж та, яка передбачена ст. 361-2 КК України. Тому, наприклад, видається помилковою кваліфікація несанкціонованого збуту або розповсюдження збереженої на комп'ютері та захищеної відповідно до законодавства інформації, що становить державну таємницю, особою, якій вона була довірена, за ст. 361-2 замість ст. 328 КК України. По-друге, виникає слушне запитання: чи дійсно слід говорити про існування якихось окремих суспільних відносин, які зумовлюються фактом збереження інформації з обмеженим доступом саме в «комп'ютерній» формі? Як при збуті чи розповсюдженні «закритої» інформації в паперовій формі, так і в електронній видається, що шкода завдається суспільним відносинам у сфері обігу такої інформації, які суттєво відрізняються за своєю суспільною значущістю та, відповідно, небезпечністю посягань на них залежно від конкретного виду такої інформації. Наприклад, із соціального та правового погляду очевидна відмінність інформації, що становить державну таємницю та має гриф обмеження доступу «цілком таємно», від персональних даних пересічного громадянина. Тому вчені переважно погоджуються із твердженням, що «комп'ютерна» форма представлення інформації сама по собі не може змінювати сутність суспільних відносин, яким завдається шкода у зв'язку з вчиненням злочину, а суспільна небезпека злочину має визначатися саме видом, змістом і категорією інформації, на яку здійснюється посягання [1, с. 118; 2, с. 173]. Дійшовши таких висновків, низка науковців висловлювала досить категоричну позицію щодо необхідності скасування досліджуваної норми. Так, наприклад, Д. С. Азаров стверджував, що саме існування ст. 361-2 КК Уаїни є безпідставним [2, с. 173]. М. В. Карчевський зазначав, що аналізована кримінально-правова норма демонструє «очевидну надлишковість кримінально-правової заборони… існує достатньо аргументів… для виключення ст. 361-2 з КК України» [3, с. 201, 203]. Д. М. Прокоф'єва наголошувала, що «формулювання диспозиції статті 361-2 ККУ не лише являє собою логічний нонсенс, але й може призвести на практиці до нових колізій» [1, с. 118]. Однак слід зазначити, що попри низку суттєвих недоліків аналізованої кримінально-правової норми, її декриміналізація призведе до ще більш негативних наслідків, адже виникне одразу декілька суттєвих прогалин у кримінально-правовому регулюванні, унаслідок чого суспільні відносини у сфері захисту деяких видів інформації з

обмеженим доступом будуть незахищеними, що сприятиме розвитку тіньового ринку такої інформації та негативно позначиться на стані національної безпеки держави загалом. Фактично, приклад злочину, передбаченого чинною статтею 361-2 КК України, специфіка розмежування його із суміжними відображають системну проблему у сфері кримінально-правової охорони інформації з обмеженим доступом в Україні: непослідовність та фрагментарність такої охорони, переоцінювання фактора «комп'ютерної» форми інформації, відсутність уніфікованого термінологічного апарату, який би відображав сучасний стан суспільних відносин у сфері її електронної обробки.

Зокрема, роблячи порівняльний аналіз складу злочину, передбаченого ст. 361-2 КК України, із суміжними, доходимо висновку, що переважна більшість із них:

1) сконструйована лише «під спеціального суб'єкта», тобто особу, якій інформація була довірена чи стала відома за характером роботи; або охоплює передачу інформації певному особливо суспільно небезпечному адресату (іноземній стороні);

2) передбачає обов'язкове настання суспільно небезпечних наслідків.

