Вважаю що джерелами фінансування Фонду можуть бути: суми, стягненні з осіб, які нанесли шкоду; відрахування в державний бюджет частини сум, одержаних: від використання роботи засуджених, від реалізації конфіскованого майна, в результаті стягнення штрафів по кримінальним справам та адміністративним правопорушенням; внески підприємств (всіх форм власності), організацій, громадян; частина сум, одержаних митними органами від реалізації вилучених товарів, які незаконно перетинають кордон; частина сум, одержаних за роботу органів реєстрації актів громадського стану та при здійсненні нотаріальних дій; відрахування з підприємств, працівники яких вчинили злочини. Звичайно, цей перелік не є вичерпним.

За своїми функціями і завданнями такий Фонд наближений до системи органів соціального захисту, тому управління соціального захисту потерпілих від злочинів може бути створене при відповідних міністерствах. Відповідні структури необхідно створити в регіональних, обласних центрах.

Створення спеціального Фонду для відшкодування шкоди потерпілим від злочинів – необхідність продиктована сьогоднішнім днем, яка має реальні шляхи здійснення.

Використана література:

1. Михайленко А. Р. Расследование преступлений: законность и обеспечение прав граждан / А. Р. Михайленко. – К. : Юринком Интер, 1999. – С. 321.

2. Щербаков Ю. В. Проблемы и перспективы защиты прав потерпевшего от преступлений [Електронний ресурс] / Ю. В. Щербаков. – Режим доступу : www.bestreferat.ru/referat-79734/html-97-k

3. Лукин В. Проблемы защиты потерпевших от преступлений: Специальный доклад Уполномоченного по правам человека в Российской Федерации Владимира Лукина / В. Лукин // Российская газета. Федеральный выпуск. – № 4676. – 4 июня 2008 г.

УДК 343.346.6

М.В. Карчевський

КРИМІНАЛЬНО-ПРАВОВІ ЗАСОБИ ПРОТИДІЇ ЗЛОЧИНАМ В СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ ТА МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ ХАРАКТЕРИЗУЮТЬСЯ ЯК НАДЛИШКОВІСТЮ ЗАБОРОНИ ТАК І ПРОГАЛИНАМИ

Чинне законодавство про кримінальну відповідальність за злочини в сфері використання комп'ютерної техніки аналізується з точки зору відсутності прогалин та ненадлишковості заборон.

Ключові слова: *злочини в сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку, прогалина в праві,*

надлишковість кримінально-правової заборони, інформація з обмеженим доступом, спеціальний суб'єкт, спам.

Действующее законодательство об уголовной ответственности за преступления в сфере использования компьютерной техники анализируется с точки зрения отсутствия пробелов и неизбыточности запретов.

Ключевые слова: *преступления в сфере использования электронно-вычислительных машин, систем, компьютерных сетей и сетей электросвязи, пробел в праве, избыточность уголовно-правового запрета, информация с ограниченным доступом, специальный субъект, спам.*

The operating criminal legislation on crimes in sphere of use of computer technics is analyzed from the point of view of absence of blanks and redundancy of an interdiction.

Key words: *crimes in sphere of use of computers, systems, computer networks and telecommunication networks, a blank in the right, redundancy of a criminally-legal interdiction, the information with the limited access, the special subject, spam.*

Наявне у чинному законодавстві кримінально-правове забезпечення протидії злочинам в сфері використання комп'ютерної техніки та мереж електрозв'язку характеризується як прогалинами так і певною надлишковістю передбачених заборон. Чітке визначення цих недоліків та формулювання пропозиції щодо їх усунення є необхідною передумовою якісного оновлення національної правової бази протидії комп'ютерній злочинності.

