у Верховній Раді України, зокрема у Комітеті Верховної Ради України з питань свободи слова та інформації, Першим заступником Голови цього Комітету, народним депутатом Гавриловим І. О.;

6 жовтня 2000 року рішенням Урядової комісії з питань інформаційно-аналітичного забезпечення органів виконавчої влади проект Концепції реформування законодавства України у сфері суспільних інформаційних відносин прийнято за основу. На виконання рішення Комісії матеріали щодо Концепції розміщуються в мережі Інтернет за адресами http://mndc.naiau.kiev.ua для обговорення науковою громадськістю та фахівцями в різних галузях суспільних відносин щодо інформації;

Концепція пройшла обговорення на спільному засіданні Консультативної ради з питань інформатизації при Верховній Раді України та науково-технічної ради Національної програми інформатизації Держкомзв'язку та інформатизації України;

Ідея кодифікації інформаційного законодавства на рівні окремого кодексу підтримана і в Академії правових наук України [10]. Проект Концепції пройшов обговорення в окремих провідних юридичних наукових та вищих навчальних закладах України: Національній юридичній академії ім. Ярослава Мудрого; Харківському Національному університеті внутрішніх справ; Національній академії внутрішніх справ, Національному Університеті "Києво-Могилянська академія" та інших.

Готові з задоволенням прийняти конструктивні зауваження, критику, пропозиції до співпраці. Окремі питання щодо наших поглядів на формування інформаційного законодавства в умовах формування інформаційного суспільства знайшли відображення у публікаціях, окремі з них подаються нижче.

На завершення хочемо подякувати керівництву НТУУ "КПІ" та НДЦ "ТЕЗІС", за підтримки яких ідея Концепції реформування законодавства України у сфері суспільних інформаційних відносин вперше була апробована на конференції "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" у 2000 році.

Література 1. Гавловський В. Д., Цимбалюк В. С., Інформаційне право. Навчально-методичний комплекс. -К. 1999. 183 с. 2. Гавловський В. Д., Цимбалюк В. С. Щодо проблем боротьби зі злочинами, що вчиняються з використанням комп'ютерних технологій // Боротьба з контрабандою: проблеми та шляхи їх вирішення. - К. НДІ "Проблем людини". 1998. С. 148-154. 3. Гавловський В. Д., Цимбалюк В. С., Корочанський О. Е. Проблеми юридичної деліктології в інформаційних відносинах // "Бизнес и безопасность". 1998 № 6. С. 19-21 4. Гавловський В., Цимбалюк В., Кашпур В. Державно-правове регулювання соціальних інформаційних відносин // Українське право. 1998 № 1. С. 173-176. (укр. і англ. мовами). 5. Гуцалюк М. Проблеми організаційно-правового забезпечення захисту інформаційних систем в Internet // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - К.: НТУУ "КПІ". – К. 2000. – С. 24-27. 6. Калюжний Р. А., Цимбалюк В. С. Інформатизація державного управління і національна безпека України. // Розбудова держави. 1993. № 8 С. 20-21. 7. Калюжний Р. А., Цимбалюк В. С. Розбудова держави та інформатизація державного управління. // Розбудова держави. 1994. № 2 С. 31-36. 8. Романюк Б. В. Камлик М. І., Гавловський В. Д., Хахановський В. Г. Цимбалюк В. С. Виявлення та розслідування злочинів, що вчиняються за допомогою комп`ютерних технологій. Посібник / За ред. Я. Ю. Кондратьєва. -К. НАВСУ. 2000. –64 с. 9. Копылов В. А. О структуре и составе информационного законодательства // Государство и право. 1996. № 6. С. 101-110. 10. Лисицький В., Тацій В. До питання реформування законодавства України у сфері суспільних інформаційних відносин // Вісник Академії правових наук України. 2000. № 4. – С. 298-302).

УДК 681.3:34

ІНФОРМАЦІЯ ЯК ПРЕДМЕТ ЗЛОЧИНУ

Дарія Прокоф'єва
НДЦ «ТЕЗІС» НТУУ «КПІ»

Анотація: **Чинне кримінальне законодавство України закріплює велику кількість складів злочинів, що посягають на інформаційну безпеку суспільства та його окремих елементів. Значна частина таких злочинів має предметом посягань інформацію як повноправний об'єкт правовідносин. Система злочинів, предметом яких є інформація, безпосередньо залежить від структури інформаційних ресурсів.**

Summary: **Ukraine criminal low in force fastens off a great many of presence crime in the act encroaching on information society safety and its separate elements. Considerable part of such crimes is information crimes, which are at the same time competent object of legal relations. Subject of the crime system is information and directly depends on the structure of the information resources.**

Ключові слова: **Інформація, злочин, безпека, таємниця, доступ, конфіденційність, матеріальний носій,**

документ, інтелектуальна власність, докази, програма, автоматизована система.

Якщо розглядати вітчизняний кримінальний закон, можна констатувати закріплення в Кримінальному Кодексі України 1960 року, так само, як в новому Кримінальному Кодексі України, який ще не набув чинності, великої кількості складів злочинів, які тією чи іншою мірою зачіпають інформаційну сферу життєдіяльності суспільства, завдаючи шкоди інформаційній безпеці як суспільства в цілому, так і його окремим елементам. Має місце підвищення суспільної небезпеки злочинів, які посягають на інформацію, інформаційні права, або вчинюються за допомогою інформації та інформаційних технологій, що безперечно вимагає відокремлення системи власне інформаційних, в тому числі й комп′ютерних, злочинів на рівні окремої глави Кримінального Кодексу. Ця тенденція певною мірою була реалізована в новому Кримінальному Кодексі України. Водночас, оскільки поки що залишається чинним Кримінальний Кодекс 1960 року, він виступатиме базою при розгляді злочинів, предметом яких є інформація, в контексті даної роботи.

В наш час інформація визнається повноправним об′єктом правовідносин (було виділено навіть особливий тип суспільних відносин – та правовідносин, - а саме інформаційний) не лише на доктринальному рівні, але й в нормах інформаційного законодавства, що має розгалужену структуру. Особливо слід підкреслити, що інформацію було визнано не лише об′єктом права інтелектуальної власності, але й права так званої майнової власності (речового права). Все це, а також важливість та потенціал інформаційних ресурсів й інформаційних технологій в інформаційному суспільстві, дає підстави закономірно розглядати інформацію як предмет злочину. Інформація є системним явищем і складається принаймні з двох підсистем, про що можна зробити висновок, спираючись на окремі міжнародні нормативно-правові акти та національне законодавство багатьох країн. Зазначимо, що поділ інформації за режимом доступу притаманний не лише пострадянському праву, а й іншим правовим системам, які належать як до континентальної, так і до англо-американської сім′ї права. До відкритої інформації зазвичай належить інформація, яка розповсюджується засобами масової інформації, надходить до загальнодоступних баз даних, та інформація, що захищається за допомогою законодавства про інтелектуальну власність. Що стосується інформації з обмеженим доступом, то на законодавчому рівні її поділ та ранжування відбувається за ступенем секретності та рівнем важливості (зокрема, для держави) із різним ступенем деталізації. Незважаючи на наявність такого загального критерію для розподілу інформації з обмеженим доступом на групи (категорії та види), зазначений розподіл в законодавстві різних країн є неоднорідним (досить часто спостерігається збіг за змістом різнопорядкових груп інформації з обмеженим доступом в різних країнах при порівняльному зіставленні системи інформації з обмеженим доступом). Так в Україні інформація з обмеженим доступом поділяється на дві категорії: конфіденційну та таємну. В свою чергу, остання поділяється на державну таємницю та іншу таємну інформацію. Так звана «інша таємна інформація» являє собою групу видів таємної інформації, що не становить державної таємниці: службова, медична, адвокатська тощо. До конфіденційної належить: комерційна таємниця; інформація про особу, яка у відповідності із законом не належить до категорії таємної; інша інформація за рішенням її власника, якщо вона не є таємною або такою, доступ до якої не може бути обмежено. В РФ система інформації з обмеженим доступом дещо інша. Інформація з обмеженим доступом не поділяється на категорії, а складається лише з видів: державної таємниці та конфіденційної інформації (як групи видів, до якої належать: комерційна таємниця, службова таємниця, медична таємниця та інша інформація за рішенням її власника, якщо вона не є державною таємницею або такою, доступ до якої не може бути обмежено) [1-15, 23].