Водночас суб'єкт аналізованого складу злочину є загальним: ним (так само як і адресатом) може бути будь-яка особа, а момент закінчення злочину (за ч. 1) із настанням суспільно небезпечних наслідків не пов'язується. Це означає, що статті в інших розділах КК України лише фрагментарно захищають суспільні відносини у сфері забезпечення конфіденційності деяких видів інформації з обмеженим доступом, а чинна редакція ст. 361-2 КК України не завжди «дублює» положення таких статей, але в низці випадків поширюється й на ті ситуації, коли діяння не підпадає під ознаки складу злочину за зазначеними вище статтями. Автором доопрацьовано розроблену М. В. Карчевським класифікацію таких випадків і деталізовано її з урахуванням системи видів інформації з обмеженим доступом [3, с. 200]. Кваліфікація діянь винятково за ст. 361-2 КК України має здійснюватись:

1) якщо предметом злочину є державна таємниця: а) її збут або розповсюдження здійснює не спеціальний суб'єкт (особа, якій інформація була довірена або стала відома за характером роботи), а загальний, будь-яка стороння особа (цей випадок не охоплюється статтею 328 КК України, оскільки суб'єкт відповідного складу злочину є спеціальним); б) її збут або розповсюдження здійснюється особою, якій інформація довірена не була, а адресатом не є іноземна держава, іноземна організація або їхні представники або принаймні умислом винного не охоплюється усвідомлення фактичної «іноземної» належності адресата (цей випадок не передбачений статтями 111 (ч. 1), 114 (ч. 1) КК України, оскільки обов'язкових ознак адресата немає) [4, с. 126];

2) якщо предметом злочину є службова інформація: а) така службова інформація була зібрана в процесі оперативно-розшукової, контр-

розвідувальної діяльності, у сфері оборони країни, її передачу здійснює спеціальний суб'єкт (особа, якій інформація була довірена або стала відома за характером роботи), але адресатом не є іноземне підприємство, установа, організація чи їхній представник або принаймні умислом винного не охоплюється усвідомлення фактичної «іноземної» належності адресата (цей випадок не передбачений ст. 330 КК України, оскільки обов'язкових ознак адресата немає); б) така службова інформація була зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності у сфері оборони країни, але її передачу іноземному підприємству, установі, організації чи їхньому представнику здійснює не спеціальний, а загальний суб'єкт (цей випадок не охоплюється статтею 330 КК України, оскільки обов'язкових ознак адресата немає); в) така службова інформація не є зібраною в процесі оперативно-розшукової, контррозвідувальної діяльності у сфері оборони країни, її збут або розповсюдження здійснює як загальний, так і спеціальний суб'єкт, а адресатом є будь-хто, зокрема й іноземна сторона (цей випадок не охоплюється ст. 330 КК України, оскільки обов'язкових ознак, що суттєво звужують зміст предмета злочину, немає);

3) якщо предметом злочину є лікарська, комерційна або банківська таємниця: а) її збут або розповсюдження здійснюється спеціальним суб'єктом, особою, якій інформація була довірена, але тяжкі наслідки / істотна шкода не настали (цей випадок не охоплюється статтями 145, 232 КК України, оскільки немає обов'язкових наслідків); б) її збут або розповсюдження здійснюється загальним суб'єктом, тобто будь-якою сторонньою особою (цей випадок не охоплюється статтями 145, 232 КК України, оскільки спеціальних ознак суб'єкта злочину немає);

4) якщо предметом злочину є відомості про проведення медичного огляду задля виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, відомості про заходи безпеки щодо особи, взятої під захист, дані оперативно-розшукової діяльності, досудового розслідування: збут або розповсюдження такої інформації здійснюється особою, якій вона довірена не була (цей випадок не охоплюється статтями 132, 381, 387 КК України, оскільки спеціальних ознак суб'єкта злочину немає);

5) якщо предметом злочину є таємниця листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, таємниця усиновлення або приватного життя: умислом винного не охоплюється допущення заподіяння шкоди конкретній особі / чітко визначеній групі осіб, натомість здійснюється збут або розповсюдження значного інформаційного масиву, в якому містяться відомості щодо великої, «абстрактної» для адресата кількості людей (цей випадок не охоплюється статтями 163, 168, 182, КК України, оскільки немає ознак складу злочину проти конституційних прав та свобод людини);

6) якщо предметом злочину є інші види інформації з обмеженим доступом, які не охороняються окремими статтями КК України.

