the scientific and legal experts means that the "detention order" should include a preventive measure, which by its actual content close to the prison.

Determined that the decision of the investigating judge or the court for permission to arrest the purpose pretext for a motion for a preventive measure in the form of detention cannot be considered "detention order" within the meaning of Article 25 of the European Convention on Extradition and not decision investigating judge or the court of custody within the meaning of Article 575 of the Criminal Code of Ukraine.

The author made a number of conclusions and generalizations on improving law enforcement Ukraine on cooperation with the International Criminal Police Organization Interpol and police agencies of European countries on extradition.

Key words: *criminal proceedings, arrest warrants, detention, extradition, extradition.*

УДК: 343.3/.7

А. В. ЛАНДІНА,
кандидат юридичних наук

АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАСОБАМИ КРИМІНАЛЬНОЇ ЮСТИЦІЇ В УКРАЇНІ

Статтю присвячено окремим аспектам забезпечення інформаційної безпеки кримінально-правовими засобами. Встановлено, що злочини проти інформаційної безпеки поміщені у різних розділах Особливої частини КК України, але мають спільні ознаки усіх елементів складу злочину, які об'єднують їх у окрему групу. Визначені основні загрози, які створюють небезпеку для інформаційного суспільства, що потребує розробки ефективних засобів їх запобігання.

Ключові слова*: інформаційна безпека, кримінальна юстиція, злочини проти інформаційної безпеки, об'єкт злочину, предмет злочину, суб'єкт злочину, джерело загрози, інформаційна війна.*

Ландина А. В. **Актуальные проблемы обеспечения информационной безопасности средствами уголовной юстиции в Украине**

Статья посвящена отдельным аспектам обеспечения информационной безопасности уголовно-правовыми средствами. Установлено, что преступления против информационной безопасности расположены в разных разделах Особенной части УК Украины, но имеют общие признаки всех элементов состава преступления, которые объединяют их в отдельную группу. Определены основные угрозы, которые создают опасность для информационного общества, что требует разработки эффективных средств их предотвращения.

Ключевые слова*: информационная безопасность, уголовная юстиция, преступления против информационной безопасности, объект преступления, предмет преступления, субъект преступления, источник угрозы, информационная война.*

Landina A.V. **Actual Problems of Security of Information Safety by Facilities of Criminal Justice in Ukraine**

The article is devoted to separate aspects of information security by recourses criminal law . It is established that crimes against information security located in different sections of the Special part of the Criminal code of Ukraine, but have common features all the elements

of the crime, that united them in a separate group. Defined the main threats that pose a risk to information society, which requires the development of effective methods of their prevention.

***Key words**: information security, criminal justice, crimes against information security, object of crime, item of crime, subject of crime, the source of the threat, information warfare.*

Кінець XX – початок XXI ст. у світі характеризується складними трансформаційними процесами, що пов'язані з переходом людства до інформаційного суспільства. Вважається, що ключовою особливістю цього переходу є стрімкий розвиток інформаційно-комунікаційних технологій та зростання значущості інформаційної складової в усіх сферах життєдіяльності людини, суспільства, держави та міжнародної спільноти[1]. Розвиток і впровадження практично в усі сфери інформаційних технологій суттєво змінює структуру суспільства, а також трансформує міжнародні відносини. Одним із найважливіших напрямів цієї трансформації стає реалізація національних інтересів щодо забезпечення національної безпеки[2]. Загалом національні інтереси держави у інформаційній сфері полягають переважно в гармонійному розвитку інформаційної структури держави.

За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки[3]. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку країни. Всі ці поняття, на нашу думку, є структурними складовими інформаційної безпеки.

Тому однією з нагальних проблем для України є необхідність прискорення формування комплексної системи правового регулювання сфери забезпечення інформаційної безпеки[4]. Найбільше навантаження у цьому напрямі порівняно із адміністративно-правовими заходами забезпечення інформаційної безпеки в Україні, на нашу думку, припадає саме на сферу кримінального права. А забезпечення інформаційної безпеки кримінально-правовими засобами повинно забезпечуватися саме у процесі діяльності органів кримінальної юстиції.