Екстраполюючи структуру інформації з обмеженим доступом у сферу скоєння злочинів та кримінально-правового закріплення відповідних складів злочинів, можна виділити злочини, предметом яких є:

1. державна таємниця;
2. інша таємна інформація;
3. конфіденційна інформація.

Таким чином, державна таємниця становить предмет наступних злочинів: державна зрада (ст. 56 КК України); шпигунство (ст. 57 КК України); розголошення державної таємниці (ст. 67 КК України); втрата документів, що містять державну таємницю (ст. 68 КК України); розголошення відомостей військового характера, що становлять державну таємницю, за відсутності ознак зради батьківщині (ч. а, в ст. 253 КК України); втрата документів, що містять відомості військового характера, які становлять державну таємницю (ч. б, в ст. 253 КК України). При цьому предметом злочинів, передбачених ст. 68 КК України та відповідними положеннями ст. 253 КК України, є матеріальні носії інформації, яка становить державну таємницю, чітко встановленого в нормах Кримінального кодексу виду, а саме – документ. Поняття “документ” є спірним, особливо в контексті ст. 68 КК України. Незважаючи на назву цієї статті “втрата документів, що містять державну таємницю”, в її тексті мова йде також і про предмети, відомості про які становлять державну таємницю. Зазначені предмети являють собою опосередковані носії інформації, що становить державну таємницю, яка

може бути достатньою мірою (для завдання шкоди інтересам України, в тому числі в сфері інформаційної безпеки) встановлена через вивчення сукупності їх інформативних ознак. Очевидно, що в ст. 68 КК України йдеться про декілька видів матеріальних носіїв інформації: документи як безпосередні носії інформації (вони не мають іншого функціонального призначення) та інші предмети матеріального світу, відомості про які становлять державну таємницю (вони мають інше функціональне призначення, ніж виключно фіксація інформації). Ст. 68 КК України, таким чином, відмежовує документи від інших матеріальних носіїв інформації (вважаємо, що це найбільш доцільно здійснювати за вказаним вище характером фіксації інформації та функціональним призначенням її матеріальних носіїв), що є безперечно більш коректним, ніж формулювання ст. 27 Закону України "Про інформацію". Разом з тим, ст. 68 КК України потребує більш чіткого змісту стосовно предмета відповідного злочину, що може бути досягнуто шляхом заміни таких понять, як "документи" та "предмети, інформація про які містить державну таємницю" на "матеріальні носії інформації, що становить державну таємницю", тобто шляхом визнання предметом злочину, передбаченого ст. 68 КК України, широкого спектру матеріальних носіїв інформації, що становить державну таємницю. Це, зокрема, позначить врахування потенціалу подальшого науково-технічного прогресу, що сприятиме видозміні та модернізації матеріальних носіїв інформації, а також появі їх нових видів. Разом з тим, необхідно відмітити, що такого роду уточнення норм КК України вимагає відповідної бази в інформаційному законодавстві, а саме: уточнення понять "документ" та "матеріальний носій інформації" (це поняття, зокрема, не є визначеним) в інформаційному законодавстві України, і в першу чергу – в Законі України "Про інформацію". Все викладене вище поширюється й відповідно на предмет злочину, передбаченого п. б, в ст. 253 КК України. Стосовно інших віднесених до цієї групи складів злочинів (ст.ст. 56, 57, 67 та ч. а, в ст. 253 КК України) предметом злочину можуть виступати будь-які матеріальні носії інформації, що становить державну таємницю, а також відповідна інформація, що не міститься на певному матеріальному носії. В останньому випадку мова йде про опосередкування передачі інформації до третіх осіб або розголошення інформації її закріпленням у свідомості суб′єкта злочину. Необхідно також відзначити, що якщо мова у відповідній статті КК не йде безпосередньо про "документи, що містять державну таємницю", які відповідно до закону повинні мати гриф секретності як обов′язковий реквізит (а рівно й предмети, інформація про які становить державну таємницю, для яких гриф секретності повинен міститися в супровідних документах), зазначений реквізит не повинен бути визначальною ознакою при окресленні предмету злочину, та, відповідно, кваліфікації діяння. Причина цього полягає в наступному: інформація, що становить державну таємницю, зафіксована на матеріальному носієві, який відповідає вимогам чинного законодавства, може не лише відбитися у свідомості ("ідеальний" носій інформації, оскільки він не є об′єктом матеріального світу, що існує об′єктивно та дозволяє здійснити доступ до інформації та її інтерпретацію без участі суб′єкта, який зазначену інформацію сприйняв або сприймає) особи, що здійснює санкціонований або несанкціонований доступ до інформації, але й бути несанкціоновано скопійована такою особою безпосередньо на матеріальний носій (який не відповідатиме встановленим законом вимогам), або ж відтворена на матеріальний носій суб′єктом, що сприйняв її (інформацію) раніше. Тому подібні матеріальні носії інформації, спеціально підготовлені для фіксації інформації, що містить державну таємницю, з наступним використанням їх зі злочинною метою, можуть (та скоріш за все, з метою приховування злочинів – будуть) не мати грифів секретності, що, однак, не свідчить про те, що інформація, яка на них міститься, не становить державної таємниці (оскільки відповідний гриф та інші необхідні реквізити присутні в первинному документі, який містить зазначену інформацію). Разом з тим, створення такого плану вторинних носіїв інформації (найчастіше – у формі документа) є характерним лише для умисних злочинів (тобто, таких, що передбачені ст.ст. 56, 57 КК України, а також ст. 67 КК України – при умисній формі вини). Зазначимо, що мова йде не про створення (тобто, виготовлення) об′єкта матеріального світу, який потенційно може виступати як носій інформації, а саме про створення власне матеріального носія державної таємниці, оскільки повною мірою носієм інформації, а особливо – інформації певного характеру, той чи інший об′єкт (предмет матеріального світу) може вважатися лише в тому випадку, коли на ньому дійсно зафіксована інформація, в даному випадку така, що становить державну таємницю. Слід ще раз підкреслити, що п. а) та п. б) (а також – п. в) – стосовно тяжких наслідків) ст. 253 КК України практично повністю дублюють склад злочинів, передбачених відповідно ст. 67 та 68 КК України, та являють собою деталізацію зазначених злочинів за предметом та суб′єктом. Зазначимо, що існування цих пунктів не є повною мірою виправданим, оскільки законодавство України про державну таємницю, по-перше, не встановлює, що відомості військового характеру, які становлять військову таємницю, можуть передаватися лише військовослужбовцям, а, по-друге, такі відомості повністю перебувають під режимом державної таємниці й не мають, окрім предметної, жодної специфіки. Крім того, відокремлення зазначених відомостей від кола державної таємниці в нормах КК протирічить положенням Закону України "Про державну таємницю", згідно з якими структура державної таємниці є єдиною, та включає відомості різноманітного характеру, не включаючи інших окремих "таємниць". Крім того, якщо за-