В першу чергу означене стосується доцільності криміналізації незаконного збуту або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК). Як свідчить проведений аналіз відмежування складу цього злочину від суміжних, кримінальна відповідальність за нього може наступати у наступних випадках:

1) коли розповсюдження або збут комп'ютерної інформації, зміст якої складає державну таємницю, здійснюється особою, якій ці відомості довірені не були, і це не пов'язано з передачею її іноземній державі, іноземній організації або їх представникам;

2) коли розповсюдження або збут комп'ютерної інформації, зміст якої складають:

- відомості про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби;
- лікарська таємниця;
- комерційна або банківська таємниця;
- відомості про заходи безпеки щодо особи, взятої під захист;
- дані досудового слідства чи дізнання;

та ці дії здійснює особа, якій дані відомості довірені не були, тобто вона не мала спеціальних зобов'язань щодо збереження їх в таємниці;

3) коли розповсюдження або збут комп'ютерної інформації, зміст якої складає лікарську, комерційну або банківську таємницю здійснює особа, якій вони були довірені, але наслідків, зазначених у ст.ст. 145 чи 232 не настало;

4) коли здійснюється розповсюдження або збут комп'ютерної інформації, зміст якої складає таємницю усиновлення (ст. 168) або приватного життя (ст. 182), але до умислу суб'єкта не включається усвідомлення та бажання або свідоме допущення, заподіяння шкоди конкретній особі, або чітко визначеній групі осіб, тобто відсутні ознаки складу злочину проти конституційних прав та свобод;

5) коли здійснюється розповсюдження або збут комп'ютерної інформації, зміст якої складають відомості з обмеженим доступом інших видів.

Для того, щоб не перевантажувати запропоновану схему, "за дужки" ми винесли такі ознаки комп'ютерної інформації, предмету злочину, передбаченого ст. 361-2 КК, як "зібрана та захищена відповідно до чинного законодавства". Однак видається, що і без цього запропонований перелік випадків, коли можливим є застосування ст. 361-2 КК, достатньо наочно демонструє очевидну надлишковість кримінально-правової заборони, передбаченої досліджуваною нормою. Дійсно, крім випадків шпигунства, не можна погодитись з тим, що слід вважати злочином розповсюдження відомостей, які складають певну таємницю, вчинене особою, якій вони не були довірені. Ситуація з відповідальністю за порушення лікарської, комерційної або банківської таємниці є ще більш наочнішою. Чи обґрунтовано вважати певні дії злочином, коли наслідки, що зумовлюють кримінальну відповідальність за них, не настали? Єдиним аргументом, який може бути використаний для обґрунтування доцільності такої відповідальності, можна вважати лише те, що кримінальна відповідальність продиктована формою цих відомостей, тим, що вони є комп'ютерною інформацією. Однак, крім того, що він спірний, цього аргументу явно недостатньо для обґрунтування кримінальної відповідальності за подібні дії. Форма інформації ні в якому разі не може обґрунтовувати підвищену суспільну небезпечність її розповсюдження або збуту.

Проте відкритим залишається питання кримінально-правової охорони інших видів інформації з обмеженим доступом. Можна сказати, що це єдина позитивна риса наявності у Кримінальному кодексі такої норми, як ст. 361-2. Вона дійсно забезпечує певну охорону суспільних відносин власності на комп'ютерну інформацію з обмеженим доступом. Однак указівка на те, що предметом цього злочину є комп'ютерна інформація з обмеженим доступом, яка *захищена* відповідно чинного законодавства, унеможливлює ефективне використання норми. Наявність такої ознаки предмету означає, що злочин, передбачений ст. 361-2 КК, буде мати місце лише тоді коли незаконно розповсюджується або збувається інформація, що обробляється із застосуванням певної системи захисту. Таким чином,