Отже, результати проведеного розмежування складу злочину, передбаченого ст. 361-2 КК України, із суміжними вказують на помилковість твердження Д. С. Азарова, що дії, передбачені аналізованою статтею, повністю охоплюються іншими кримінально-правовими нормами (статті 111 (ч. 1), 114 (ч. 1), 232, 328, 330 КК України) [2, с. 173]. Натомість можна констатувати парадоксальну ситуацію: по-перше, ст. 361-2 КК України дійсно створює конкуренцію з низкою наявних кримінально-правових норм, які захищають конфіденційність окремих видів інформації з обмеженим доступом, а, по-друге, вона передбачає відповідальність за передачу інформації з обмеженим доступом за тих обставин, що не охоплюються складом суміжних злочинів. Питання кваліфікації діянь у першому випадку є суперечливим і не може однозначно вирішуватися на практиці. Найбільш виправданою з прикладного погляду видається кваліфікація за сукупністю, де у формулі кваліфікації одна стаття відображатиме суспільну значущість конкретного виду інформації з обмеженим доступом, а інша – факт «комп'ютерної» обробки інформації в захищеній відповідно до законодавства системі.

Думку про необхідність кваліфікації за сукупністю в наведених вище випадках підтримує і М. В. Рудик, зазначаючи, що в разі, наприклад, розповсюдження або збуту відомостей, які становлять особисту або сімейну таємницю, за допомогою використання комп'ютера вчинене повинно бути кваліфіковане за сукупністю злочинів, передбачених статтями 182 та 361-2 КК України, а у випадку несанкціонованого ознайомлення з електронною кореспонденцією особи шляхом злому її інтернет-скриньки та подальшого оприлюднення відповідної інформації в мережі «Інтернет» чи розповсюдження іншим шляхом вчинене повинно бути кваліфіковано за сукупністю статей 163 та 361-2 КК України. За сукупністю статей 361-2 та 111 (або 114) КК України вчений пропонує кваліфікувати й дії особи (громадянина України або, відповідно, іноземця чи апатрида), яка здійснює передачу іноземній стороні державної таємниці, що зберігається в захищеній комп'ютерній системі [5, с. 100–102].

Саме такий підхід у кваліфікації в правовій ситуації, що розглядається, на практиці видається найоптимальнішим, але його не можна вважати ідеальним з юридичного погляду. Як зазначав М. Й. Коржанський, кваліфікація може бути правильною лише тоді, якщо буде застосовано саме ту норму, яка передбачає це діяння, тобто застосовано лише одну й лише певну, конкретну норму. Використання ж винятково статті 361-2 КК України, як це обґрунтовувалося вище, є недоцільним із причини її невідповідності ступеню тяжкості діянь щодо передачі низки видів інформації з обмеженим доступом (зокрема, державної таємниці) і з урахуванням того факту, що «комп'ютерність» інформації не перетворює її на якусь іншу, а шкода злочином завдається саме

тим суспільним відносинам, які пов'язані з виникненням та обробкою кожного конкретного виду інформації з обмеженим доступом.

Суперечливим видається й питання кваліфікації діянь особи, яка, маючи законний доступ до створеної та захищеної згідно з чинним законодавством інформації з обмеженим доступом, що обробляється в комп'ютерній формі, її незаконно копіює і в подальшому збуває. Частина 2 статті 362 КК України передбачає відповідальність спеціального суб'єкта за несанкціоноване перехоплення або копіювання відповідної інформації, якщо це призвело до її витоку. Тобто склад злочину є матеріальним, закінчений із моменту настання суспільно небезпечного наслідку – витоку відповідної інформації. Постає запитання: якщо умислом особи, яка має законний доступ до «закритої» комп'ютерної інформації, охоплюється як її копіювання, так і подальший збут або розповсюдження, наприклад, шляхом розміщення в публічному доступі в мережі «Інтернет», чи мають такі дії додатково кваліфікуватися за ст. 361-2 КК України? У практиці діяльності ДКІБ СБ України непоодинокі випадки документування саме такої ситуації.