стосування терміну "військова таємниця" до інформації, що становить державну таємницю, є недоцільним у зв′язку з протиріччям з законодавством про державну таємницю, це не означає, що зазначений термін взагалі позбавлений сфери застосування. Навпаки, як справедливо відзначається в п. г) ст. 253 КК України, існують відомості військового характеру, що не підлягають оголошенню, однак не становлять державної таємниці. Як бачимо власне з формулювання відповідної норми становище таких відомостей в структурі інформації з обмеженим доступом не визначене, оскільки на законодавчому рівні слід виділити відповідний вид таємної інформації, закріпивши за ним назву "військова таємниця". Це, звісно, потребує певного реформування змісту статті КК України. Зазначимо, що чинний КК РФ взагалі відмовився від використання терміну "військова таємниця", що, на наш погляд, доцільно в статтях, що закріплюють склади злочинів, предметом яких виступає державна таємниця, однак необгрунтовано позбавляє кримінально-правового захисту відомості військового характеру, що не становлять військової таємниці, але не підлягають розголошенню [1, 2, 11, 12, 22].

Таємна інформація – це, відповідно до Закону України "Про інформацію", категорія інформації з обмеженим доступом (поряд з конфіденційною інформацією), розголошення якої завдає шкоди особі, суспільству і державі. Визнання інформації певного виду такою, що належить до категорії таємної, здійснюється державою в публічних інтересах та закріплюється в нормах закону (на відміну від порядку визнання інформації конфіденційною). Таємна інформація може бути об′єктом права власності та інтелектуальної власності, однак норми законодавства щодо інф>Ёрмації з обмеженим доступом мають перевагу у застосуванні порівняно з нормами законодавства про власність та інтелектуальну власность. Норми щодо віднесення інформації до категорії таємно**ї** є імперативними, і їх виконання не залежить від волі власників таємної інформації або інших осіб (на відміну від диспозиційного характеру норм віднесення інформації до категорії конфіденційної, відповідно до яких особа може, але не зобов(язана становлювати режим обмеженого доступу до інформації, яка їй належить). Конкретні відомості визнаються такими, що належать до категорії таємної інформації з моменту свого виникнення, або з моменту надходження у володіння визначених законом суб′єктів (якщо такі відомості за своїм змістом належать до передбаченого законом виду таємної інформації), конфіденційними ж - з моменту винесення відповідного рішення власника інформації, оскільки неможливою є конфіденційність a priori, тобто, вимога держави на рівні закону щодо обов′язковості визнання певної інформації конфіденційною. В разі, коли склад відомостей, що становлять певний вид таємної інформації, безпосередньо визначений в нормах закону, додаткових процедур з віднесення зазначених відомостей до категорії таємної інформації не потрібно. Якщо ж склад відомостей в межах певного передбаченого законом виду таємної інформації може підлягати змінам, або його наведення безпосередньо в законі є недоречним з міркувань інформаційної безпеки, питання про склад конкретних відомостей в межах виду таємної інформації вирішується державним органом чи посадовою особою, на яких такий обов′язок покладений законом, шляхом формування переліків відомостей, які становлять відповідний вид таємної інформації. Інформація, що визнана конфіденційною за рішенням її власника або уповноваженої ним особи, може також бути віднесена до категорії таємної у випадках, передбачених законом. Обмеження доступу до інформації, яка належить до категорії таємної, може носити строковий або, якщо інше не встановлене законом, безстроковий характер. До структури таємної інформації, виходячи з чинного інформаційного законодавства України, входить не лише державна таємниця, але й інша таємна інформація. Якщо державна таємниця являє собою специфічний вид таємної інформації, то про таємну інформацію, що не становить державної таємниці ("інша таємна інформація"), можна вести мову як про сукупність окремих видів таємної інформації (що не становлять державної таємниці). «Інша таємна інформація» на сьогоднішній день не має чітко закріпленої в законодавстві структури (хоча потребує вичерпної визначеності, осільки її існування фактично є обмеженням права на інформацію), але може бути визначена, виходячи зі змісту правових норм, присвячених окремим видам такої інформації, які містяться в законах, що контекстно не належать до інформаційного законодавства. За результатами їх аналізу може бути зроблений висновок, що «інша таємна інформація» становить систему видів таємної інформації, яка не становить державної таємниці. Таємна інформація, що не становить державної таємниці, одержала кримінально-правовий захист не в повному обсязі. Така таємна інформація виступає предметом наступних складів злочинів: шпигунство в формі збирання відомостей, що не становлять державної таємниці за завданням іноземної розвідки (ч. 2 ст. 57); передача іноземній організації відомостей, що становлять службову таємницю (ст. 68′); розголошення відомостей про проведення медичного огляду на зараження вірусом імунодефіциту людини та його результатів (ст. 108-4); розголошення таємниці усиновлення (ст. 115′); порушення таємниці кореспонденції (ст. 131); розголошення даних попереднього слідства або дізнання (ст. 181); розголошення військових відомостей, що не підлягають оголошенню, однак не становлять державної таємниці (п.п. г-д ст. 253). Таким чином, в розумінні чинного КК України, предметом злочину може виступати: службова таємниця; військова таємниця (в тому значенні, в якому цей термін використовується в наведеній вище класифікації); таємниця