проблематичним буде застосування даної норми для кваліфікації тих випадків, коли особа збуває або розповсюджує інформацію з обмеженим доступом, яку, наприклад, було отримано з захищеної комп'ютерної мережі шляхом подолання системи захисту, тобто на момент розповсюдження інформація з обмеженим доступом уже не захищалася спеціальними технічними засобами. Зауважимо, що подібні випадки траплялися, вони стосувалися незаконного розповсюдження такого виду комп'ютерної інформації з обмеженим доступом, як електронні бази персональних даних. Наприклад, у 2003 році в продажу з'явилися бази даних російських операторів мобільного зв'язку "Мобільні ТелеСистеми" та "Бі лайн". Крім прізвищ абонентів вони містили паспортні дані, адресу місця проживання, індивідуальний номер платника податків та іншу інформацію. Зазначимо також, що ринок персональних даних – це сегмент комп'ютерної злочинності, який швидко розвивається, деякі фахівці оцінюють його в 3 мільярди доларів США на рік [0]. Але, нажаль, відзначені недоліки статті 361-2 КК унеможливлюють її застосування для протидії новому виду комп'ютерної злочинності, який швидко розвивається. Для того, щоб бути об'єктивними необхідно зазначити, що персональні дані певною мірою захищені кримінальним законодавством: ст. 182 КК України передбачає відповідальність за порушення недоторканності приватного життя, однак використання цієї норми для протидії незаконним операціям з електронними базами персональних даних видається не зовсім ефективним. Ця стаття забезпечує фрагментарний захист суспільних відносин від аналізованого посягання, адже безпосереднім об'єктом незаконних дій з електронними базами персональних даних є право власності осіб (юридичних або фізичних), які на законних підставах придбали або створили ці бази, а конституційне право на недоторканність приватного життя виступає, як видається, лише додатковим факультативним об'єктом таких діянь.

Наведених вище аргументів достатньо для того, щоб зробити висновок про виключення ст. 361-2 з Кримінального кодексу. Однак це не означає, що необхідно декриміналізовувати збут або розповсюдження відомостей з обмеженим доступом. Дана проблема, як видається, не відноситься до злочинів в сфері використання інформаційних технологій. Вище ми зазначали, що форма представлення інформації не є визначальним чинником суспільної небезпечності її збуту або розповсюдження. Отже логічним буде повернення до цього питання у контексті дослідження кримінально-правових засобів охорони суспільних відносин щодо забезпечення доступу до інформації.

Певні прогалини в кримінально-правовій охороні суспільних відносини зумовлені вадами *конструкції об'єктивної сторони* складу злочину, передбаченого ст. 361 КК України. Як уже зазначалося, даний склад злочину є матеріальним, його об'єктивна сторона складається з діяння (несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних

мереж чи мереж електрозв'язку), суспільно небезпечних наслідків (витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації та порушення порядку її маршрутизації) та причинного зв'язку між діянням і наслідками. Отже, відповідно до чинного законодавства настання вказаних наслідків не буде визнаватися злочином, якщо їм не передувало несанкціоноване втручання в роботу засобів опрацювання інформації. Наприклад, під час коли електронно-обчислювальна машина не була ввімкнена, тобто принципово неможливим було втручання в її роботу, на жорсткий диск здійснено вплив потужним електромагнітним випромінюванням, наслідком чого виявилася втрата інформації, що знаходилася на ньому. Використання ст. 361 КК для кваліфікації даного випадку виключається, оскільки не було несанкціонованого втручання в роботу ЕОМ. Зазначимо також, що фізичне знищення або пошкодження носія, який був відокремлений від ЕОМ, АС або комп'ютерної мережі, з метою знищення інформації, яка на ньому знаходиться, знову ж таки з цієї самої причини неможливо кваліфікувати за даною статтею. В останньому випадку можна говорити лише про умисне знищення чужого майна, але використання ст. 194 КК допускається лише тоді, коли в результаті знищення було заподіяно шкоду у великих розмірах. Крім того, така кваліфікація не відповідала б об'єкту посягання: шкоду заподіяно інформаційним відносинам, а діяння кваліфікується як посягання на відносини власності на річ. Без несанкціонованого втручання в роботу ЕОМ, автоматизованих систем або комп'ютерних мереж можливим є й ознайомлення з інформацією, яка в них обробляється. Наприклад, за допомогою спеціального обладнання можливо, знаходячись на певній відстані від ЕОМ, отримувати відеосигнал, який подається на монітор та ознайомлюватися з інформацією, яка відображається на ньому. Блокувати комп'ютерну інформацію також можливо без несанкціонованого втручання в роботу засобу її оброблення. Отже, вада конструкції об'єктивної сторони складу несанкціонованого втручання (ст. 361 КК) полягає в тому, що вона не враховує можливість заподіяння вказаних у нормі суспільно небезпечних наслідків без вчинення передбаченого в нормі діяння. Крім того, відсутність несанкціонованого втручання (діяння) не означає, що настання даних наслідків втрачає суспільну небезпечність. Як уже неодноразово відзначалося, головним чинником суспільної небезпечності комп'ютерного злочину є значущість інформації.