Наприклад, у межах кримінального провадження за матеріалами ДКІБ СБ України дії співробітника одного з міністерств, який несанкціоновано копіював службову інформацію з ЄАІС державного органу та збував стороннім особам, кваліфіковані за сукупністю ч. 3 ст. 362, ч. 2 ст. 361-2, ч. 1 ст. 364 КК України. Тобто діяльність із збуту інформації з обмеженим доступом кваліфікована не лише як «копіювання.., що мало наслідком її витік» (ст. 362 КК України), але окремо і як «збут / розповсюдження» (ст. 361-2 КК України), а також як «зловживання владою або службовим становищем» (ст. 364 КК України) [6]. Водночас у подібних випадках є приклади й іншої кваліфікації, а саме – винятково за статтею 362 КК України [7].

Аналіз диспозиції статті 361-2 КК України свідчить, що умисні дії спеціального суб'єкта (який несанкціоновано скопіював захищену «комп'ютерну» інформацію з обмеженим доступом) з ознайомлення чи надання доступу стороннім особам до такої інформації потребують самостійної кримінально-правової кваліфікації за ст. 361-2 КК України та виходять за межі складу злочину, передбаченого ч. 2 ст. 362 КК України. Останній, на думку автора, має не прямий умисел, а змішану форму вини, тобто «копіювання… що призвело до витоку» характеризується прямим умислом щодо копіювання та необережністю щодо витоку. Натомість злочин, передбачений ч. 1 ст. 361-2 КК України, може бути вчинений лише з прямим умислом. Такі помилки у кваліфікації, вірогідно, виникають через певну інертність правоохоронної системи, оскільки до моменту доповнення КК України ст. 361-2, тобто за відсутності спеціальної норми, в аналізованій ситуації відповідні діяння правильно кваліфікувалися за ст. 362 КК України.

Слід звернути увагу й на той факт, що в диспозиції статті 361-2 КК України вказано на обов'язкову ознаку «комп'ютерної» інформації з

обмеженим доступом як предмета злочину: її «створення та захищеність відповідно до чинного законодавства». Виникає запитання: як кваліфікувати дії із несанкціонованого збуту / розповсюдження інформації з обмеженим доступом: 1) яка створена та/або захищена з порушенням вимог українського законодавства; 2) за відсутності будь-яких положень законодавства щодо її захисту, яка захищена власником на свій розсуд, наприклад, шляхом створення захищеної комп'ютерної мережі або шляхом шифрування даних.

Очевидно, що шкоду суспільним відносинам у сфері обігу конкретного виду інформації з обмеженим доступом буде завдано в обох випадках, але ст. 361-2 КК України у своїй чинній редакції однозначно унеможливлює її застосування для захисту таких відносин у першому випадку та суттєво ускладнює у другому. Отже, вказівка ст. 361-2 КК України на таку обов'язкову ознаку інформації як «створення та захищеність відповідно до чинного законодавства» за відсутності належного правового регулювання порядку захисту при комп'ютерній обробці цілої низки різних видів інформації з обмеженим доступом фактично унеможливлює ефективне використання аналізованої кримінально-правової норми для протидії новому виду комп'ютерної злочинності, пов'язаному із функціонуванням тіньового ринку «закритої» інформації.

Таку парадоксальність ситуації, пов'язаної з наявністю статті 361-2 у КК України, найбільш влучно охарактеризував М. В. Карчевський, який указав не лише на її надлишковість, але й одночасно на спричинення статтею суттєвих законодавчих прогалин. Передумовою виникнення цієї проблеми є помилкова оцінка законодавцем правового значення автоматизованої обробки даних, адже дії, що призводять до витоку інформації, незалежно від її форми – будь вона електронна або паперова, – це посягання саме у сфері забезпечення доступу до інформаційного ресурсу. Небезпечність посягання має визначатися суспільною значущістю відносин у сфері обігу конкретного виду інформації з обмеженим доступом, а не інструментом її автоматизованої обробки [3, с. 202–215; 8].