повідомлень, що передаються засобами зв′язку; таємниця усиновлення; таємниця попереднього розслідування; лікарська таємниця (частково). Слід зазначити, що формулювання диспозицій відповідних статей КК України не виділяє матеріальних носіїв інформації, яка становить ту чи іншу таємницю (з вищенаведених), як самостійного предмету злочинів. Це, однак, не означає, що вся кримінально-захищувана таємна інформація є мовною – вона може бути як зафіксованою в свідомості людини, так і зафіксованою на певних матеріальних носіях. В останньому випадку діяння, що становить об′єктивну сторону конкретного злочину, маючи предметом інформацію, опосередковується доступом – законним або протиправним – до її матеріальних носіїв. Загальною властивістю матеріальних носіїв інформації, що не становить державної таємниці, є відсутність єдиного встановленого законодавством переліку необхідних реквізитів, зокрема, грифів секретності, й порядку їх надання зазначеним матеріальним носіям. Виходячи з наведеного вище змісту норм Закона України "Про державну таємницю" можна впевнено констатувати лише те, що матеріальні носії інформації, що не становить державної таємниці, зокрема, таємної (а рівно й конфіденційної) не можуть одержувати грифів секретності, передбачених для матеріальних носіїв державної таємниці ("особливої важливості", "таємно", "цілком таємно"). В цілому ж, як вже зазначалося вище, питання таємної інформації, що не становить державної таємниці, в достатній мірі не врегульовані інформаційним законодавством України. В першу чергу відсутньою є чітка система зазначеної інформації – її побудови, яка має забезпечити однакове розуміння змісту цієї підкатегорії інформації з обмеженим доступом. Відповідно єдиному розумінню та застосуванню норм закону (в тому числі, кримінального) не сприяють уривчасті намагання сформулювати правила обігу такої інформації в нормах законів неінформаційного характеру, які призводять, в свою чергу, до суперечностей з Конституцією України, базовими актами інформаційного законодавства, а також безпосередньо до суперечностей у визначеннях та правилах обігу для окремих видів таємної інформації, що не становить державної таємниці, не зумовлені їхніми змістовними особливостями. Це, однак, не позбавляє можливості побудувати систему таємної інформації, що не становить державної таємниці, на доктринальному рівні й визначитись зі станом її кримінально-правового захисту. Останньою групою злочинів, предметом яких виступає інформація з обмеженим доступом, є злочини, що посягають на конфіденційну інформацію. Чинний КК України передбачає два склади, що можуть бути віднесені до цієї групи злочинів. Це ст. 148^6 "Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю" та ст. 148^7 "Розголошення комерційної таємниці". Предметом злочинів, склади яких передбачені зазначеними статтями, є окремий вид конфіденційної інформації, а саме – комерційна таємниця. Конфіденційна інформація - відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов. Громадяни, юридичні особи, які володіють інформацією ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їхнього професійного, ділового, банківського, комерційного та іншого інтересу, та не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність до категорії конфіденційної, та встановлюють для неї систему (спосіб) захисту. Виняток становить інформація комерційного та банківского характеру, а також інформація, правовий режим якої встановлено ВР України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої є загрозою життю і здоров′ю людей. Таким чином, власник інформації як в підприємницькій, так і в інших сферах є незалежним в питанні визначення режиму доступу до інформації, крім випадків, передбачених законом, перелік яких має бути вичерпним. До конфіденційної інформації, таким чином, може бути віднесений досить широкий спектр питань в різних сферах життєдіяльності суб'єктів правовідносин. В тексті статті 148^6 законодавець безпосередньо вказує, який саме різновид конфіденційної інформації покликана захищати зазначена стаття. Таким різновидом конфіденційної інформації є комерційна таємниця. Законодавством України визначене поняття комерційної таємниці підприємства. Це відомості, які не є державною таємницею, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, розголошення яких може завдати шкоди його інтересам. Склад і обсяг таких відомостей, порядок їх захисту визначає керівник підприємства, або підприємець-громадянин [1-13].

Так звана "група" злочинів, предметом яких виступає комп′ютерна інформація, в чинному КК України 1960 року представлена лише одним складом. Це порушення роботи автоматизованих систем, передбачене ст. 198′ КК України. Ст. 198′ КК України має наступну диспозицію: "Умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації". Як кваліфікуючу ознаку зазначеного складу ч. 2 ст. 198′ КК України визначає завдання шкоди у великих розмірах, скоєння

злочину повторно або за попереднім зговором групою осіб. Таким чином, як бачимо, ст. 198′ є досить об′ємною за своїм змістом. Фактично вона передбачає два самостійні склади злочину: втручання в роботу автоматизованих систем та розповсюдження шкідливих (рос. "вредоносных") програм та технічних засобів, призначених для незаконного проникнення в АС. Ці склади – з незначними відмінностями – виступають аналогами складів злочинів, передбачених ст. 272-273 нового КК РФ, які складають главу 28 КК РФ "Злочини в сфері комп′ютерної інформації". Існування такого роду розділу в КК РФ, а також розділів кримінальних кодексів та окремих нормативних актів кримінального законодавства в цілій низці країн являє собою істотне зрушення на шляху до відокремлення так званих інформаційних злочинів у самостійну групу. Інформаційні злочини, безперечно, не вичерпуються комп′ютерними, з чим погоджується значна кількість дослідників власне проблеми комп′ютерних злочинів. Однак останні продовжують залишатися практично єдиним предметом інтересу в інформаційній сфері для представників наук кримінального циклу, оскільки лише вони, як було зазначено вище, мають кримінально-правову базу, що дозволяє розцінювати такого роду злочини як самостійну групу, що має специфічний об′єкт (в проекті нового КК України також передбачена глава "Злочини в сфері використання автоматизованих електронно-обчислювальних систем"). Для цих злочинів, як відносно нового виду злочинної діяльності, безпосередньо пов′язаної з розвитком інформаційного суспільства, простежується навіть історія їхнього розвитку. Виступаючи лише частиною інформаційних злочинів, так звані комп′ютерні злочини виявляють явний системний характер, який робить їх привабливими як окремий об′єкт дослідження, в той час, як існування системи інформаційних злочинів, а головне – її структура, потребує доведення та аргументації. Разом з тим, вже сьогодні криміналістичні дослідження та аналіз зарубіжного досвіду демонструють недосконаліть кримінально-правового закріплення складів комп′ютерних злочинів, а також необгрунтованість визначення кола інформаційних злочинів лише як комп′ютерних. Слід також відмітити, що доктрина на пострадянському просторі досі не виробила чіткого поняття "комп′ютерного злочину", відносячи до цих злочинів іноді навіть викрадення комп′ютерів. При цьому значна кількість дослідників відмічає спірність власне терміну "комп′ютерні злочини" як технологічно заангажованого та такого, що сприяє виникненню різного роду непорозумінь (аналогічні суперечки досі точаться й навколо термінів "комп′ютерне право", "інформаційно-комп′ютерне право" тощо). Відмічаючи численність норм, присвячених комп′ютерним злочинам (поки що за традицією ми в даній роботі вживатимемо цей термін) в кримінальному праві різних країн, а також присвячених їхньому аналізу наукових праць, до яких ми ще звертатимемося в цьому підрозділі даної роботи, вважаємо доцільним розпочати дослідження з відповідної норми кримінального кодексу України, а саме за ст. 198′. Предметом злочину, передбаченого ст. 198′, виступають: автоматизовані системи, які у відповідності із Законом України "Про захист інформації в автоматизованих системах" від 5. 07. 1994 р. являють собою "системи, що здійснюють автоматизовану обробку даних та до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки та зв′язку), а також методи та процедури, програмне забезпечення", носії інформації (комп′ютерної) – фізичні об′єкти, поля та сигнали, хімічні середовища, накопичувачі даних в інформаційній системі; інформація, що циркулює в АС – сукупність всіх даних та програм, що використовуються в АС незалежно від способу їх фізичного або логічного представлення (ст. 1 Закону України "Про захист інформації в автоматизованих системах"); програмні та технічні засоби, призначені для незаконного втручання в роботу автоматизованих систем. При цьому зазначені програмні та технічні засоби виступають предметом самостійного складу злочину (що відрізняється від втручання в роботу автоматизованих систем), а також можуть виступати знаряддям здійснення втручання в роботу автоматизованих систем. Програмні засоби, призначені для незаконного проникнення в АС – це специфічні комп′ютерні програми (програмні блоки, програмне забезпечення), за допомогою яких можна здійснити несанкціонований доступ до інформації, що зберігається або обробляється в АС, або забезпечує зберігання та обробку в АС іншої інформації. Їхній спектр є достатньо широким, однак кримінальну відповідальність за ст. 198′ тягне лише розповсюдження таких програмних засобів, які здатні призвести до спотворення (викривлення) або знищення інформації або її носіїв, зокрема, шляхом викривлення процесу обробки інформації. Таким чином, як власне незаконне проникнення в АС (а також несанкціонований доступ до інформації, що не перебуває в АС або не призначена для обслуговування їх роботи), так і розповсюдження програмних засобів для його здійснення, якщо це не завдає шкоди інформації або її матеріальним носіям, не є кримінально караним (що є не досить виправданим, оскільки може призвести до ознайомлення з інформацією, й, відповідно, до її закріплення у свідомості особи, що здійснює такий незаконний доступ до інформації, а рівно й до її копіювання на матеріальні носії – без завдання шкоди інформації або її носіям). Те ж саме можна констатувати й щодо технічних засобів, призначених для незаконного проникнення в автоматизовані системи. Під такими технічними засобами розуміють різного роду пристрої, обладнання тощо, що забезпечують безпосереднє підключення до АС або до каналів передачі даних, або ж здатні шляхом формування полів, сигналів, середовищ створити