Окремі питання інформаційної безпеки, зокрема щодо забезпечення кримінально-правової охорони інформації досліджувалися у роботах Д. С. Азарова, П. П. Адрушка, К. І. Бєлякова, П. С. Берзіна, В. Д. Гавловського, В. І. Голубєва, В. П. Ємельянова, М. В. Плугатиря, А. М. Ришелюка, В. І. Шакуна, Я. Р. Якубовського та ін. Комплексному системному дослідженню проблем кримінально-правової охорони інформаційної безпеки в Україні присвячена монографія М. В. Карчевського[5]. Окремі аспекти даної проблеми були також розглянуті Н. А. Савіновою у контексті дослідження кримінально-правової політики забезпечення інформаційного суспільства в Україні[6].

Одним із проблемних питань досліджуваної проблематики є питання визначення кола суспільно небезпечних діянь, що посягають на інформаційну безпеку, та їх спільних рис, які об'єднують їх у одну групу злочинів. Крім того, потрібно визначити основні напрями діяльності кримінальної юстиції у частині забезпечення інформаційної безпеки в Україні на усіх рівнях, враховуючи наявність норм КК України, що встановлюють кримінальну відповідальність за злочини проти інформаційної безпеки.

До злочинів проти інформаційної безпеки відповідно до змісту норм Особливої частини КК України можна віднести такі з них: злочини проти основ національної безпеки України (ч. 3 ст. 109, ч. 1 ст. 110, ч. 1 ст. 111, ст. 114); злочини проти життя та здоров'я особи (ст. 132, ст. 145); злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина (ст. 158, ч. 1 ст. 159[1], ч. 1 ст. 161, ст. 163, ст. 168, ст. 171, ст. 176, ст. 177, ст. 182); злочини проти власності (ст. 189); злочини у сфері господарської діяльності (ст. 203[1], ч. 2 ст. 209[1], ст. 216, ст. 220[1], ст. 220[2], ст. 222, ст. 223[1], ст. 231, ст. 232, ст. 232[1], ст. 232[2]; злочини проти довкілля (ст. 238); злочини проти громадської безпеки (ст. 256, ст. 258[2], ст. 259); злочини проти громадського порядку та моральності (ст. 295, ст. 300, ст. 301); злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації (ст. 238, ст. 329, ст. 330); злочини проти авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян та злочини поти журналістів (ст. 345[1], ст. 347[1], ст. 348[1], ст. 349[1], ст. 359, ст. 360); злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст. 361, ст. 361[1], ст. 361[2], ст. 362, ст. 363, ст. 363[1]); злочини у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг (ст. 366, ст. 366[1]); злочини проти правосуддя (ст. 376[1], ст. 381, ст. 387); злочини проти порядку несення військової служби (військові злочини) (ст. 422, ст. 435); злочини проти миру, безпеки людства та міжнародного правопорядку (ст. 436, ст. 436[1], ст. 445).

Незважаючи на те, що вище було вказано досить багато злочинів, що посягають на інформаційну безпеку України, є ще норми, які можна віднести до зазначених, але за умови використання для цього інформаційних технологій або спрямування злочину проти певних інформаційних ресурсів (наприклад, ст. 209 «Легалізація (відмивання) доходів, одержаних злочинним шляхом», злочини проти власності, ст. 255 «Створення злочинної організації», ст. 258 «Терористичний акт», ст. 258[1]–258[5], ст. 303 «Сутенерство або втягнення особи в заняття проституцією» та ін.).

Незважаючи на те, що на перший погляд у переважної більшості вказаних злочинів немає нічого спільного, вони мають окремі ознаки елементів своїх складів, які їх певним чином поєднують. Склад злочину визначається у теорії кримінального права як сукупність чотирьох обов'язкових елементів: об'єкта, об'єктивної сторони, суб'єкта та суб'єктивної сторони[7]. Крім того, кожен із цих елементів має обов'язкові та факультативні ознаки. За допомогою цих ознак встановлюється і сам елемент у цілому як певна юридична конструкція, і власне суспільна небезпечність самого вчиненого злочину та суспільна небезпечність особи злочинця. На основі цього відбувається кваліфікація злочину, що у подальшому визначає розмір і вид покарання, достатній і адекватний для кожного конкретного випадку.

Усі злочини, які посягають на інформаційну безпеку, як, власне, і усі інші злочини, мають власний об'єкт посягання. Незважаючи на те, що теорія кримінального права містить безліч теорій щодо визначення поняття загального

об'єкта злочину, ми будемо виходити із теорії, яка підтримується О. М. Костенком та співробітниками Інституту держави і права ім. В. М. Корецького. Як зазначалося, згідно із даною теорією, об'єктом злочину визнається охоронюваний кримінальним законом порядок відносин між людьми, що виникають у суспільстві з приводу матеріальних і нематеріальних предметів.

