ОДЕСЬКА НАЦІОНАЛЬНА ЮРИДИЧНА АКАДЕМІЯ

РУДИК МИХАЙЛО ВІКТОРОВИЧ

УДК 343.2.01

НЕЗАКОННИЙ ЗБУТ, РОЗПОВСЮДЖЕННЯ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Спеціальність 12.00.08 – кримінальне право та кримінологія;
кримінально-виконавче право

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата юридичних наук

Одеса – 2007

Дисертацією є рукопис.

Робота виконана в Харківському національному університеті внутрішніх справ. Міністерства внутрішніх справ України.

Науковий керівник: кандидат юридичних наук
АЛЬОШИН Дмитро Петрович,
Харківський національний університет внутрішніх справ,
доцент кафедри кримінального права і кримінології;

Офіційні опоненти: доктор юридичних наук, професор
ГЛУШКОВ Валерій Олександрович,
Київський національний університет імені Тараса Шевченка,
завідувач кафедри кримінального права та кримінології;

кандидат юридичних наук, доцент
ВАРТИЛЕЦЬКА Інна Анатоліївна
Київський національний університет внутрішніх справ,
професор кафедри кримінального права

Захист відбудеться "__" __ 2007 р. о "_" годині на засіданні спеціалізованої вченої ради Д 41.086.01 Одеської національної юридичної академії за адресою: 65009, м. Одеса, вул. Фонтанська дорога, 23.

З дисертацією можна ознайомитись у бібліотеці Одеської національної юридичної академії за адресою: 65009, м. Одеса, вул. Піонерська, 2.

Автореферат розісланий "_" 2007 р.

Учений секретар
спеціалізованої вченої ради Л.Р. Біла

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Однією з рис сучасного суспільства є бурхливий розвиток науково-технічного прогресу взагалі й електронно-обчислювальної техніки, зокрема. Розвиток інформаційної сфери, забезпечення її безпеки стають одними з пріоритетних завдань національної політики розвинених країн світу. Як вважають фахівці, за темпами розвитку, за впливом на соціально-економічну інфраструктуру, за внеском у науково-технічну революцію мікроелектронна й комп'ютерна галузі промисловості, що становлять базу інформаційного простору будь-якої країни, не мають аналогів. І на сьогоднішній день вони стали одними з потужних і наукомістких у світі. Розвиток інформаційної сфери, забезпечення її безпеки стає одним із пріоритетів національної політики України. Однак використання електронно-обчислювальної техніки породило не тільки технічні, але й правові проблеми. Серйозним негативним наслідком цього явища для суспільства є так звані «комп'ютерні злочини». Ця проблема внаслідок інформатизації всіх сторін діяльності суспільства стає все гострішою. Так, якщо протягом 2002–2006 р. підрозділами ДСБЕЗ розкрито 2535 злочинів, що посягали на комп'ютерну інформацію (у 2002 р. було розкрито 311 злочинів (з яких до суду направлено 266), у 2003 – 464 (з яких до суду направлено 290), у 2004 – 562 (з яких до суду направлено 367), то у 2005 р. – 615 (з яких до суду направлено 364), а в 2006 р. – 583 (з яких до суду направлено 415) злочини. Найбільшу питому вагу мають злочини у сфері комп'ютерних та Інтернет-технологій – 29%, у сфері функціонування електронних платежів або платіжних карток – 15%; у сфері телекомунікацій – 24%.

Науково-теоретичною базою дисертаційного дослідження та сформульованих висновків щодо комп'ютерної інформації з обмеженим доступом, стали праці таких учених-юристів, як Д.С. Азаров, Д. Айков, П.П. Андрушко, П.Д. Біленчук, К.І. Беляков, Г.М. Борзенков, І.А. Вартилецька, О.Г. Волеводз, Б.В. Волженкін, А.Ф. Волобуєв, В.О. Голубєв, М.В. Гуцалюк, В.О. Глушков, О.О. Дудоров, Б.А. Кормич, Ю.І. Ляпунов, В.А. Мазуров, А.А. Музика, С.О. Орлов, І.В. Смолькова, Є.Л. Стрельцов та ін. Широко використовувалися отримані у цих роботах результати, а також загальнотеоретичні положення кримінального права, які розроблялися такими вченими, як М.І. Бажанов, Б.С. Волков, С.В. Дьяков, І.Я. Козаченко, В.С. Комісаров, М.Й. Коржанський, В.М. Кудрявцев, Н.Ф. Кузнєцова, Б.С. Нікіфоров, М.І. Мельник, П.П. Михайленко, О.І. Рарог, В.Я. Тацій, М.І. Панов, М.І. Хавронюк, С.С. Яценко та ін. Разом із тим, в науці дуже мало приділялося уваги дослідженню питань незаконного одержання, поширення й використання як комп'ютерної інформації в цілому, так і окремих її видів, не сформульоване також правове визначення таємниці. Існуючі в юридичній літературі визначення таких інститутів, як комерційна, банківська таємниці, мають суперечливий, розпливчастий характер, що також обумовило актуальність та необхідність здійснення дисертаційного дослідження. Актуальність обраної теми обумовлюється й тим, що до Кримінального кодексу України включено нові, не відомі колишньому кримінальному законодавству норми, які передбачають відповідальність за посягання на комп'ютерну інформацію з обмеженим доступом. Так, Законом України від 23 грудня 2004 р. КК України було доповнено ст. 361^2 «Несанкціоновані збут або розповсюдження інформації з обме-

женим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації». Зазначені нововведення у Кримінальному кодексі України вимагають теоретичного осмислення не тільки термінологічного апарату окремих видів таємниць, аналізу відповідних складів злочинів, але й комплексного, системного дослідження злочинів, що посягають на один із перерахованих видів таємниць, вчинених за допомогою засобів комп'ютерної техніки. Наведені обставини зумовили вибір теми дисертаційного дослідження, її теоретичну та практичну значимість.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконано відповідно до п. 1.6 рекомендованих відділенням кримінально-правових наук Академії правових наук України, пріоритетних напрямків розвитку правової науки України на 2005–2010 рр., (затверджені Загальними зборами АПрН України 09.04.2004 р.), п. 2.4 "Пріоритетних напрямків наукових та дисертаційних досліджень, які потребують першочергового розроблення і впровадження в практичну діяльність органів внутрішніх справ, на період 2004 – 2009 рр.", (затверджені наказом МВС України № 755 від 05.07.2004 р.), і пп. 1.1, 5.3 "Пріоритетних напрямків наукових досліджень Харківського національного університету внутрішніх справ на 2006–2010 рр." і є складовою планів наукових досліджень кафедри кримінального права та кримінології Харківського національного університету внутрішніх справ.