Таким чином, формулювання ознак злочинів в сфері використання інформаційних технологій, яке містить вказівку на діяння у вигляді несанкціонованого втручання в роботу комп'ютерної техніки є недоцільним.

Певні прогалини чинного кримінального законодавства пов'язані також з законодавчим визначенням *суб'єкта злочину, передбаченого ст. 363 КК*. Таким суб'єктом є особа, яка відповідає *за експлуатацію* електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж

або мереж електрозв'язку. Це визначення перебуває у явній невідповідності з формами об'єктивної сторони цього злочину. Яка може виявлятися у порушенні *порядку захисту* інформації, *правил захисту* інформації або *правил експлуатації* комп'ютерної техніки. Слід погодитися з зауваженням Д.С. Азарова про те, що "не може вважатися злочином порушення правил (порядку) захисту інформації, вчинене особою, яка за забезпечення цього захисту відповідає, а за дотримання правил експлуатації техніки – ні"[0, с. 78]. Тобто формулювання ознак спеціального суб'єкта злочину, передбаченого ст. 363 КК, значно звужує можливості використання цієї норми, створює певні прогалини у кримінально-правовій охороні суспільних відносин від злочинних посягань в сфері використання інформаційних технологій. Ці прогалини пов'язані з кваліфікацією злочинних дій осіб, які відповідають тільки за дотримання порядку або правил захисту комп'ютерної інформації.

Наступна прогалина кримінально-правової охорони суспільних відносин в сфері забезпечення дотримання вимог експлуатації комп'ютерної техніки, порядку та правил захисту інформації, пов'язана з невідповідністю норм конструктивних галузей права потребам захисту суспільних відносин в сфері використання інформаційних технологій. Як зазначалося вище, на сьогодні спеціальні вимоги встановлюються лише щодо захисту державної інформації або інформації, захист якої спеціально передбачено в законі. Відповідно і ст. 363 КК виступає елементом саме цього правового механізму інформаційної безпеки. Її наявність дозволяє притягати до кримінальної відповідальності осіб, які порушують вимоги захисту інформації, але головним чином сприяє, як видається, підвищенню ефективності попередження комп'ютерних злочинів у державному секторі. Стимулюючи відповідальних осіб застосовувати заходи захисту інформації, дана норма забезпечує в решті решт значне зниження вірогідності посягання на державний інформаційний ресурс. Однак статистичні дані свідчать про певну невиправданість такого підходу. Це перш за все дані Українського Антивірусного Центру: 1) у першому півріччі 2004 року втрати від вірусних атак в Україні склали 290 мільйонів гривень; 2) найбільші збитки в розрахунку на один ПК спостерігаються в середньому бізнесі, де витрати на технічний захист інформації мінімальні; 3) значно збільшилася кількість вірусних інцидентів, пов'язаних з домашніми користувачами, основна причина масового поширення вірусів у цьому сегменті – практично повна відсутність антивірусних засобів; 4) збитки від вірусних атак в Україні у першій половині 2004 року зросли на 30% порівняно з аналогічним періодом 2003 року [0]. Отже, можна сміливо стверджувати, що відсутність спеціального нормативного регулювання у сфері захисту недержавної інформації призводить до недостатності заходів щодо захисту такої інформації, які мають здійснюватися її власниками, та, певною мірою, потенційно небезпечна зростанням показників

комп'ютерної злочинності. Недостатність заходів захисту недержавного інформаційного ресурсу є одним з віктимологічних факторів комп'ютерної злочинності. При цьому можливості використання ст. 363 КК для стимулювання застосування засобів інформаційної безпеки в цьому сегменті інформаційних відносин значно обмежені через відсутність норм, які б зобов'язували їх використовувати.