Слід констатувати, що наявні в КК України засоби захисту зазначених відносин не можуть забезпечити ефективну протидію новому, стрімко зростаючому виду злочинності у сфері так званої «тіньової цифрової економіки», оскільки, як це було проілюстровано на прикладі розмежування злочину, передбаченого ст. 361-2 КК України, із суміжними, вони встановлюють лише фрагментарну кримінально-правову охорону зазначеної сфери. Вирішити аналізовану проблему не можна лише декриміналізацією досліджуваного злочину, оскільки розв'язання внаслідок цього одних правових колізій призведе до появи інших. Необхідним є комплексний перегляд наявної системи кримінально-правових норм, які забезпечують охорону суспільних відносин у сфері доступу до інформації, з урахуванням актуальних змін у сфері її комп'ютерної обробки, зумовлених досягненнями науково-технічного прогресу.

Висновки. Злочин, передбачений ст. 361-2 КК України, відрізняється від суміжних (предметом яких є окремі види інформації з обмеженим доступом): а) предметом злочину, ширшим за своїм обсягом, – охоплює всі види інформації з обмеженим доступом (за умови їх створення та захищеності згідно з чинним законодавством); б) загальним суб'єктом злочину – низка суміжних складів злочину передбачає наявність спеціального суб'єкта, тобто особи, якій надано законний доступ до відповідної інформації; в) відсутністю вимог щодо адресата отримання інформації – об'єктивна сторона низки суміжних складів злочинів передбачає дії із передання інформації певному «особливо небезпечному» адресату (іноземна сторона); г) моментом закінчення безвідносно до настання тяжких наслідків чи істотної шкоди – їх настання є необхідною умовою низки суміжних складів злочинів; д) умислом, який спрямований на збут або розповсюдження абстрактного масиву даних, а не особистих відомостей щодо конкретно визначеної особи, що притаманно злочинам проти приватності.

У випадках, коли здійснюється посягання на вид інформації з обмеженим доступом, яка охороняється окремою статтею КК України, але вона збережена в комп'ютерній формі, створена та захищена згідно з чинним законодавством, постає запитання: яку в такому разі норму вважати спеціальною – в якій міститься вказівка на конкретний вид інформації (переважно санкція суттєво більша, ніж за ст. 361-2 КК України) чи на факт її «комп'ютерності»? Низка науковців вказувала, що в такій ситуації виникає невиправдана конкуренція кримінально-правових норм, а саме: існування ст. 361-2 у КК України є необґрунтованим та свідченням надмірної криміналізації. Наукова позиція щодо необхідності вирішення цієї проблеми шляхом виключення аналізованої статті з КК України є помилковою: це призведе до виникнення прогалин у кримінально-правовому регулюванні, оскільки аналізована норма встановлює охорону ширшого кола суспільних відносин, ніж спеціальні, щодо окремих видів інформації та охорону суспільних відносин щодо видів інформації з обмеженим доступом, які жодними іншими кримінально-правовими нормами не охороняються. Зазначене відображає загальну проблему несистемності кримінально-правової охорони інформації з обмеженим доступом в Україні, що актуалізується у зв'язку з поширеністю її комп'ютерної обробки.

Список використаних джерел

1. Прокоф'єва Д. М. Об'єкт та предмет злочинів проти інформаційної безпеки України : дис. … канд. юрид. наук : 12.00.08. Київ, 2006. 269 с.

2. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження). Київ : Атіка, 2007. 304 с.

3. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України. Луганськ : РВВ ЛДУВС імені Е. О. Дідоренка, 2012. 526 с.

4. Самойлова О. С. Кримінально-правова характеристика передачі або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави : дис. … канд. юрид. наук : 12.00.08. Київ, 2006. 255 с.

5. Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : дис. … канд. юрид. наук : 12.00.08. Харків, 2007. 229 с.

6. Вирок Шевченківського районного суду м. Києва від 5 червня 2015 р по справі № 761/9834/15-к. URL: http://www. reyestr. court.gov.ua (дата звернення: 20.04.2020).

7. Бондаренко І. Д. Організаційно-правові засади захисту державних електронних інформаційних ресурсів : оглядове видання. Київ : Наук.-вид. центр НА СБ України, 2015. 103 с.