Мета і задачі дослідження. Метою дослідження є формулювання єдиного підходу до питань застосування норм кримінального права та вирішення актуальних питань кваліфікації злочинних посягань на комп'ютерну інформацію з обмеженим доступом, розробка рекомендацій щодо вдосконалення чинного кримінального законодавства та правозастосовчої практики.

Відповідно до поставленої мети в дисертації розв'язано такі основні задачі:

досліджено законодавче регулювання різних видів таємниць, закріплених у вітчизняному та зарубіжному кримінальному законодавстві;

проаналізовано окремі види таємниць і визначено їх класифікацію;

здійснено системний та порівняльний аналіз складів злочинів, які передбачають відповідальність за посягання на таємницю: приватного життя, комерційну, банківську, державну;

розглянуто дискусійні питання кваліфікації злочинів, пов'язаних з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом;

розроблено пропозиції щодо вдосконалення чинного законодавства у сфері кримінально-правової охорони комп'ютерної інформації з обмеженим доступом.

Об'єктом дослідження є суспільні відносини, пов'язані з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом.

Предметом дослідження є незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом.

*Методи дослідження***.** Поряд із загальнонауковими методами пізнання (аналіз, синтез та ін.) були використані спеціальні методи: формально-логічний метод (надав можливість проаналізувати положення кримінально-правової доктрини, зокрема щодо злочинів у сфері незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом); метод системно-структурного аналізу (за його

допомогою досліджено ознаки складів злочинів, які передбачають відповідальність за посягання на конфіденційну інформацію, яку становлять таємниці приватного життя, комерційна, банківська, державна тощо); метод формально-догматичного аналізу (за його допомогою здійснено тлумачення відповідних кримінально-правових норм, що передбачають кримінальну відповідальність за незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом, окремих понять і термінів); порівняльно-правовий метод (використовувався при аналізі кримінально-правових норм законодавства окремих зарубіжних країн, які передбачають відповідальність за злочини у сфері незаконного збуту, розповсюдження конфіденційної комп'ютерної інформації), метод соціологічного опитування (використано для вивчення особливостей практики застосування норм КК України практичними працівниками підрозділів ОВС України у сфері протидії незаконному збуту, розповсюдженню комп'ютерної інформації з обмеженим доступом).

Нормативно-теоретичною базою дослідження є Конституція України, Кримінальний кодекс України, інші закони України щодо протидії незаконному збуту, розповсюдженню комп'ютерної інформації з обмеженим доступом, законодавства зарубіжних країн, а також наукова література з кримінального права, кримінології, міжнародного права, цивільного права.

Наукова новизна одержаних результатів. Дисертація є першим в Україні комплексним монографічним дослідженням, присвяченим проблемам, що пов'язані з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом.

На базі результатів дослідження сформульовано нові наукові положення, висновки та рекомендації:

вперше:

надано авторське визначення правового поняття незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом. Під незаконним збутом слід розуміти будь-які безоплатні чи оплатні форми реалізації комп'ютерної інформації з обмеженим доступом, у зв'язку з чим вона переходить у власність або розпорядження іншої особи. Під незаконним розповсюдженням комп'ютерної інформації з обмеженим доступом мається на увазі її опублікування, показ, а також інші дії, внаслідок яких інформація стає надбанням інших осіб;

запропоновано класифікацію комп'ютерної інформації за такими критеріями: 1) ступінь таємності; 2) суб'єкт інформаційних відносин, якому фактично належить така інформація. Окрім цього, надано класифікацію злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом за допомогою родового об'єкта злочину. В залежності від цих критеріїв виділено три групи таємниць: 1) приватного життя; 2) комерційна та банківська; 3) державна;

визначено основний безпосередній об'єкт злочину, передбаченого ст. 361^2 КК України, під яким розуміють суспільні відносини у сфері обігу комп'ютерної інформації щодо правомірного здійснення особою інформаційної діяльності стосовно комп'ютерної інформації, що становить одну з груп таємниць – таємницю приватного життя, комерційну, банківську та державні таємниці;

удосконалено: дослідження ознак об'єктивної сторони складів злочинів у сфері незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом;

набули подальшого розвитку:

аргументи щодо необхідності разом з речами матеріального світу визнавати предметом злочину й інші матеріальні утворення, зокрема комп'ютерну інформацію, що зафіксована на матеріальному носієві. На підставі цього зроблено висновок, що предмет є обов'язковою ознакою всіх аналізованих складів злочинів та одним із визначальних критеріїв при відмежуванні від суміжних посягань;

ідеї про те, що поняттям «істотної» шкоди, що передбачене у ч. 2 ст. 232 КК України, слід вважати: банкрутство, ліквідацію організації, припинення діяльності приватного підприємця, скорочення робочих місць, значні збої в роботі податкових і митних органів, заподіяння шкоди здоров'ю людей.

Практичне значення одержаних результатів. Основні положення та результати дисертаційного дослідження можуть бути використані у:

законотворчості – в процесі подальшого удосконалення ст.ст. 361–363 Кримінального кодексу України та при підготовці постанов Пленуму Верховного Суду України з питань, пов'язаних з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом;

науково-дослідницькій діяльності – для подальшого вивчення питань, пов'язаних з кримінально-правовою характеристикою незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом;

навчальному процесі, при викладанні курсу кримінального права, а також при підготовці навчально-методичних матеріалів з теорії кримінального права.

Висновки та пропозиції дисертаційного дослідження можуть бути використані: при вдосконаленні Кримінального кодексу України в частині, що передбачає відповідальність за злочини у сфері незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом; при викладанні курсу кримінального права; при підготовці навчально-методичних матеріалів з теорії кримінального права, а також у практичній діяльності підрозділів Департаменту державної служби боротьби з економічною злочинністю МВС України

Особистий внесок здобувача. В опублікованій у співавторстві з Д.П. Альошиним статті "Міжнародний досвід протидії незаконному збуту та розповсюдженню конфіденційної інформації" здобувачеві належать запропоновані обґрунтування щодо пропозицій з удосконалення вітчизняного кримінального законодавства в частині кримінально-правової охорони таємниці.