На нашу думку, спільним для всіх зазначених злочинів є те, що вони мають своїм об'єктом порядок забезпечення інформаційної безпеки у сфері обігу інформації в суспільстві, використання інформаційних ресурсів та інформаційних технологій. Він у переважній більшості названих складів не є основним об'єктом (за винятком таких злочинів, як злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, для яких порядок забезпечення інформаційної безпеки у сфері інформаційних технологій є основним). Специфіка сфери інформаційної безпеки залежить від родового об'єкта, який визначений для таких злочинів у межах розділів Особливої частини КК України.

Також потрібно наголосити на тому, що однією з ознак об'єкта як елементу складу злочину суспільно небезпечних діянь проти інформаційної безпеки є предмет злочину. Тому, виходячи з цього, суб'єкт кожного із злочинів у сфері інформаційної безпеки повинен усвідомлювати особливий характер інформації, з якою пов'язане вчинення суспільно небезпечного діяння. Виникає питання: чи може остання теза означати, що суб'єкт злочинів проти інформаційної безпеки унаслідок володіння особливим видом інформації або який усвідомлює, що вчинення злочину пов'язане із такою інформацією, наділений ознаками спеціального суб'єкта? Для цього потрібно розуміти, що є предметом злочину проти інформаційної безпеки.

Предмет злочину – це факультативна ознака об'єкта злочину, що проявляється у матеріальних цінностях (котрі людина може сприймати органами чуття чи фіксувати спеціальними технічними засобами), з приводу яких та шляхом безпосереднього впливу на які (або без такого впливу) вчиняється злочинне діяння[8]. Оскільки злочини проти інформаційної безпеки завжди пов'язані із порушенням правил обігу певної інформації, то всі вони повинні вважатися злочинами предметними, тому що така інформація сприймається органами чуття людини та/або фіксується спеціальними технічними засобами. Тому при кваліфікації цих злочинів органами досудового розслідування обов'язково повинен встановлюватися їх предмет, оскільки предмет набуває статусу обов'язкової ознаки об'єкта злочинів проти інформаційної безпеки.

Предмет злочину проти інформаційної безпеки зумовлює і вид суб'єкта злочину. Ряд суб'єктів злочину можуть вчинювати злочини у сфері обігу інформації лише у силу виконання певних службових обов'язків, що зумовлює доступ до інформації визначеного характеру. Тому спеціальний суб'єкт при вчиненні злочинів зумовлюється певним службовим становищем, яке займає особа і використовує його при вчиненні злочину, який посягає на інформаційну безпеку.

Але суб'єкт злочину згідно із теорією кримінального права може вважатися спеціальним не лише у тому випадку, коли він займає особливе службове

становище. Суб'єкт може бути спеціальним і за ознаками віку, статі, особливого емоційного та/або фізичного стану, соціальних особливостей. Усі ці ознаки у певних випадках можуть впливати на характеристику суб'єкта інформаційних злочинів.

Щодо проблеми вчинення злочинів, що посягають на порядок забезпечення інформаційної безпеки в суспільстві, юридичною особою, то тут зазначимо таке. Ми вважаємо, що юридична особа позбавлена можливості усвідомлювати, передбачати, бажати, свідомо припускати або легковажно розраховувати на ненастання наслідків свого діяння, а також зазнавати страждань через певні обмеження[9]. Це порушує ряд принципів кримінального права, зокрема принцип винної відповідальності за вчинене суспільно небезпечне діяння; принцип особистої відповідальності; принцип індивідуалізації покарання. Винне ставлення до суспільно небезпечного діяння та його наслідків можливий лише з боку фізичної особи. Те саме можна сказати і про інші зазначені вище принципи – їх дотримання можливе лише у випадку, якщо суб'єктом злочину є фізична особа. Тому ми вважаємо, що юридична особа не може бути суб'єктом злочину взагалі.

Отже, у кожному конкретному випадку вчинення злочину проти інформаційної безпеки потрібно встановлювати, чи властиві суб'єкту даного злочину якісь особливі ознаки і яким чином вони впливають на кваліфікацію злочину та суспільну небезпечність самого суб'єкта.

Спільними ознаками для суб'єктів злочинів проти інформаційної безпеки є ті, що визначені у ст. 18 КК України: осудність, ознака фізичності, досягнення віку кримінальної відповідальності та вчинення злочину, передбаченого КК України. Ніякі інші спільні ознаки суб'єктів злочинів цього виду визначити неможливо. Вирішальне значення при встановленні суб'єкта злочину, що посягає на інформаційну безпеку, має предмет такого злочину.