8. Постанова Славутського міськрайонного суду Хмельницької обл. від 13 червня 2012 р. по справі № 2214/2287/2012. URL: http://www.reyestr.court.gov.ua (дата звернення: 20.04.2020).

Рецензенти:
кандидат юридичних наук
Н. Ткачук,
кандидат юридичних наук
О. Шамсутдінов

Аннотация. В статье раскрыта специфика разграничения преступления, предусмотренного ст. 361-2 УК Украины, со смежными составами преступлений. Раскрыты особенности предмета данного состава преступления и охарактеризованы факторы, которые приводят к неоправданной конкуренции уголовно-правовых норм.

По результатам сравнительного анализа состава преступления, предусмотренного ст. 361-2 УК Украины, со смежными составами преступлений, выделены и систематизированы их отличительные критерии в зависимости от конкретного вида информации, являющейся предметом преступления. Обосновано, что большинство смежных составов преступлений сконструированы или «под специального субъекта», или охватывает передачу информации определенному особенно общественно опасному адресату (иностранной стороне), или предусматривает обязательное наступление общественно опасных последствий.

Раскрыта специфика квалификации действий по несанкционированному сбыту /

Abstract. The article is dedicated to the specifics of distinction between the crime provided by Art. 361-2 of the Criminal Code of Ukraine and related crimes. Specifics of the subject of this corpus delicti are revealed. Factors resulting in unjustified conflict of laws are studied.

Based on the results of a comparative analysis of the corpus delicti under Art. 361-2 of the Criminal Code of Ukraine, with related elements of crimes, their distinctive criteria are identified and systematized depending on the specific type of information that is the subject of the crime. It is stated that the vast majority of related crimes are designed «to fit a special subject», or include the transfer of information to a particularly dangerous addressee (foreign party), or result inevitably in socially dangerous consequences.

The article also presents specifics of qualifying actions for unauthorized sale / dissemination of classified information which:

1) is created and / or protected in violation of Ukrainian law;

2) in case of absence of any legal provisions for its protection, is protected by the owner at his / her own discretion, for example,

распространению информации с ограниченным доступом, которая:

1) создана и / или защищена с нарушением требований украинского законодательства;

2) при отсутствии каких-либо положений законодательства о ее защите охраняется владельцем на свое усмотрение, например, путем создания защищенной компьютерной сети или путем шифровки данных.

Определены особенности разграничения преступления, предусмотренного ст. 361-2 УК Украины, со смежными в зависимости от вида информации с ограниченным доступом в качестве предмета преступления.

Обосновано, что декриминализация преступления, предусмотренного ст. 361-2 УК Украины, как это предлагали некоторые ученые, приведет к еще более негативным последствиям, ведь возникнет сразу несколько существенных пробелов уголовно-правового регулирования общественных отношений в сфере защиты отдельных видов информации с ограниченным доступом.

В результате проведенного исследования обосновано, что возникает необходимость комплексного пересмотра существующей системы уголовно-правовых норм, обеспечивающих защиту общественных отношений в сфере доступа к информации, с учетом актуальных изменений в сфере ее «компьютерной» обработки, связанных с достижениями научно-технического прогресса.

Ключевые слова: информация с ограниченным доступом, преступление, сбыт, распространение.

by creating a secure computer network or by encrypting data.

The particularities of making distinction between the crime under Art. 361-2 of the Criminal Code of Ukraine and relates crimes depending on the type of classified information as a subject of the crime.

It is substantiated that decriminalization of the crime under Art. 361-2 of the Criminal code of Ukraine, as it is proposed by some scientists, will lead to negative consequences, because there will be several significant gaps in criminal law regulation of public relations concerning certain types of information protection.

As a result of research it is substantiated that it is necessary to conduct comprehensive review of the system of criminal law standards for the protection of social relations in the field of access to information taking into account significant changes in the sphere of information computer processing following the science and technology achievements.

Key words: classified information, crime, sale, dissemination.