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

умови для несанкціонованого доступу до інформації з метою ознайомлення з нею особами, що не мають права доступу до такої інформації, або ж з метою впливу на процес обробки інформації в АС, порушення роботи АС, викривлення або знищення інформації або її носіїв (матеріальних) [3, 11, 12, 17, 20].

Ст. 273 КК РФ, яку можна розглядати як аналог норми ст. 198′ КК України, передбачає такий склад злочину, як розповсюдження програмних та технічних засобів, призначених для незаконного проникнення в АС, однак предмет першої певною мірою відрізняється від відповідного предмету ст. 198′ КК України. По-перше, предметом ст. 273 КК РФ є лише програмні засоби, а саме – шкідливі програми. При цьому, по-друге, шкідливість програм передбачає не лише їхню здатність до спотворення або знищення інформації, але й здатність призводити до несанкціонованого блокування й копіювання інформації. Крім того, в ст. 273 КК РФ мова йде про модифікацію інформації, а не про викривлення, як це має місце в ст. 198′ КК України. Це представляється більш вірним, оскільки небезпечними є (можуть бути) будь-які несанкціоновані зміни, а не лише такі, що викривляють інформацію. Слід також відмітити, що ст. 273 КК РФ визначенням відповідного предмета підкреслює суспільну небезпеку будь-яких шкідливих програм як різновиду інформаційної зброї, незалежно від того, чи призначені вони (окрім шкідливих властивостей) ще й для незаконного проникнення в АС, або ж для здійснення несанкціонованих дій над інформацією, в тому числі й в умовах санкціонованого доступу (наприклад, коли особа одержує доступ до інформації з метою ознайомлення з нею, однак право модифікувати, копіювати чи знищувати інформацію такій особі при цьому не надається). Ст. 198′ КК України "Порушення роботи автоматизованих систем" розміщена в главі IX КК України "Злочини проти порядку управління", що відповідним чином визначає і об′єкт цього злочину – як суспільні відносини в сфері належного здійснення управління (родовий об′єкт). Разом з тим таке визначення об′єкту злочину, передбаченого ст. 198′ КК України, явно не відповідає дійсності (що підтверджує розгубленість законодавця при вирішенні питання, куди б "подіти" новий та специфічний склад злочину). Незважаючи на те, що Законом України "Про захист інформації в АС" передбачені вимоги, що пред′являються до роботи АС та обробки в них інформації, ці правила стосуються (сфера їхньої дії) діяльності власників (володарів АС). Навіть якщо відкинути той факт, що АС не належить монопольно державі, та крім загальних правил, встановлених зазначеним Законом, всі решта встановлюються власником інформації, - а це вже ставить під сумнів існування "порядку управління" в тому значенні, в якому він має місце як родовий об′єкт інших злочинів, передбачених гл. IX КК України – порушити порядок управління в сфері функціонування АС, скоріш за все, може саме власник АС та особи, що на нього працюють, а не особи, що не мають до роботи АС жодного стосунку (які, однак, й вбачаються як суб′єкт порушення роботи автоматизованих систем). Кінцевою метою суб′єкта, який посягає на роботу автоматизованих систем, є саме інформація, яка циркулює в АС, навіть в тому випадку, коли на конкретній інформації випробовуються засоби порушення процесу обробки інформації. Це особливо чітко демонструє формулювання ст. 198′ КК України, де обов′язково передбачається як дійсний (для втручання в роботу АС) або потенційний (для розповсюдження програмних та технічних засобів) наслідки вчинюваних винним дій знищення або пошкодження інформації (тим більше про інформацію, як про кінцеву мету втручання в роботу АС, мова може йти у випадках, коли таке втручання мало місце задля ознайомлення з інформацією). Тому, щодо злочину, передбаченого ст. 198′ КК України так само, як і щодо інших злочинів, що мають інформацію своїм предметом, доцільно вести мову про специфічний родовий (а також можливо – видовий) та безпосередній об′єкт, оскільки останній може розглядатися як похідний від родового. Навіть у випадку, якщо предметом злочину виступають інформаційні технології в процесі їхнього функціонування, або як такі, що містять інформацію, це безпосередньо пов′язане з інформацією як предметом злочину, тобто предмет злочину буде комплексним. Зазначимо також, що з рівним успіхом об′єктом злочину, що розглядається (та інших злочинів відповідної групи), можуть виступати й суспільні відносини в сфері права власності, оскільки інформацію на законодавчому рівні визнано предметом вказаних злочинів. Втручання в роботу АС в багатьох випадках взагалі не є метою, задля якої вчинюється злочин (тобто суб′єкт злочину як правило не планує знищити якусь абстрактну інформацію лише тому, що вона циркулює в АС), а становить собою засіб вчинення інших злочинів. Водночас, шляхом втручання в роботу АС можуть бути вчинені інші протиправні дії проти охоронюваної законом інформації (не передбачені поки що кримінальним кодексом України), а також окремі злочини, передбачені КК України як злочини неінформаційного характеру, в яких інформація, може бути виділена як додатковий предмет. Мова йде в першу чергу про "комп′ютерні розкрадання" та "комп′ютерні шахрайства", які мають значну питому вагу в посяганнях на інформаційну безпеку (та суспільні відносини в сфері здійснення законних майнових прав) суб′єктів правовідносин, а також безперечно лідирують за розмірами матеріальної шкоди, що завдається. Вітчизняний законодавець поки що не виділив специфіки зазначених протиправних дій, не передбачивши навіть відповідних кваліфікуючих ознак злочину, що мало б бути обумовлено підвищеною суспільною небезпекою злочинів, які вчинюються за допомогою інформаційних техно-

логій та АС зокрема. В таких випадках не завжди може виявитися можливою й кваліфікація відповідних дій за сукупністю як протиправних, що передбачені ст. 198′ КК України, оскільки "на вхід" АС-"жертви" може подаватися шкідлива інформація як знову створювана, а не спотворюватись інформація, яка вже циркулює в АС (шкідливі наслідки, таким чином, викликаються тим, що неправдиву інформацію було оброблено та сприйнято як правдиву). З урахуванням зазначених обставин в зарубіжних країнах з окремих традиційних складів злочинів, щодо яких має місце тенденція зростання кількості випадків застосування інформаційних технологій задля їх скоєння, що, в свою чергу, надає зазначеним злочинам певної специфіки порівняно з первинним станом, виділяють нові склади, які враховують всі ці особливості, що цілком закономірно в умовах інформаційного суспільства [16, 18, 19, 21, 22, 23-27].