Апробація результатів дослідження. Основні положення та висновки дисертаційного дослідження доповідалися та обговорювалися на засіданнях кафедри кримінального права та кримінології Харківського національного університету внутрішніх справ; у виступах на міжнародній науково-практичній конференції «Кримінальний кодекс України 2001 року: проблеми застосування і перспективи удосконалення» (7–8 квітня 2006 р., м. Львів); науково-практичній конференції «Актуальні проблеми сучасної науки в дослідженнях молодих вчених» (12 травня 2006 р., м. Харків).

Публікації. Основні результати дисертаційного дослідження оприлюднені у семи статтях, п’ять із яких опубліковані у наукових фахових виданнях, що входять до переліку, затвердженого ВАК України, та у двох тезах виступів на конференціях.

Структура дисертації обумовлена метою й предметом дослідження, відповідає логіці наукового пошуку й вимогам ВАК України, складається зі вступу, трьох розділів, семи підрозділів, висновків, списку використаних джерел, додатків. Загальний обсяг роботи складає 180 сторінок, список використаних джерел складає 213 найменувань і міститься на 18 сторінках, додатки – 14 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** обґрунтовується актуальність теми дослідження та визначається ступінь наукової розробки теми, зв’язок з науковими програмами, планами, темами, мета та завдання, об’єкт, предмет і структура дослідження, формулюється його методологічна основа, підкреслюється наукова новизна і практичне значення, наводиться апробація результатів дослідження.

Перший розділ «Порівняльно-правовий аналіз норм, що передбачають кримінальну відповідальність за незаконний збут, розповсюдження комп’ютерної інформації з обмеженим доступом у зарубіжних країнах» складається з двох підрозділів.

У ***підрозділі 1.1. «Порівняльний аналіз кримінального законодавства США та деяких європейських країн у сфері незаконного збуту, розповсюдження комп’ютерної інформації з обмеженим доступом»*** піддаються кримінально-правовому аналізу нормативні бази таких високорозвинутих країн, як США, Велика Британія, Португалія, Німеччина, Франція, Швейцарія, Іспанія, Італія, Голландія, Японія та Китайська Народна Республіка. Цілеспрямоване вивчення кримінальних кодексів дозволило здійснити аналіз стану розробки проблеми захисту комп’ютерної інформації з обмеженим доступом у цих країнах. На підставі результатів аналізу зроблено певні висновки щодо удосконалення вітчизняного кримінального законодавства щодо захисту комп’ютерної інформації з обмеженим доступом. Так, кримінальні законодавства технологічно розвинутих країн мають як позитивний характер, так і містять певні недоліки у протидії незаконному збуту, розповсюдженню комп’ютерної інформації з обмеженим доступом. Основним недоліком більшості зарубіжних кримінальних кодексів у частині охорони суспільних відносин щодо розповсюдження інформації з обмеженим доступом є те, що більшість з проаналізованих диспозицій містять ознаку, за якої порушення кримінальної справи можливе лише на підставі скарги потерпілого, тобто це справи приватного обвинувачення. У кримінальних кодексах деяких країн нічого не говориться про захист банківської таємниці.

А якщо такий склад є, то кримінально караним є лише збут таких відомостей, але збирання конфіденційної інформації кримінальної відповідальності цими кодексами не передбачається. Спостерігається також негативне явище, коли потерпіла сторона (власник комп’ютерної системи) не зацікавлена повідомляти правоохоронні органи про факти скоєння протиправних посягань на комп’ютерну інформацію з обмеженим доступом, що знаходиться у його власності.

У ***підрозділі 1.2. «Розвиток законодавства, що регулює кримінально-правові відносини, пов'язані з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом у деяких пострадянських країнах»*** піддаються аналізу законодавчі бази, що регулюють кримінально-правові відносини, пов'язані з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом у деяких пострадянських країнах. Зокрема це Російська Федерація, Республіки Казахстан, Білорусь, Латвійська Республіка. Цей аналіз є дуже важливим, тому що формування їхніх кримінальних законодавств відбувалося у приблизно рівних умовах після розпаду СРСР. Для повного та об'єктивного аналізу кримінальних кодексів цих країн було вивчено модельний кримінальний кодекс держав – учасниць Співдружності Незалежних Держав, який було прийнято 17 лютого 1996 р. в Санкт-Петербурзі. У кримінальних кодексах пострадянських країн та модельному кримінальному кодексі СНД насамперед були розглянуті склади злочинів, які передбачають кримінальну відповідальність за посягання на комп'ютерну інформацію з обмеженим доступом, та їх співвідношення з чинним КК України. На підставі аналізу зроблено висновок, що прийнятий Модельний кримінальний кодекс країн-учасниць СНД, кримінальні кодекси Російської Федерації, Республік Казахстан, Білорусь, Латвійської Республіки мають дуже важливе значення для кримінально-правової охорони суспільних відносин у сфері використання комп'ютерної інформації з обмеженим доступом. Поряд з недоліками вони мають і переваги над чинним кримінальним законодавством України у сфері охорони комп'ютерної інформації з обмеженим доступом. Наприклад, у 1996 р. у Модельному кримінальному кодексі країн – учасниць СНД у статті, що передбачає кримінальну відповідальність за незаконне одержання інформації, яка становить комерційну або банківську таємницю (ст. 269), та розголошення комерційної або банківської таємниці (ст. 270) у диспозиціях цих норм вже була зазначена така ознака об'єктивної сторони, як незаконне проникнення в комп'ютерну систему або мережу. Якщо, наприклад, порівняти цю норму зі ст. 232 КК України, то така дія як незаконне розголошення комерційної та банківської таємниці за допомогою комп'ютера не знайшла свого відображення. Хоча, водночас, ст. 163 КК України містить у складі об'єктивних ознак таку дію на відміну від ст. 153 Модельного кримінального кодексу країн-учасниць СНД. Стаття 289, яка передбачає кримінальну відповідальність за неправомірне заволодіння комп'ютерною інформацією, також як і ст. 361^2 КК України, предмет злочину розкриває не повною мірою. Таким чином, кримінальне законодавство названих вище пострадянських країн і КК України у сфері охорони комп'ютерної інформації з обмеженим доступом знаходиться на стадії розробки та становлення, а зміни, що сьогодні відбуваються, є лише першим кроком на шляху врегулювання та захисту суспільних відносин у сфері використання комп'ютерної інформації з обмеженим доступом.