Цілком зрозуміло, що ефективним захист інформації буде за умови комплексного використання технічних, програмних та організаційних засобів. Очевидно також і те, що ставити власникам недержавної інформації вимоги, подібні до тих, які передбачаються наведеними нормативними документами, недоцільно, крім того, це навряд чи сприятиме розвиткові відносин інформатизації в країні. Однак проблема законодавчого стимулювання більш широкого використання засобів захисту недержавної інформації є наявною та потребує якнайшвидшого розв'язання. Таким чином, ще одним напрямком вдосконалення національного законодавства є створення нормативної бази для розвитку системи захисту недержавної інформації, яка б відповідала можливостям її власників і забезпечувала достатньо надійний захист відповідного сегменту національного інформаційного ресурсу. Це сприятиме попередженню комп'ютерної злочинності та забезпечить більш широкі можливості реалізації конституційного права на інформацію.

Отже, чинний механізм кримінально-правової охорони відносин в сфері використання інформаційних технологій містить прогалини, зумовлені як недосконалістю диспозиції ст. 363 так і недоліками законодавчого регулювання використання засобів захисту інформації. Мабуть найбільш серйозним аргументом на підтвердження цього висновку є вкрай незначна практика використання ст. 363, яка вступає у очевидну конфронтацію з кримінологічними характеристиками цих посягань. Фахівці з інформаційної безпеки подавляючу більшість комп'ютерних злочинів пов'язують саме з діяльністю спеціальних суб'єктів, осіб які мають певні повноваження щодо інформації, яка виступає предметом посягання. Чинне законодавство містить дві норми, про відповідальність таких осіб – статті 362 та 363 КК. Однак, серед осіб, засуджених у 2008 році, лише 12,3% були засуджені за ст. 362, а за ст. 363 взагалі не було засуджено жодної особи [0]. Тобто практика застосування національного законодавства явно не відповідає експертним оцінкам щодо структури комп'ютерної злочинності. При цьому дана невідповідність знаходиться далеко за межами статистичної похибки, мова йде про подавляючу більшість в оцінках експертів та меншість у статистичних показниках. Зрозуміло, що це зумовлюється не тільки вадами чинного законодавства, хоча останні є достатньо вагомим чинником ситуації, що склалася.

Враховуючи означені недоліки ст. 363 КК, суб'єктом порушення правил експлуатації комп'ютерних систем, порядку чи правил захисту

комп'ютерних даних пропонується визнавати особу, яка відповідає за дотримання вимог інформаційної безпеки. Зауважимо, що термін "інформаційна безпека" ми вживаємо в цій нормі у вузькому значенні, розуміючи під нею сукупність вимог щодо забезпечення працездатності комп'ютерної техніки та іншого телекомунікаційного обладнання, організації та здійснення програмного, технічного й організаційного захисту комп'ютерних даних. Ще раз зазначимо, що для забезпечення ефективного використання даної норми необхідним є також доповнення законодавства положеннями про обов'язок використання засобів захисту інформації у недержавному секторі.

Окремою проблемою протидії суспільно небезпечним посяганням у сфері використання комп'ютерної техніки в контексті дотримання принципу відсутності прогалин є *питання відповідальності за розповсюдження спаму* (SPAM, sending of predatory and abusive e-mail). "Спам" представляє собою множинні повідомлення електронної пошти рекламного або порнографічного характеру, а також повідомлення іншого змісту, що використовуються, як правило, для введення в оману з метою подальшого вчинення шахрайства. До істотних ознак спаму також відносять те, що подібні листи отримувач або не замовляв, або не може відмовитися від їх отримання у подальшому.