Злочини, які мають предметом власне документи, не вичерпуються складами, що передбачені ст. 193, 193′, 194, 194′ КК України. Це дозволяє виділити наступну групу злочинів, які підлягають дослідженню, як такі, що посягають на різноманітні матеріальні носії інформації: виготовлення або збут підробних грошей та цінних паперів (ст. 79); підлог виборчих документів (ст. 128); порушення законодавства про референдум /у формі підлогу документів/ (ст. 129′); порушення порядку випуску та обігу цінних паперів (ст. 148^3 ч. 2); підробка знаків поштової оплати та проїзних квитків (ст. 153); незаконне виготовлення марок акцизного збору (ст. 153′); посадовий підлог (ст. 172); ухилення військовозобов′язаних від зборів та обліку /в формі підробки документів/ (ст. 192); викрадення або пошкодження документів, штампів, печаток (ст. 193); купівля, продаж або інша оплатна передача чи одержання посвідчення або іншого офіційного документа (ст. 193′); підробка документів, штампів і печаток, збут їх та використання завідомо підроблених документів (ст. 194); знищення, підробка або заміна номерів вузлів та агрегатів транспортного засобу (ст. 194′); незаконне використання емблеми червоного хреста (ст. 200); незаконне підняття державного прапора України (ст. 201); незаконний обіг документів на одержання наркотиків (ст. 229^{13}); незаконна видача рецепта (ст. 229^{14}); ухилення від військової служби /в формі підробки документів/ (ст. 243); незаконне носіння знаків червоного хреста та півмісяця (ст. 263). При цьому склади злочинів, передбачені ст.ст. 193, 193′, 194 КК України є, так би мовити, ключовими, такими, що охоплюють практично всі інші наведені склади злочинів, тобто, всі решта можуть бути розглянуті на їхньому прикладі, з відповідними доповненнями. Необхідно зазначити, що диспозиція ст. 193 КК України вказує на те, що документи (офіційні або приватні), а також штампи та печатки, для того, щоб визнаватися предметом злочину, передбаченого ст. 193 КК України (ч. 1), мають перебувати у державних або громадських організаціях. З одного боку, така конкретизація, очевидно, має за мету виділити більш-менш чітке коло документів, що захищаються кримінально-правовими засобами, і відповідно, є виправданою. Разом з тим, не меншою мірою небезпеці злочинних посягань піддаються документи, особливо – офіційні, що знаходяться у громадян. Крім того, в державних або громадських юридичних особах може знаходитись значна кількість різноманітних документів неофіційного характеру, зокрема й таких, що в силу наведених вище ознак не потребують кримінально-правового захисту: чернетки, первинні версії документів, поточні записи, фотокартки, що не мають стосунку до діяльності юридичної особи, де вони зберігаються. Це ще раз підтверджує необхідність виділення іншого критерія для надання кримінально-правового захисту (таким критерієм може слугувати суб′єктивна значимість документа для його власника та його охоронюваність останнім). При цьому офіційні документи повинні мати кримінально-правовий захист в будь-якому разі, тобто незалежно від того, у фізичних чи юридичних осіб вони перебувають. Зазначимо, що предмет злочинів, передбачених ст. 193 та 194 КК України, описаний в диспозиції відповідних статей більш конкретизовано: це офіційні документи, що видаються підприємством, установою, організацією (причому в ст. 194 знову підкреслюється, що ці юридичні особи мають бути державними або громадськими), а крім того, надають права або звільняють від обов′язків. Таке визначення предмета злочину також може бути подвійно розтлумачене. З одного боку, воно дозволяє чітко визначити коло документів, що одержують кримінально-правовий захист від протиправних діянь, передбачених ст.ст. 193′ та 194 КК України. Однак, з іншого боку, це означає, що, наприклад, від підробки не захищеними виявляються інші (не правовстановлюючі) офіційні, а також різноманітні приватні документи. Водночас, досить часто вони виступають вірогідним об′єктом підробки, наприклад, якщо мова йде про заповіти, які, хоча й посвідчуються нотаріусами, не можуть розглядатися як такі, що видаються "підприємствами, установами та організаціями". Крім того, вже йшлося про роль документів в процесі доказування. Враховуючи, що КК України не містить спеціальних статей, які б встановлювали відповідальність за підробку (фальсифікацію) доказів, зокрема документів, останні практично позбавлені кримінально-правового захисту, що вважається недопустимим. Більш-менш однозначно визначившись з предметом злочинів, що посягають на матеріальні носії інформації та порядок її належного функціонування, можна дійти висновку, що об′єкт зазначених злочинів на цей час також не є єдиним. Визначити суспільні відносини, які, виходячи з чинного кримінального законодавства, визнаються об′єктом злочинів, що досліджуються в даному підрозді-

лі, дозволяє розташування статей, що встановлюють відповідальність за відповідні злочини, в структурі Особливої частини КК України. Переважну більшість таких злочинів законодавець відносить до злочинів проти порядку управління, а відповідно, як об′єкт розглядаються суспільні відносини в сфері належного здійснення управління (нагадаємо, що після попереднього дослідження інтерес становитимуть злочини, передбачені ст.ст. 128, 129′, 172, 192-194, 229^{13-14}, 243, а також – щодо цінних паперів, які не є кредитними грошима – ст. 79, 148^{3}). Водночас, навіть ті автори, які обмежують групу злочинів, що посягають на матеріальні носії інформації та порядок їх належного функціонування, включаючи до неї виключно злочини проти порядку управління, передбачають в окремих випадках наявність додаткових об′єктів [11, 12].