Для об'єктивної сторони спільним є те, що всі зазначні вище злочини можуть бути вчинені лише шляхом дії, оскільки порушити порядок суспільних відносин у частині забезпечення інформаційної безпеки практично неможливо шляхом бездіяльності (таке можливо лише у випадку сприяння третім особам отримати/передати/поширити певну інформацію, що вже утворюватиме співучасть). Що стосується факультативних ознак об'єктивної сторони злочинів проти інформаційної безпеки, то нічого спільного для цих злочинів серед них немає. У кожному конкретному випадку при кваліфікації злочину визначається, як та чи інша ознака впливає на суспільну небезпечність даного злочину.

Суб'єктивна сторона також має спільні риси для всіх злочинів проти інформаційної безпеки. Обов'язковою ознакою цього елементу складу злочину є вина, формами якої є умисел та необережність. Враховуючи положення норм КК України, зазначених вище, які передбачають відповідальність за злочини проти інформаційної безпеки, можна зробити висновок, що усі вони можуть вчинюватися лише умисно. Це, зокрема, або визначено у диспозиції самої норми, де акцентується увага саме на умисному вчиненні відповідного злочину, або випливає як висновок із самого змісту диспозиції норм. Такі факультативні ознаки суб'єктивної сторони складу злочину, як мотив, мета та емоцій-

ний стан, не мають спільних для всіх злочинів проти інформаційної безпеки рис і можуть впливати на кваліфікацію конкретного діяння у кожному конкретному діянні.

Щодо забезпечення інформаційної безпеки засобами кримінальної юстиції, то тут є ціла низка проблемних питань, які в умовах стрімкого розвитку новітніх інформаційних технологій вимагають негайного вирішення. Основним інструментом кримінальної юстиції є КК України. Але також потрібна розробка ефективних засобів протидії вчиненню цих злочинів, оскільки більшість напрямів, у яких вчинюються злочини проти інформаційної безпеки, так і залишаються неврегульованими.

Кримінальна юстиція України покликана забезпечувати, поряд із іншими, інформаційну безпеку у суспільстві на декількох рівнях. Так, А. М. Кузьменко вважає, що існує три рівні забезпечення інформаційної безпеки в суспільстві, до яких належать: особистісний рівень, який включає формування в особи власного раціонального, критичного мислення, яке повинно базуватися на принципі свободи вибору; загальносуспільний рівень, який передбачає формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні сильні ЗМІ тощо; загальнодержавний рівень, який передбачає загальне інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам[10]. І для забезпечення інформаційної безпеки на кожному з цих рівнів кримінальна юстиція повинна застосовувати спеціальні засоби. Всі ці рівні взаємопов'язані і відсутність регулювання інформаційної безпеки на одному зумовлює її відсутність і на інших двох.

На нашу думку, встановлення кримінальної відповідальності за ряд злочинів проти інформаційної безпеки має найбільше значення саме для загальнодержавного рівня, оскільки притягнення особи до кримінальної відповідальності за вчинення злочинів є засобом державного примусу і одним із основних кримінально-правових засобів впливу кримінальної юстиції на певні явища, зокрема, для забезпечення інформаційної безпеки. Кримінальна відповідальність, і, як наслідок, призначення відповідного покарання, встановлюється від імені держави, чим здійснюється забезпечення безпеки у всіх сферах на рівні державного регулювання.

На особистісному рівні інформаційна безпека формується залежно від особистісних якостей особи. Це залежить від рівня культури особи, ступеня її інтелектуального розвитку, від рівня правосвідомості тощо. Адже свобода вибору людини залежить саме від цих якостей. Для забезпечення інформаційної безпеки на цьому рівні кримінальна юстиція повинна вживати заходів для підняття правової та особистої культури громадян, що забезпечить дотримання приписів у сфері забезпечення інформаційної безпеки. Це можуть бути інформаційні повідомлення у аудіо-, відеоформаті чи друкованому вигляді, які доводитимуть до відома людей, обіг якої інформації та використання яких інформаційних ресурсів та інформаційних технологій є правомірним, а який –

протиправним. Крім того, повинна проводитися робота по забезпеченню правомірного доступу до інформаційних ресурсів, обіг яких не є обмеженим і потреба у яких виникає у людини, що сприятиме тому, що особа відмовиться від використання протиправних засобів для отримання такої інформації. Кримінальна юстиція повинна забезпечити обізнаність людини на особистісному рівні щодо притягнення до кримінальної відповідальності за вчинення певних суспільно небезпечних діянь, які посягають на інформаційну безпеку.