Отже, розповсюдження спаму, як правило, полягає в надсиланні великій кількості адресатів повідомлень, які вони не замовляли. Суспільна небезпечність такого діяння має певну специфіку. З точки зору конкретного користувача матеріальні збитки від розповсюдження спаму незначні, вони, врешті-решт, зводяться до оплати Інтернет-послуг, пов'язаних з отриманням зайвої кореспонденції. Однак з точки зору провайдерів, організацій, що надають послуги доступу до Інтернету, спам є досить небезпечним явищем, оскільки його наявність створює зайве, некорисне навантаження обладнання й ускладнює роботу інформаційної системи. Ще одним показником суспільної небезпечності спаму є втрати робочого часу працівників підприємств, установ та організацій, які використовують Інтернет у своїй роботі. Зазначимо, що за даними компанії "Ашманов і Партнери", яка є провідним виробником антиспамерського програмного забезпечення в Росії, обсяг спаму в російському поштовому Інтернет-трафіку у 2004 році склав 75-80%, а збитки від його розповсюдження – мінімум 250 мільйонів євро [0]. За даними наукового підрозділу компанії Websense Inc., у серпні 2010 року серед всього обсягу електронної кореспонденції спам склав 82,2 %, в абсолютних цифрах 3,62 мільярдів(!) листів [0]. І хоча доля національного сегменту в цьому інформаційному потоці невелика, але з великою вірогідністю можна прогнозувати, що подібні проблеми очікують українських користувачів мережі Інтернет і провайдерів у найближчому майбутньому. Чи готове українське законодавство до цього?

На жаль, на це питання неможливо відповісти позитивно. Стаття 363-1 КК України передбачає відповідальність за масове розповсюдження повідомлень електрозв'язку, однак кримінальна відповідальність, у разі вчинення таких дій, настає тільки тоді, коли спричинено наслідки у вигляді порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Як уже зазначалося, розповсюдження спаму, як правило, не призводить до таких наслідків. Ситуація, коли в результаті масового розповсюдження повідомлень електрозв'язку настають зазначені наслідки, є винятковою. Порушення або припинення роботи засобів опрацювання інформації слід віднести до абсолютно нетипових наслідків розповсюдження спаму. Отже, маємо констатувати, що інформаційні суспільні відносини через недосконалість статті 363-1 КК України практично не захищені від посягань, пов'язаних із розповсюдженням спаму. "Звичайне" розповсюдження спаму не можна кваліфікувати за даною нормою, оскільки воно не призводить до наслідків, зазначених в статті 363-1 КК. Тому, до недоліків чинного кримінального законодавства слід віднести і його недостатню ефективність в протидії такій майбутній інформаційній загрозі як спам.

Наведений висновок підтверджується також співставленням показників судової статистики та фактичних даних щодо діяльності українських спамерів. Так, згідно з інформацією Державної судової адміністрації, у 2007-2008 рр. суди не розглядали кримінальних справ про злочини, передбачені ст. 363-1 КК [0]. У подальшому ситуація докорінно не змінилася. В той же час, за даними міжнародної громадської організації The Spamhaus Project, серед 10 найнебезпечніших спамерів світу налічується 3 особи, діяльність яких пов'язують з Україною [0]. Крім цього, відповідно до висновків, зроблених експертами цієї організації, близько 80% світового спаму слід пов'язувати з однією сотнею встановлених спамерів, дані про них об'єднані в спеціалізованій базі даних The Register of Known Spam Operations (ROKSO). Українців в цій сотні четверо. Інакше кажучи, існує чотири особи або груп осіб, які здійснюють масові розсилки з території України в світовому масштабі [0]. Тобто Україна і українці є вельми помітними учасниками процесів, пов'язаних з розповсюдженням спаму, але ця тенденція не знаходить відображення в практиці українських судів.

Таким чином, стосовно дотримання принципу ***відсутності прогалин та ненадлишковості заборони*** при криміналізації злочинів в сфері використання комп'ютерної техніки та мереж електрозв'язку маємо зазначити, наступне:

1. Чинна редакція ст. 361-2 дозволяє говорити як про надлишковість заборони, яка у ній сформульована, так і про формування цією нормою певних прогалин у законодавстві. Надлишковість стосується криміналіза-

ції діянь, які не можна визнавати суспільно небезпечними в контексті інших норм щодо відповідальності за незаконні дії з інформацією з обмеженим доступом. Прогалини пов'язані з невдалим формулюванням ознак предмета, які значно звужують можливості норми, роблять кримінально-правові засоби, передбачені нею, такими, що не відповідають сучасним потребам протидії злочинам в сфері використання інформаційних технологій.

2. Конструкція об'єктивної сторони ст. 361 КК України зумовлює прогалини, що полягають у неможливості притягнення до кримінальної відповідальності осіб, що заподіють вказані у нормі суспільно небезпечні наслідки без вчинення передбаченого в нормі діяння.