Група злочинів, що має своїм предметом об′єкти інтелектуальної власності, згідно з чинним КК України, складається з двох складів: порушення авторських прав (ст. 136 КК України) та порушення прав на об′єкти права інтелектуальної власності (ст. 137 КК України). Вже формулювання назв зазначених статей є некоректним, оскільки при співставленні дозволяє дійти висновку про те, що об′єкти авторського права начебто не належать до об′єктів інтелектуальної власності (права інтелектуальної власності). Разом з тим, належність об′єктів авторського права до об′єктів інтелектуальної власності не викликає сумнівів, незважаючи на дискусійний характер інститута інтелектуальної власності з точки зору його складу (про що вже відмічалося стосовно комерційної таємниці). Так, з точки зору цивільно-правової охорони виділяють дві форми інтелектуальної власності: авторське право та право промислової власності, при цьому до останнього відносять право на винаходи, корисні моделі, промислові зразки, право на науково-технічну інформацію, а також право на секрети виробництва та інші інститути, що не охоплюються авторським правом, оскільки перелік об′єктів промислової власності згідно з Паризькою конвенцією 1893 року не є вичерпним. Згідно з іншою точкою зору, у світі існують три загальновизнаних форми інтелектуальної власності: авторське право, патентне право, а також інститут комерційної таємниці, тобто відбувається розподіл інститута промислової власності на патентне право та секрети виробництва (про недоцільність виділення комерційної таємниці як форми промислової власності, а не різновиду інформації з обмеженим доступом, вже відмічалося в одному з попередніх підрозділів, присвячених злочинам, предметом яких виступає інформація з обмеженим доступом). В будь-якому разі злочини, які розглядатимуться в цьому підрозділі, мають своїм предметом об′єкти інтелектуальної власності (оскільки порушення права інтелектуальної власності в його різних формах можливе лише щодо конкретних об′єктів інтелектуальної власності, тим більше виходячи з диспозицій відповідних статей є підстави вести мову про предметний склад злочинів). Інше питання полягає в тому, наскільки повним є кримінально-правовий захист прав на об′єкти інтелектуальної власності, тобто чи на всі об′єкти інтелектуальної власності він поширюється. Однак винний завжди прагне привласнити той чи інший результат інтелектуальної праці, а не абстрактно порушити чиєсь право [4-7].

Відсутність підстав до застосування спеціальних форм та підстав правового захисту не означає того, що певна інформація не підлягає правовому захистові взагалі. Згідно з чинним законодавством повинна мати охорону будь-яка інформація, однак за умови, що вона є документованою або публічно-оголошеною. Як вже зазначалося вище, поняття “документована інформація” викликає певні ускладнення в розумінні, особливо у співставленні з тезою про одержання інформацією правового захисту незалежно від форми її представлення. Це пов′язане в першу чергу з фактом існування інформації, закріпленої на так званих “ідеальних” носіях (на відміну від матеріальних), тобто відбитої у свідомості людини. Вважаємо, що така інформація потребує правового захисту, в тому числі кримінально-правового. Приклади кримінально-правового захисту інформації, відбитої у свідомості людини, можуть бути наведені, зокрема, щодо інформації з обмеженим доступом: так, державна зрада в формі шпигунства або власне шпигунство будуть мати місце незалежно від того, чи одержані відомості (ті, що передаються суб′єктом відповідного злочину) з матеріальних носіїв інформації, чи добровільно або примусово – від осіб, яким така інформація довірена. Аналогічним чином це відбувається й при розголошенні інформації з обмеженим доступом – воно найчастіше здійснюється особами, яким довірено зазначену інформацію, мовним шляхом (звідси й назва відповідного злочину) [11, 12].

Однак інформація з обмеженим доступом не є єдиним різновидом інформації, що здатна відбиватися та фіксуватися у свідомості людини – здатність до цього є притаманною інформації в цілому. При цьому слід зазначити, що окрема інформація взагалі може не закріплюватися на матеріальних носіях – тобто не закріплюватись в матеріальних носіях у вигляді специфічного блока відомостей, які становлять інтерес в світлі конкретної мети (наприклад, показання свідка), - а первинно існувати виключно в свідомості людини. Звісно, враховуючи особливості представлення та закріплення інформації, про яку йде мова (закріплену в свідомості людини) слід відзначити характер можливих злочинних посягань на неї: навряд чи мова може йти про завдання шкоди цілісності та достовірності такої інформації. Водночас, оскільки така інформація не є загальновідомою в силу тих чи інших обставин, вона може становити інтерес для зловмисників. Таким чином, вона

може виступати предметом злочинів, суть яких полягає в незаконному одержанні інформації. В цьому випадку шкода, що завдається інформаційній безпеці, є подвійною: небезпеці підлягає не лише інформація (внаслідок її незаконного одержання), але й порушується конституційне право громадян на розповсюдження інформації на власний розсуд. При цьому факт незаконного одержання інформації може мати місце незалежно від того, чи лежить на особі, яка володіє відповідною інформацією, обов′язок повідомити її певним суб′єктам. Не має значення також і те, хто саме незаконно (в незаконний спосіб) одержує інформацію – той суб′єкт, якому інформація обов′язково має бути повідомлена, або ж іншими особами (зазначимо лише, що для цих "інших осіб" інформація може й не мати того характеру, – а, відповідно, й інтересу, яким зумовлене її незаконне одержання – як для суб′єктів, яким інформацію обов′язково має бути повідомлено). Кримінальний Кодекс України на цей час містить два склади злочинів, що можуть бути віднесені до досліджуваної групи. Очевидний предметний характер одного з них підкреслюється не завжди, хоча в даному випадку ця складність проявляється в дещо іншому аспекті, ніж для посягань на об′єкти права інтелектуальної власності та права авторства на них – в цьому складі злочину звичайно виділяють потерпілого. Мова йде про такий склад злочину, як примушування давати показання (ст. 175 КК України). В структурі Особливої частини КК України зазначений склад розташований в главі VIII "Злочини проти правосуддя". Об′єкт злочинів, що належать до даної групи, який визначається, виходячи з існуючої конструкції Особливої частини КК України, вже розглядався на прикладі такого злочину, як розголошення таємниці попереднього слідства (ст. 181 КК України). Однак, якщо склад злочину, передбаченого ст. 181 КК України, носить очевидний інформаційний характер (посягає на безпеку інформації з обмеженим доступом), "інформаційність" злочину, передбаченого ст. 175 КК України, не є настільки очевидною. Це пов′язане, як вже зазначалося, з подвійною небезпекою посягання для інформаційної безпеки, а також з наявністю потерпілого. Щодо предмета злочину, передбаченого ст. 175 КК України, можна стверджувати, що він являє собою інформацію, яка не є загальнодоступною, хоча може й не становити інформацію з обмеженим доступом. У випадку, коли інформація одночасно становить й інформацію з обмеженим доступом, необхідно в першу чергу дослідити правовий режим того конкретного різновиду інформації з обмеженим доступом, який має місце в конкретному випадку – слід встановити, чи мають право на доступ до такої інформації органи та особи, що здійснюють попереднє розслідування, або ж ні, яке це має місце щодо адвокатської таємниці. В останньому випадку на особу, у віданні якої на законній підставі знаходиться зазначена інформація, не може покладатися обов′язок повідомляти цю інформацію органам або особам, що здійснюють попереднє розслідування (а також суду, хоча судді й не визначені як потенційні суб′єкти злочину, передбаченого ст. 175 КК України). Таким чином, будь-які дії щодо одержання від вказаних осіб такої інформації – навіть такі, які в усіх інших випадках не могли б розглядатися як неправомірні – стосовно інформації з абсолютним обмеженням доступу завжди будуть неправомірними. Крім того, інформація становить інтерес з точки зору розслідування та розкриття злочинів. Наступною особливістю інформації є те, що вона – крім зазначених вище випадків, а також випадків, коли допитуваний не зобов′язаний давати показання (підозрюваний, обвинувачений та їхні близькі родичі) – має бути в обов′язковому порядку повідомлена органам чи особам, що ведуть попереднє розслідування. Зазначені особливості інформації, що становить предмет злочину, передбаченого ст. 175 КК України, дозволяють з′ясовувати й відповідні особливості особи потерпілого. В свою чергу, все це впливає на властивості об′єктивної сторони відповідного злочину. Так, будь-які примусові дії (їхні форми детально розглянуті в кримінально-правовій літературі) із здобуття інформації, яка хоча й становить інтерес в процесі попереднього розслідування або судового розгляду, однак на яку не поширюється режим обмеженого доступу абсолютного характеру, слід розцінювати як незаконні, а відповідно – і як такі, що створюють об′єктивну сторону злочину. Щодо осіб, не зобов′язаних повідомляти інформацію, незаконними будуть не лише дії, які безпосередньо примушують до дачі показань, але й апелювання до неіснуючого обов′язку повідомляти інформацію або ж попередження про неіснуючу кримінальну відповідальність за відмову від дачі показань. Іншим злочином, що входить до групи, яка розглядається, є злочин, передбачений ч. 2 ст. 57 КК України, а саме: "передача або збирання за завданням іноземної розвідки відомостей, що не становлять державної чи військової таємниці, для використання їх на шкоду інтересам України, вчинені іноземним громадянином або особою без громадянства". Особливістю предмета зазначеного злочину є те, що ним, за змістом чинного законодавства, може виступати й загальновідома інформація, на поширення якої в Україні немає обмежень, тобто будь-які "документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі". При цьому, на думку законодавця, такі відомості не повинні стати надбанням іноземної розвідки, водночас попереднє готування, спланованість "завдання іноземної розвідки" може бути характерною лише для збирання інформації. Разом з тим, якщо від особи, яка відповідає ознакам потенційного суб′єкту цього злочину, було одержано інформацію без інформування цієї особи про мету подальшого використання зазначеної інформа-