Найскладнішим, на нашу думку, є забезпечення інформаційної безпеки на суспільному рівні. По-перше, складнощі виникають із формуванням якісного інформаційно-аналітичного простору. Адже в умовах стрімкого розвитку новітніх інформаційних технологій важко контролювати обіг інформації в суспільстві і забезпечити відсутність для вільного доступу інформації обмеженого рівня доступності і забороненої законом інформації. Це стосується передусім такої інформації у світовій мережі Internet. В Україні досі не вироблено якісних програм, які б забезпечували більш-менш якісний захист контенту від шкідливої і забороненої законом інформації. Найбільш незахищеною категорією у суспільстві від впливу такої інформації залишаються неповнолітні.

Другою проблемою у частині забезпечення інформаційної безпеки на суспільному рівні є забезпечення наявності сильних незалежних ЗМІ. Як правило, ЗМІ залежно від прихильностей їх власника, надають інформацію упереджено, що створює загрозу невідповідності такої інформації дійсності (її недостовірності), чим порушується право людини на отримання достовірної інформації. Також за допомогою ЗМІ створюється загроза маніпулювання суспільною свідомістю, що також є неприпустимим.

До основних загроз, які існують у сфері інформаційної безпеки, відносять такі: намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації[10]. До інших видів загроз окремі автори відносять: «прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави»[12]. Також перелік таких загроз визначено у Законі України «Про основи національної безпеки»[13].

Особливо актуальним наразі є така загроза інформаційній безпеці, як так звана інформаційна війна. Інформаційні війни, незважаючи на вдавану невелику безпеку, мають підвищений рівень суспільної небезпечності. Потрібно враховувати при цьому, що «інформаційна війна використовує переваги технологічних удосконалень…. Зброєю в цьому напрямі є пристрої та технології, які використовуються для широкомасштабного, цілеспрямованого, швидкого та таємного впливу на цивільні та військові інформаційні системи суперника»[14].

Таким чином, у межах вирішення даного питання перед органами кримінальної юстиції постає проблема як у застосуванні вже існуючих засобів, так і вироблення нових методів протидії та запобігання суспільно небезпечним

впливам у сфері інформаційної безпеки України. Тому, з метою якомога більш ефективного вирішення цих завдань, мають бути насамперед визначені цілі такої діяльності, основні форми і методи досягнення таких цілей, що повинно реалізуватися у межах діяльності органів державної влади, зокрема органів кримінальної юстиції. Це повинно відбуватися в умовах всебічного і глибокого аналізу соціально-економічного, політичного, культурного рівнів розвитку сучасної держави, суспільства і окремих осіб, а також детального вирахування наслідків такої діяльності залежно від обраного варіанта забезпечення інформаційної безпеки у тій чи іншій сфері життєдіяльності відповідно до того, на якому рівні здійснюватиметься така діяльність. І, оскільки інформаційна безпека – це особлива правоохоронювана галузь, органи кримінальної юстиції при виробленні заходів забезпечення такої безпеки, повинні залучати фахівців із інших галузей (технічних, економічних, соціальних, гуманітарних тощо). Лише їх співпраця забезпечить вироблення ефективних і актуальних засобів забезпечення інформаційної безпеки в Україні.