3. Певні прогалини створює законодавче визначення суб'єкта злочину, передбаченого ст. 363 КК, яке не відповідає можливим формам об'єктивної сторони даного посягання, крім цього неефективність даної норми зумовлена недоліками законодавчого регулювання використання засобів захисту інформації

4. Прогалини мають місце при формулюванні кримінально-правової заборони масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК). Вони полягають у тому, що відповідальність за розповсюдження спаму пов'язана з наслідками, які є абсолютно нетиповими для подібних дій, відповідно подавляюча більшість випадків розповсюдження спаму не підпадає під ознаки злочину, передбаченого цією нормою.

Використана література:

1. Monthly Websense Email Security Threat Brief "In The Mail", August 2010, Volume 3, Issue 8 // Режим доступу: http://securitylabs.websense.com/content/Assets/report-in-the-mail-aug-10-en.pdf

2. The Register of Known Spam Operations (ROKSO) database // Офіційний сайт міжнародної громадської організації The Spamhaus Project. Режим доступу: http://www.spamhaus.org/statistics/spammers.lasso

3. The World's Worst Spammers // Офіційний сайт міжнарної громадської організації The Spamhaus Project. Режим доступу: http://www.spamhaus.org /statistics/spammers.lasso

4. Ашманов И., Власова А., Тутубалин А. Спам 2004: подробный аналитический отчет. – http://www.cyber-crimes.ru/statistic/Spam-2004_detail.html

5. Гриців М.І., Антощук В.В. Узагальнення судової практики розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку // Електронний ресурс. Офіційний сайт Верховного Суду України. Режим доступу: http://www.scourt.gov.ua/

6. Законодавство про кримінальну відповідальність за "комп'ютерні" злочини: науково-практичний коментар і шляхи вдосконалення / А.А. Музика, Д.С. Азаров. – К.: Вид. Паливода А.В., 2005.

7. Сайтарлы Т. Право граждан на неприкосновенность частной жизни не имеет достаточного правового обеспечения // Новости сайта Центра исследования компьютерной преступности. – 21.01.2005. – Режим доступа: // http://www.crime-research.ru/news/21.01.2005/1772

8. Украина: потери от вирусных атак в первом полугодии 2004 г. составили около 45 млн. евро. // Новости сайта Центра исследования компьютерной преступности. – 30.07.2004. – Режим доступа: http://www.crime-research.ru/news/30.07.2004/1320.

УДК 343.131

Л.В. Карабут

ФУНКЦІОНАЛЬНЕ ПРИЗНАЧЕННЯ КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНОЇ ДІЯЛЬНОСТІ

Дано визначення і здійснено аналіз функціонального призначення кримінально-процесуальної діяльності. Обґрунтовано перелік функцій, що їх кримінально-процесуальна діяльність виконує у суспільстві.

Ключові слова: *кримінально-процесуальна діяльність; функціональне призначення; цілі; функції.*

Дано определение и осуществлен анализ функционального назначения уголовно-процессуальной деятельности. Обоснован перечень функций, осуществляемых уголовно-процессуальной деятельностью в обществе.

Ключевые слова: *уголовно-процессуальная деятельность; функциональное назначение; цели; функции.*

There were made the determination and the analysis of the functional setting of criminal-judicial activity. There numbers of functions that is carries out by the criminal-judicial activity in society are grounded.

Key words: *criminal- judicial activity; functional setting; aims; functions.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Реформування кримінально-процесуального законодавства, яке то активізується, то знову затихає, не може бути ефективним без з'ясування у рамках юридичної теорії питання про те, яким є функціональне призначення кримінально-процесуальної діяльності. Ігнорування даного питання у теорії кримінального процесу може призвести до ухвалення неякісного кримінально-процесуального закону в цілому, або окремих його частин. З'ясування питання про функціональне призначення кримінально-процесуальної діяльності як одного із різновидів державної діяльності є чинником, що може посприяти забезпеченню стабільності прийнятих законів та ефективності їхнього застосування. Дослідження даного питання здатне посприяти започаткуванню у вітчизняній теорії кримінального процесу