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

ції, або ж якщо збирання інформації велося за межами України, важко співвіднести можливість реалізації кримінальної відповідальності за відповідний злочин з положеннями ч. 1 ст. 50 Закона України "Про інформацію", а саме з нормою про те, що міжнародна інформаційна діяльність, здійснювана Україною, полягає, зокрема в "…цілеспрямованому поширенні за межами України державними органами і об'єднаннями громадян, засобами масової інформації та громадянами всебічної інформації про Україну". Особливо слід враховувати, що сучасні технічні можливості, зокрема використання глобальної мережі Інтернет, за незначний час, без зміни місця перебування та без порушення чиїхось інтересів роблять доступною будь-яку відкриту інформацію будь-якому користувачеві, причому простежити подальшу долю цієї інформації, а в окремих випадках і особу користувача, досить складно або взагалі неможливо. Тому, на наш погляд, положення кримінального законодавства щодо злочину, який розглядається, потребують істотного реформування, інакше це безперечно відіб'ється на їх дієвості [1, 11, 12].

Література: 1. Закон України "Про інформацію" від 2.10.1992 р. // Закони України. - Т. 4. – К., 1996. 2. Закон України "Про державну таємницю" від 21.01.1994 р. // Закони України. - Т. 7. – К., 1997. 3. Закон України "Про захист інформації в автоматизованих системах" від 5.07.1994 р. // Закони України. - Т. 7. - К., 1997. 4. Закон України "Про авторське право і суміжні права" від 23.12.1993р. // Закони України. - Т. 6. – К., 1996. 5. Закон України "Про охорону прав на винаходи та корисні моделі" від 15.12.1993р. // Закони України. - Т. 6. – К., 1996. 6. Закон України "Про охорону прав на знаки для товарів та послуг" від 15.12.1993р. // Закони України. - Т. 6. – К., 1996. 7. Закон України "Про охорону прав на промислові зразки" від 15.12.1993 р. // Закони України. - Т. 6. - К., 1996. 8. Закон України "Про адвокатуру" від 19.12.1992 р. // Закони України. - Т. 4. - К., 1996. 9. Закон України "Основи законодавства України про охорону здоров'я" від 19.11.1992 р. // Закони України. - Т. 4. - К., 1996. 10. Закон України "Про банки та банківську діяльність" від 20.03.1991 р. // Закони України. - Т. 1. - К., 1996. 11. Кримінальний кодекс України. // www.liga.kiev.ua. 12. Науково-практичний коментар до Кримінального кодексу України.- К., 2000. 13. Про перелік відомостей, що не становлять комерційної таємниці, Постанова КМ України від 9 серпня 1993 р. № 611 // Збірник постанов Уряду України. 1993, № 12. 14. Минимальные стандартные правила Организации Объединенных наций, касающиеся отправления правосудия в отношении несовершеннолетних ("Пекинские правила") от 29. 11. 1985 г. // Права человека и судопроизводство: Собрание международных документов. - Produced by USIA Regional Program Office, Vienna. 15. The European Union Directives, http:// www2.echo.lu/ legal/en/dataport/directiv/ directiv/html. 16. УК Российской Федерации, от 13. 06. 1996 г. № 63-ФЗ // Собрание законодательства РФ, 1996. № 25. 17. Баранов А. А. Уголовная ответственность за компьютерные преступления // Безопасность информации, 1996, № 2. 18. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. - М., 1989. 19. Батурин Ю. М. Проблемы компьютерного права. - М., 1991. 20. Біленчук П. Д., Ващенко С. В. Визначення об'єкту злочину, пов'язаного з посяганням на роботу комп'ютерних систем. // Інформаційні технології та захист інформації: Збірник наук.праць. - Запоріжжя, 1998,- № 2. С. 94-96. 21. Вехов В. Компьютерные преступления, М., 1996. 22. Комментарий к Уголовному кодексу Российской Федерации: в 2 т. / Под ред. О. Ф. Шишова.- М.: ООО «Издательство Новая Волна», 1998. 23. Копылов В. А. Информационное право: Учебное пособие. - М.: Юристъ, 1998. 24. Крылов В. В. Информационные компьютерные преступления. - М.: Издательская группа ИНФРА • М - НОРМА, 1997. 25. Кузнецов П. А. Информационная война и бизнес. // Конфидент. 1996. № 4. С. 21-23. 26. Курило А. П. Об ответственности за правонарушения при работе с информацией // Вопросы защиты информации. 1994. № 2. С. 19-20. 27. Рачук Т. В. Уголовные наказания за информационные преступления. // Конфидент. 1996. № 4. С. 25-27.

УДК 343. 32

ВІДПОВІДАЛЬНІСТЬ ЗА РОЗГОЛОШЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ ЗА НОВИМ КРИМІНАЛЬНИМ ЗАКОНОДАВСТВОМ УКРАЇНИ

Олександр Шамсутдінов
Служба безпеки України

Анотація: **Розглянуті кримінальна відповідальність за розголошення державної таємниці, сучасні проблеми вдосконалення кримінального законодавства України у сфері охорони державної таємниці.**