1. *Савінова Н. А.* Кримінально-правова політика забезпечення інформаційного суспільства в Україні: дис. докт. юрид. наук, спец. 12.00.08. Львів, 2013. С. 6; **2.** *Галамба М.* Інформаційна безпека України: поняття, сутність та загрози // Юридичний журнал. – 2006. – № 12. URL: http://www.justinian.com.ua/article.php?id=2509 **3.** *Доктрина інформаційної* безпеки України. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/U514_09.html **4.** *Олійник О. В.* Стан забезпечення інформаційної безпеки в Україні // Юридичний вісник. – 2014. – № 2(31). С. 64; **5.** *Карчевський М. В.* Кримінально-правова охорона інформаційної безпеки України: монографія / МВС України, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.; **6.** *Савінова Н. А.* Кримінально-правова політика забезпечення інформаційного суспільства в Україні: дис. докт. юрид. наук, спец. 12.00.08. Львів, 2013. 510 с.; **7.** *Склад злочину* та його елементи. URL: http://bookish.link/ugolovnoe-pravo/sklad-zlochinu-yogo.html **8.** *Музика А. А., Лащук Є. В.* Предмет злочину: теоретичні основи пізнання: монографія. Київ : ПАЛИВОДА А. В., 2011. С. 167; **9.** *Осадча А. С.* Спеціальний суб'єкт злочину: генезис, функції, проблеми кваліфікації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Харків, 2015. С. 9.; **10.** *Кузьменко А. М.* Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства // Часопис Київського університету права. – 2010. – № 4. С. 318; **11.** *Про основи національної* безпеки України: Закон України // Відомості Верховної Ради України (ВВР). – 2003. – № 39, ст. 351. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15 **12.** *Чудінова Н. В., Грицюк Ю. І.* Інформаційна безпека України та види джерел загроз і небезпек // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами : матер. наук.-практ. конф. (Львів, 14 грудня 2011 р.) Львів : Львівський ДУВС., 2011. С. 250; **13.** *Про основи національної* безпеки України: Закон України // Відомості Верховної Ради України (ВВР). – 2003. – № 39, ст. 351. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15 **14.** *Чудінова Н. В., Грицюк Ю. І.* Інформаційна безпека України та види джерел загроз і небезпек // Проблеми застосування

інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами : матер. наук.-практ. конф. (Львів, 14 грудня 2011 р.) Львів : Львівський ДУВС., 2011. С. 252.

Landina A.V. **Actual Problems of Security of Information Safety by Facilities of Criminal Justice in Ukraine**

The article is devoted to specific aspects of information security criminal law means. Most in this direction falls on the criminal law. Information security should be provided in the course of activity of bodies of criminal justice.

One of the problematic issues of the researched issues is the question of determining the circle of socially dangerous acts that infringe on the security of information, and their similarities that unite them into one group of offenses. Also, you need to determine the main directions of activities of criminal justice in terms of ensuring information security in Ukraine at all levels, given the presence of norms of the criminal code of Ukraine, which establish criminal liability for crimes against information security.

It is established that crimes against information security located in different sections of the Special part of criminal code of Ukraine, but have common features of all elements of the offense that united them into a separate group. All crimes against information security under the criminal code of Ukraine, are United by a number of common features which distinguish them from the totality of crimes: despite the fact that all these crimes are located in various chapters of the Special part of criminal code of Ukraine, which determines their ancestral object, they has as its direct object (primary or secondary mandatory) procedure for ensuring information security in the sphere of circulation of information in society the use of information resources and information technology. Whereas crimes against information security is always associated with the violation of traffic specific information, all they should be considered as subject crimes because such information is perceived by the human senses and/or is fixed with special technical means. Therefore, in the classification of these crimes by the preliminary investigation bodies must set their subject, as the subject acquires the status of a mandatory feature of the object of crimes against information security. The subject of crimes against information security determines a type of the perpetrator. Common features for subjects of crimes against information security are those that are defined in article 18 of the criminal code of Ukraine: sanity, sign of phisically, the age of criminal responsibility and committing a crime under the criminal code of Ukraine. No other common signs of constituent entities of the type of crime can't be determined. Crucial in establishing the subject of the crimes encroaching on information security, is the subject of such crimes. The objective side of crimes against information security is always characterized by action. The subjective side of crimes against information security is characterized by fault in the form of intent.

Defined the main threats that pose a risk to information society, which requires the development of effective means of their prevention. The main threats that exist in the field of information security include the following: attempts to manipulate public consciousness, in particular through the dissemination of inaccurate, incomplete or biased information. To other types of threats some authors include: manifestations of curtailment of freedom of speech and access of citizens to information; dissemination by media of the cult of violence, cruelty, pornography; computer crime and computer terrorism; disclosure of information which constitutes a state secret, and confidential information which are the property of the state or aimed to meet the needs and national interests of society and the state. Especially relevant now the threat of information security is a so-called "information war".

In the framework the solution of this question before the organs of criminal justice, the problem arises as to the application of existing tools and the development of new methods of counteraction and prevention of socially dangerous actions in the field of information security of Ukraine. Because information security is a special pravoohraniteli industry, the criminal justice authorities in the development of measures to ensure such security, is expected to attract specialists from other areas (technical, economic, social, humanitarian, etc.). Only their cooperation will ensure the development of effective and relevant means of ensuring information security in Ukraine.

***Key words**: information security, criminal justice, crimes against information security, object of crime, item of crime, subject of crime, the source of the threat, information warfare.*