Другий розділ «Кримінально-правова характеристика об'єктивних ознак незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом» складається з трьох підрозділів.

У ***підрозділі 2.1. «Поняття та класифікація комп'ютерної інформації з обмеженим доступом»*** надаються поняття та класифікація комп'ютерної інформації з обмеженим доступом. Акцентується увага на знаходження балансу між забезпеченням таємниці й забезпеченням права на інформацію; правову охорону відомостей, що становлять таємницю, й відповідальності за посягання на таємницю; розголошення конфіденційних відомостей і відомостей, що становлять державну таємницю; погодженості правового регулювання охорони таємниці в різних галузях законодавства. Розв'язання цих проблем деякою мірою пов'язане з чітким визначенням загального поняття "таємниця" та винайденням класифікаційних критеріїв, за допомогою яких можна об'єднати ті чи інші таємниці в групи з метою їх подальшого вивчення. Нині в українському законодавстві є відсутнім загально-правове поняття таємниці. У науковій літературі при визначенні окремих видів таємниць висловлюються спірні, часом суперечливі погляди. У ряді визначень є відсутніми чіткі ознаки таємниці, що, безумовно, ускладнює формування правильної правової оцінки, кваліфікації у випадку посягання на таємниці, що охороняються законом. Вітчизняне законодавство не має єдиного нормативно-правового акта, який систематизував би та визначав перелік інформації, яка є конфіденційною. На сьогоднішній день окремі питання обмеження обігу й розповсюдження конфіденційної інформації регулюються нормами Конституції України і багатьох інших галузей та інститутів права. Усе це свідчить про необхідність теоретичного осмислення та розробки єдиних класифікаційних критеріїв, за допомогою яких стануть можливими чітке розмежування інформації з обмеженим доступом та визначення ознак, за якими їх можна об'єднати в ті чи інші масиви конфіденційної інформації або групи з метою їх подальшої класифікації для полегшення їх теоретичного дослідження та практичного застосування. Уперше здійснено класифікацію комп'ютерної інформації за такими критеріями: 1) за ступенем таємності; 2) за суб'єктом інформаційних відносин, якому фактично належить така інформація. Окрім цього надано класифікацію складів злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом за допомогою родового об'єкта злочину. В залежності від цих критеріїв виокремлено три групи таємниць: приватного життя, комерційна, банківська та державна.

Серед перерахованих критеріїв на особливу увагу заслуговує останній. Так, за родовим об'єктом в Особливій частині Кримінального кодексу України побудовані та об'єднані склади злочинів, що регулюють суспільні відносини у різних сферах життя. У чинному законодавстві чітко зазначені такі групи таємниць, як державна, банківська та комерційна. Однак у ньому нічого не говориться про таку групу відомостей, як таємниця приватного життя. За допомогою вищезазначених класифікаційних критеріїв, особливо завдяки останньому, можливо визначити наявність такої групи відомостей.

У ***підрозділі 2.2. «Об'єкт та предмет незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом»*** розглядаються питання об'єкта та предмета незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом. Зокрема, висвітлено основні підходи до визначення змісту об'єкта та предмета злочину. Значення об'єкта для складів злочинів, що посягають

на таємницю, полягає в такому. По-перше, за родовим об'єктом виділені конкретні види таємниць, що охороняються кримінальним законом: приватного життя, комерційна, банківська, державна, а також здійснено включення цих складів злочинів до відповідних розділів Особливої частини КК України. По-друге, ці розділи сформульовані у певній послідовності, що відповідає новій ієрархії цінностей в українському суспільстві: особистість – суспільство – держава – кримінально-правовий захист таємниці приватного життя (розд. 5, ст.ст. 159, 163, 168, 182), комерційна й банківська таємниці (розд. 7, ст.ст. 231, 232), державна таємниця (розд. 1, ст.ст. 111, 114; розд. 14, ст.ст. 328, 329; розд. 19, ст. 422). Основним безпосереднім об'єктом злочинних посягань необхідно визнавати окремі суспільні відносини у сфері обігу комп'ютерної інформації, яка має обмежений доступ щодо правомірного здійснення певною особою інформаційної діяльності стосовно комп'ютерної інформації, яка становить один із блоків таємниць (приватного життя, комерційна, банківська та державна таємниці), та якій завдано шкоди конкретним злочинним посяганням (злочином). Додатковим безпосереднім об'єктом злочинів у сфері обігу комп'ютерної інформації з обмеженим доступом є відносини власності щодо цієї комп'ютерної інформації. Факультативним безпосереднім об'єктом аналізованих посягань можуть бути суспільні відносини, у сфері яких здійснюється інформаційна діяльність щодо захисту комп'ютерної інформації з обмеженим доступом (наприклад, при незаконному розголошенні відомостей, які становлять комерційну таємницю, факультативним безпосереднім об'єктом виступають відносини у сфері захисту честі та ділової репутації особи). Об'єктом злочину, передбаченого ст. 361^2 КК України, є встановлений відповідними законодавчими актами порядок користування інформацією, яка має обмежений доступ, а також право володіння такою інформацією. Важливе, а часом вирішальне, значення для кваліфікації конкретних складів злочинів, у тому числі й злочинів, що посягають на таємницю, є предмет злочину. При аналізі кримінально-правових норм, що передбачають кримінальну відповідальність за посягання на один із трьох блоків таємниць закономірно випливає, що предметом цих злочинів є комп'ютерна інформація, яка становить один із цих блоків (приватного життя, комерційна, банківська та державна таємниці). Тобто предметом складів цих злочинів є відомості, що віднесені відповідними особами та державними органами до тієї чи іншої таємниці, які, у свою чергу, мають оцифрований вигляд та знаходяться у пам'яті комп'ютера чи на зовнішніх запам'ятовуючих пристроях (наприклад, лазерні диски, дискети, USB флеш накопичувачі). Предметом вищезазначеного злочину необхідно розуміти інформацію з обмеженим доступом, яка створена та захищена відповідно до чинного законодавства. Однак у цьому визначенні бракує такої ознаки, як комп'ютерна інформація, адже саме цей критерій свідчить про те, що не вся інформація з обмеженим доступом може бути предметом злочину, передбаченого ст. 361^2 КК України.

У ***підрозділі 2.3. «Об'єктивна сторона незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом»*** досліджуються питання об'єктивної сторони незаконного збуту та розповсюдження комп'ютерної

інформації з обмеженим доступом. Об'єктивна сторона злочинів, предметом яких є таємниця (приватного життя, комерційна, банківська, державна), переважно характеризується активними діями, хоча є склади об'єктивних сторін складів злочинів, які характеризуються як дією, так і бездіяльністю (ст.ст. 159, 329, 422). Найбільш поширеними способами є збирання, розповсюдження та використання. Розголошення зазначених відомостей здійснюється усно, письмово, за допомогою каналів зв'язку, у засобах масової інформації по комп'ютерних та телекомунікаційних мережах. Об'єктивна сторона ст. 361^2 КК України полягає у вчиненні несанкціонованого збуту або розповсюдженні комп'ютерної інформації з обмеженим доступом, яка створена та захищена відповідно до чинного законодавства. При цьому, на думку деяких авторів, обов'язковою умовою є знаходження інформації з обмеженим доступом в ЕОМ (комп'ютерах), комп'ютерних мережах або на носіях такої інформації. Несанкціонований збут означає будь-які безоплатні чи оплатні форми реалізації комп'ютерної інформації з обмеженим доступом, унаслідок чого вона переходить у власність або розпорядження іншої особи. Причому збут утворює склад злочину, передбаченого ст. 361^2 КК України, лише за умови, якщо він вчиняється несанкціоновано, тобто з порушенням вимог чинного законодавства, що регулює питання обігу комп'ютерної інформації з обмеженим доступом. Під розповсюдженням комп'ютерної інформації з обмеженим доступом розуміється її опублікування, показ, а також інші дії, унаслідок яких ця інформація стає надбанням інших осіб. З аналізу найбільш розповсюджених способів підготовки та скоєння злочину, передбаченого ст.ст. 361, 361^2 КК України, випливає, що чіткої межі між ними немає. Деякі із зазначених способів виконують роль допоміжних, які, у свою чергу, працюють на основний, що обрав злочинець, виходячи з конкретної злочинної мети та обставин суспільно-небезпечного діяння. Вищенаведені способи неправомірного доступу до комп'ютерної інформації повинні бути враховані працівниками правоохоронних і судових органів при кваліфікації та розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, а також мереж електрозв'язку.

Третій розділ «Кримінально-правова характеристика суб'єктивних ознак незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом» містить два підрозділи.

У ***підрозділі 3.1. «Суб'єктивна сторона незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом»*** досліджено питання суб'єктивної сторони незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом. Суб'єктивна сторона складів злочинів, що передбачають кримінальну відповідальність за незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом характеризуються прямим умислом, спеціальною метою – розголошення або використання цих відомостей, а також мотивом – корисливою або іншою особистою зацікавленістю. Підкреслюється, що для визначення виду умислу необхідно враховувати мотив вчинення даного злочину. Найбільш поширеними мотивами такого злочину є користь, заздрість або інша особиста зацікавленість, прагнення до одержання особистої матеріальної вигоди шляхом незаконного розголошення або, тим більше, використання чужих секретів, помста,

заздрість, образа, родинні й товариські спонукання, бажання догодити близькій людині та ін. Суб'єктивна сторона ст. 361^2 КК України характеризується прямим умислом, а також мотивами – корислива, особиста зацікавленість, низинні спонукання. Ці мотиви є притаманними більшості складів злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом, на основі чого можна зробити висновок, що злочинець має такі ж самі цілі та наміри щодо протиправних дій, спрямованих на незаконний збут, розповсюдження комп'ютерної інформації, які становлять таємницю приватного життя особи.

Суб'єктивна сторона несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації порівняно з суб'єктивною стороною незаконного розголошення комп'ютерної інформації, що становить комерційну або банківську таємницю, співпадає в частині умислу (прямого) та спеціальної мети – розповсюдження або збут цих відомостей, а також мотиву – корисливою або іншою особистою зацікавленістю.

Отже, незаконне розповсюдження, збут відомостей, що становлять таємницю приватного життя (ст.ст. 182, 163, 159, 168 КК України), комерційну, банківську таємницю (ст.ст. 231, 232 КК України) і державну таємницю (ст.ст. 111, 114, 328 КК України), вчинених за допомогою комп'ютера, характеризується умисною формою вини (прямий умисел), корисливими мотивами, іншою особистою зацікавленістю або іншими низинними спонуканнями (ст.ст. 182, 168, ст. 232 КК України), метою – розголошення або незаконне використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК України), використання відомостей на шкоду зовнішній безпеці України (ст.ст. 111, 114 КК). Суб'єктивна сторона розголошення державної таємниці за ст. 328 КК України характеризується як умисною, так і необережною формою вини. Суб'єктивна сторона втрати документів, що містять державну таємницю, передбачена ст. 329 КК України і характеризується лише необережною формою вини.

У ***підрозділі 3.2. «Суб'єкт незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом»*** досліджуються питання суб'єкта незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом. Особливістю суб'єкта у розглянутих складах є те, що ним може бути як особа, що не має доступу до відомостей, які становлять таємницю (незаконне одержання), так і навпаки, суб'єктом розголошення таємниці приватного життя, комерційної, банківської, державної, а також втрати документів, що містять державну таємницю, може бути тільки особа, якій таємниця довірена по службі, роботі, у розпорядженні якої перебували документи, предмети, що містять відомості, віднесені до таємниці.

ВИСНОВКИ

В результаті дослідження комплексу проблем, пов'язаних з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом, сформульовані основні теоретичні положення і пропозиції, спрямовані на удосконалення відповідних норм чинного кримінального законодавства України.

1. Для вирішення питань щодо кваліфікації злочинних посягань на комп'ютерну інформацію з обмеженим доступом необхідно удосконалити диспозицію ст. 361^2, а саме, конкретизувати та назвати види інформації з обмеженим доступом. При такому підході незаконний збут, розповсюдження комерційної та банківської таємниці вчинені за допомогою комп'ютера, слід кваліфікувати за сукупністю ст. 232 та ст. 361^2 КК України. Цей варіант є доцільним, оскільки за такою кваліфікацією охоплюється як предмет злочину, так і спосіб вчинення злочинних дій.

2. Порівняльний аналіз кримінально-правового захисту таємниці у вітчизняному та зарубіжному законодавстві дозволяє зробити деякі висновки, що не претендують на винятковість і, безумовно, мають спірні позиції, припущення з удосконалення українського кримінального законодавства в частині кримінально-правового захисту таємниці. Основним недоліком більшості кримінальних кодексів у частині охорони суспільних відносин щодо розповсюдження конфіденційної інформації є те, що більшість з проаналізованих диспозицій містять таку ознаку, як порушення кримінальної справи стосовно злочинів, які посягають на таємницю можливо лише за умови наявності скарги потерпілого. Тобто це справи приватного обвинувачення. У кримінальних кодексах деяких країн нічого не говориться про захист банківської таємниці. Але, якщо такий склад є, то кримінально караним є лише збут таких відомостей. Стосовно ж дій щодо збору конфіденційної інформації кримінальна відповідальність не встановлюється. Спостерігається також значний відсоток латентності серед цього роду злочинів, яка обумовлена тим, що потерпіла сторона (власник комп'ютерної системи) не зацікавлена в інформуванні правоохоронних органів про факти скоєння протиправних посягань на комп'ютерну інформацію з обмеженим доступом, що знаходиться у її власності.

3. Вивчення диспозиції ст. 361^2 КК України дозволяє зробити висновок, що вона є бланкетною, а щодо визначення терміна «інформація з обмеженим доступом» відсилає до ст. 30 Закону України «Про інформацію». Однак формулювання визначення вищезазначеного терміну у ст. 30 не є чітким, недостатньо приділено уваги таким інститутам, як таємниця приватного життя, професійна, комерційна та банківська. Отже, існує потреба подальшої конкретизації не тільки інституту державної таємниці, але й таємниці приватного життя, професійної, комерційної та банківської як видів інформації з обмеженим доступом.

4. Запропоновано авторське визначення основного безпосереднього об'єкта злочину, передбаченого ст. 361^2 КК України, під яким слід розуміти суспільні відносини у сфері обігу комп'ютерної інформації щодо правомірного здійснення певними особами чи особою інформаційної діяльності стосовно комп'ютерної інформації, що становить одну з груп таємниць (приватного життя, комерційна, банківська та державна таємниці), яким спричинена шкода конкретним злочинним посяганням.

5. Не підлягаючу грошовій оцінці шкоду у ст.ст. 231, 232 КК України, пропонується вважати «істотною». Відповідальність за завдання такої шкоди в результаті незаконного розголошення або використання відомостей, що становлять комерційну, податкову або банківську таємницю, варто віднести банкрутство й ліквідацію організації або індивідуального підприємця, скорочення великої

кількості робочих місць, значні збої в роботі податкових і митних органів, заподіяння шкоди здоров'ю людей (у цьому випадку зазначені дії будуть кваліфікуватися за сукупністю зі статтями КК, що передбачають відповідальність за заподіяння такої шкоди) і т.д. Зважаючи на те, що злочини, передбачені ст.ст. 231, 232 КК України, є матеріальними, при їхній кваліфікації є необхідним встановлення причинного зв'язку між вчиненими діями та наслідками. У кримінальному законі розмір завданої «істотної» шкоди не є конкретизованим, має оціночний характер. У підручниках з кримінального права України, коментарях до КК України це поняття або не розкривається або зазначається, що «міра» завданої шкоди визначається судом залежно від обставин справи. Визначення істотної шкоди вимагає або законодавчого розроблення, або відповідних роз'яснень на рівні Пленуму Верховного Суду України для виключення можливих судових помилок і правильного застосування положення ст. 232 КК України. Шкода як результат незаконного розголошення або використання відомостей, що становлять комерційну або банківську таємницю, як правило, зумовлює економічні втрати комерційної організації або банку, підрив авторитету або ділової репутації, зрив вигідних угод і т.ін.

6. Основним безпосереднім об'єктом злочинних посягань на комп'ютерну інформацію з обмеженим доступом необхідно визнавати суспільні відносини у сфері обігу комп'ютерної інформації щодо правомірного здійснення певними особами чи особою інформаційної діяльності стосовно комп'ютерної інформації, яка становить одну з груп таємниць (приватного життя, комерційна, банківська та державна таємниці), яким спричинена шкода конкретним злочинним посяганням.

Додатковим безпосереднім об'єктом злочинів у сфері обігу комп'ютерної інформації з обмеженим доступом є відносини власності щодо цієї комп'ютерної інформації.

Факультативним безпосереднім об'єктом аналізованих посягань можуть бути суспільні відносини, у сфері яких здійснюється інформаційна діяльність із захисту комп'ютерної інформації з обмеженим доступом (наприклад, при незаконному розголошенні відомостей, які становлять комерційну таємницю, факультативним безпосереднім об'єктом виступають відносини у сфері захисту честі та ділової репутації особи).

7. При аналізі норм, які передбачають кримінальну відповідальність за посягання на один із трьох блоків таємниць, закономірно випливає, що предметом цих злочинів є комп'ютерна інформація, яка становить один із цих блоків (приватного життя, комерційна, банківська та державна таємниці). Тобто предметом проаналізованих складів злочинів є відомості, що віднесені відповідними особами та державними органами до тієї чи іншої таємниці, які, у свою чергу, мають оцифрований вигляд і знаходяться у пам'яті комп'ютера чи на зовнішніх запам'ятовуючих пристроях (наприклад, лазерні диски, дискети, USB флеш накопичувачі). Таким чином, разом із речами матеріального світу варто визнавати предметом злочину й інші матеріальні утворення, зокрема, комп'ютерну інформацію. Тобто предмет є обов'язковою ознакою всіх складів проаналізованих злочинів, яка поряд із деякими іншими дає можливість відмежовувати ці посягання від суміжних.

8. До класифікаційних критеріїв комп'ютерної інформації необхідно віднести: 1) ступінь таємності; 2) суб'єкт інформаційних відносин, якому фактично належить та-

ка інформація; окрім цього визнати родовий об'єкт злочину як такий, що дає змогу класифікувати склади злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом, і за допомогою якого виділені три групи таємниць: 1) приватного життя; 2) комерційна, банківська; 3) державна.

9. До предмета ст.ст. 231, 232 КК України слід віднести відомості, що становлять комерційну або банківську таємницю на матеріальних носіях інформації, а також представлені в іншій формі. Це комп'ютерна інформація, що утримується як на постійних, так і оперативних запам'ятовуючих пристроях, виведена на екран монітора, що передається по технічних каналах зв'язку, тобто існує в електронному вигляді. До зазначеного ряду предметів також можна віднести винаходи, корисні моделі, промислові зразки, що мають певну матеріалізовану форму, які незапатентовані їх законними власниками й охороняються в режимі комерційної таємниці.

10. Аналіз диспозиції ст. 232^1 КК України дає можливість поставити питання про доцільність конкретизації способів можливого умисного розголошення, іншого використання інформації про емітента, про його цінні папери або правочини щодо них. Ці способи можна викласти прямо у диспозиції. Законодавцю необхідно зважити таку конструкцію диспозиції та передбачити можливі негативні наслідки, які можуть мати вираження у колізії норм Особливої частини КК України, та як наслідок – існування різноманіття точок зору щодо тлумачення окремих положень ст. 232^1 КК України.

11. Об'єктивна сторона складів злочинів, що посягають на таємницю (приватного життя, комерційну, банківську, державну), у більшості випадків характеризується активними діями, хоча є склади злочинів, які характеризуються як дією, так і бездіяльністю (ст.ст. 159, 329, 422). Найбільш розповсюдженими способами є збір, розповсюдження та використання. Розголошення зазначених відомостей здійснюється усно, письмово, за допомогою каналів зв'язку, у засобах масової інформації по комп'ютерних та телекомунікаційних мережах.

12. Суб'єктивна сторона незаконного розголошення комп'ютерної інформації, що становлять комерційну або банківську таємницю, характеризується прямим умислом та спеціальними цілями – розголошення або використання цих відомостей, і мотивом – корисливою або іншою особистою зацікавленістю.

13. Найбільш розповсюдженими мотивами незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом є користь або інша особиста зацікавленість, прагнення до одержання особистої матеріальної вигоди шляхом незаконного розголошення або використання чужих секретів, помста, заздрість, образа, родинні й товариські спонукання, бажання догодити близькій людині та ін.

14. З метою виключення неоднозначного тлумачення закону та практики його застосування, диспозицію ст. 232 КК України доцільно викласти у такій редакції: «Незаконне розголошення або використання відомостей, що становлять комерційну або банківську таємницю, без згоди їхнього власника або іншого законного користувача, особою, якій ці відомості були довірені або стали відомі у зв'язку зі здійсненням професійних або службових обов'язків, учинене з корисливої або іншої особистої зацікавленості, яке завдало істотної шкоди суб'єктові господарської діяльності».

Позитивна сторона таких змін вбачається не лише в остаточному вирішенні питання визначення ознак суб'єкта даного складу злочину, але й у правильності та повноті кваліфікації дій, пов'язаних з посяганням на конфіденційну економічну інформацію. У випадку прямої вказівки у передбаченій ст. 232 КК України нормі на спеціальні ознаки суб'єкта злочину, особи, що збирали відомості, які становлять комерційну або банківську таємницю і не мали до них доступу на законних підставах, навіть при їхньому подальшому використанні, можуть бути притягнуті до кримінальної відповідальності тільки за ст. 231 (якщо в їх діях не міститься іншого складу злочину). У протилежному випадку, дії, які передбачені частинами однієї статті, та які утворюють різні склади злочинів, вимагають самостійної кваліфікації з усіма відповідними правовими наслідками.

15. Особливістю суб'єкта у досліджених складах є те, що ним може бути особа, яка не має доступу до відомостей, що становлять таємницю (незаконне одержання). Однак суб'єктом розголошення таємниці приватного життя, комерційної, банківської, державної, а також втрати документів, які містять державну таємницю, може бути лише особа, якій таємниця довірена по службі, роботі, у розпорядженні якої перебували документи, предмети, що містять відомості, віднесені до таємниці.

16. Аналіз найбільш розповсюджених способів підготовки та скоєння злочину, передбаченого ст.ст. 361, 361^2 КК України, свідчить, що чіткої межі між ними немає. Деякі із зазначених способів відіграють роль допоміжних, які, у свою чергу, працюють на основний, що обрав злочинець, виходячи з конкретної злочинної мети та обставин суспільно-небезпечного діяння. Вищенаведені способи неправомірного доступу до комп'ютерної інформації повинні бути враховані працівниками правоохоронних органів при кваліфікації та розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

17. Незаконне втручання в роботу автоматизованих ЕОМ, їх систем чи комп'ютерних мереж, що характеризується підвищеною суспільною небезпекою, зумовлюється виникненням широких можливостей для заподіяння суттєвої шкоди. Необхідно також пам'ятати про існування різноманітних засобів втручання у роботу автоматизованих ЕОМ (комп'ютерів). Ними можуть бути як програмні, так і технічні засоби, призначені для незаконного проникнення в автоматизовані ЕОМ, їх системи чи комп'ютерні мережі і здатні спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

18. Практика застосування норм розділу XVI Особливої частини Кримінального Кодексу України практичними працівниками підрозділів Департаменту державної служби боротьби з економічною злочинністю МВС України свідчить, що існують значні недоліки, як у їхніх знаннях чинного кримінального законодавства, так і в недостатньому розробленні кримінального законодавства в частині злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), надмірна бланкетність складів, у разі чого їх практичне застосування є дуже складним.

Вищенаведені висновки не претендують на обов'язковість їх прийняття, однак вони можуть бути враховані законодавцем як при вдосконаленні чинних норм, так і при введенні нових складів злочинів, що мають на меті захист суспільних відносин у сфері обігу та використання комп'ютерної інформації з обмеженим доступом.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Рудик М.В. Понятійний апарат предмета злочину, передбаченого статтею 363 КК України // Вісник Національного університету внутрішніх справ. – 2005. – № 29. – С. 131-135.

2. Рудик М.В. Професійна таємниця як об'єкт кримінально-правової охорони // Вісник Національного університету внутрішніх справ. – 2005. – № 31. – С. 124-128.

3. Рудик М.В. Суспільна небезпека від незаконного збуту й поширення комп'ютерної інформації з обмеженим доступом // Вісник Запорізького юридичного інституту. – 2005. – № 3. – С. 120-124.

4. Рудик М.В. До питання про захист комп'ютерної інформації з обмеженим доступом в ОВС // Актуальні проблеми сучасної науки в дослідженнях молодих учених. – 2005. – № 8. – С. 49-55.

5. Рудик М.В. (у співавторстві з Д.П. Альошиним) Міжнародний досвід протидії незаконному збуту та розповсюдженню конфіденційної інформації // Актуальні проблеми держави та права. – Одеса: Юрид. л-ра. – 2006. – № 27. – С. 222-228.

6. Рудик М.В. Шляхи вирішення проблеми кваліфікації злочинних посягань на комп'ютерну інформацію з обмеженим доступом // Актуальні проблеми сучасної науки в дослідженнях молодих учених: Зб. наук. пр. – Харків: Вид-во Харк. нац. ун-ту внутр. справ. – 2006. – С. 34-37.

7. Рудик М.В. Об'єкт та предмет незаконного збуту та розповсюдження комерційної та банківської таємниці // Право і безпека. – 2006/5□2 – С. 70-72.

АНОТАЦІЯ

Рудик М.В. **Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом. –** Рукопис.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. – Одеська національна юридична академія Міністерства освіти і науки України, Одеса, 2007.

В дисертації досліджується суспільно-небезпечні дії, пов'язані з незаконним збутом, розповсюдженням комп'ютерної інформації з обмеженим доступом, розробляється термінологічний апарат окремих видів таємниць, аналізуються відповідні склади злочинів, що посягають на інформацію з обмеженим доступом, скоєних за допомогою засобів комп'ютерної техніки. Сформульовано єдиний підхід до питань застосування норм кримінального права щодо захисту комп'ютерної інформації з обмеженим доступом, визначено найбільш актуальні питання кваліфікації злочинних посягань на інформацію з обмеженим доступом, розроблено рекомендації з удосконалення чинного кримінального законодавства та правозастосовчої практики. Вивчено та проаналізовано законодавче регулювання різних видів таємниць, що закріплені в національному та іноземному законодавст-

вах. Здійснено системний та порівняльний аналіз складів злочинів, які передбачають відповідальність за посягання на таємницю: приватного життя, комерційну, банківську, державну. Розроблено пропозиції щодо удосконалення чинного законодавства у сфері кримінально-правової охорони комп'ютерної інформації з обмеженим доступом. Практичне значення дослідження полягає в розробці конкретних пропозицій щодо змін і доповнень чинного кримінального законодавства, яке охороняє суспільні відносини у сфері використання комп'ютерної інформації з обмеженим доступом. Його результати можуть бути використані при вдосконаленні норм Кримінального кодексу України та у практичній діяльності підрозділів ОВС України.

Ключові слова: незаконний збут, розповсюдження, комп'ютерна інформація, таємниця, матеріальний носій інформації, кваліфікація злочинних посягань, обмежений доступ, електронно-обчислювальна машина.

АНОТАЦИЯ

Рудик М.В. **Незаконный сбыт, распространение компьютерной информации с ограниченным доступом. –** Рукопись.

Диссертация на соискание ученой степени кандидата юридических наук по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. – Одесская национальная юридическая академия Министерства образования и науки Украины, Одесса, 2007.

В диссертации исследуются общественно-опасные действия, связанные с незаконным сбытом, распространением компьютерной информации с ограниченным доступом. Разрабатывается терминологический апарат отдельных видов тайн, анализируются соответствующие составы преступлений, которые посягают на информацию с ограниченным доступом, совершенных с помощью средств компьютерной техники. Сформулирован единый подход к вопросам применения норм уголовного права относительно защиты компьютерной информации с ограниченным доступом, выявлены наиболее актуальные вопросы квалификации преступных посягательств на информацию с ограниченным доступом, разработаны рекомендации относительно усовершенствования действующего уголовного законодательства и правоприменительной практики. Изучено и проанализировано законодательное регулирование различных видов тайн, которые закреплены в национальном и иностранном законодательствах. Осуществлен системный и сравнительный анализ составов преступлений, предусматривающих ответственность за посягательство на тайну: частной жизни, коммерческую, банковскую, государственную. Разработаны предложения относительно усовершенствования действующего законодательства в сфере уголовно-правовой охраны компьютерной информации с ограниченным доступом. Практическое значение исследования заключается в разработке конкретных предложений относительно изменений и дополнений к действующему уголовному законодательству, которое охраняет общественные отношения в сфере использования компьютерной информации с ограниченным доступом. Его результаты могут быть использованы при совершенствовании норм Уголовного кодекса Украины и в практической деятельности органов и подразделений ОВД Украины.

Ключевые слова: незаконный сбыт, распространение, компьютерная информация, тайна, материальный носитель информации, квалификация преступных посягательств, ограниченный доступ, электронно-вычислительная машина.

SUMMARY

Rudik M.V. **Illegal sale, distribution of computer information of the limited access.** – Manuscript.

The dissertation for candidate's degree in jurisprudence in speciality 12.00.08 – Criminal law and Criminology; Criminal-executive law. – Odessa national law academy of Ministry education and science, Odessa, 2007.

Dissertation deals with the research of the public-dangerous effects, related to the illegal sale, distribution of computer information with the limited access. To development of terminology apparatus separate types of secrets, analysis of the proper compositions of crimes which trench upon information with the limited access, accomplished by facilities of computer technique. Single approach to the questions of application of norms of criminal law in relation to defense of computer information with the limited access is formulated, the most actual questions of qualification of criminal assaults on information with the limited access are exposed, recommendations in relation to the improvement of active criminal law and law practice are developed. The legislative adjusting of different types of secrets which are fastened in the legislation national and foreign is studied and analyzed. The system is carried out, and also comparative analysis of compositions of crimes which foresee responsibility for encroachment on a secret: private life, commercial, bank, state, the grounded suggestions in relation to the improvement of active law in the field of criminal law defense of computer information with the limited access are developed. The practical meaning of research consists in development of concrete suggestions in relation to the amendments and supplements of active criminal law which protect the public relations in the field of the use of computer information of the limited access. At perfection of norms of the Criminal code of Ukraine, and practical activity units of internal affairs of Ukraine.

Key words*:* illegal sale, distribution, computer information, secret, material data carrier, qualification of criminal trespasses, limited access, computer.