

14. Яремко Г. З. *Бланкетні диспозиції в статтях Особливої частини Кримінального кодексу України: дис. ... кандидата юрид. наук : 12.00.08 / Яремко Галина Зіновівна.* - Львів, 2010—408 с.
15. Гуцина Н. А. *Системные связи в праве / Н. А. Гуцина // Право и политика -2005.-№5. -С. 10-14.*
16. Яремко Г. З. *К'янкетні диспозиції в статтях Особливої частини Кримінального кодексу України : [монографія] / Яремко Г. З. ; за ред. В. О. Іавроцького. - Львів : Львівський державний університет внутрішніх справ, 2011. - 432 с.*

Болдарь Г.С. Міжгалузеві зв'язки кримінального права: поняття та класифікація

У статті розглянуті найбільш типові форми міжгалузевих зв'язків у нормах Загальної та Особливої частин КК України. Розкрито їх поняття, види, та основні ознаки.

Ключові слова: міжгалузеві зв'язки, система права, форми міжгалузевої взаємодії, бланкетна диспозиція.

Болдарт Г.С. Межотраслевые связи уголовного права: понятие и классификация

В статье рассмотрены наиболее типичные формы межотраслевых связей в нормах Общей и Особенной частей УК Украины. Раскрыто их понятие, виды и основные признаки.

Ключевые слова: межотраслевые связи, система права, формы межотраслевого взаимодействия, бланкетная диспозиция.

Boldar G. Y. The inter-branch connections in criminal law: the notion and classification

In the article legal analysis of the most typical forms of the inter-branch connection in the norms of the General and Special parts of the Criminal Code of Ukraine is carried out. Then notion, types and principal signs.

Key words: inter-branch connections, system of law, forms of inter-branch reciprocity, blanket disposition.

САВІНОВА Н.А.

КІБЕРЗЛОЧИННІСТЬ: ВИТОКИ ТА ТЕНДЕНЦІЇ ДЕТЕРМІНАЦІЇ В УМОВАХ РОЗВИТКУ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

УДК 343.79

Якщо ще десять років тому у нашій державі єдиний склад злочину, що передбачав кримінальну відповідальність за втручання в роботу КОМ. систем та комп'ютерних мереж та розповсюдження комп'ютерного вірусу переважно викликали здивовані посмішки, а кілька освічених спеціалістів в області протидії хакерським посяганням намагалася протистояти кібератакам на банки, сьогодні повною мірою зрозуміло, що то був лише повільний початок такої, що ескалує, навали кібернетичної злочинності, що набирає шалених обертів пропорційно динаміці інформаційного суспільства.

Навіть на первинних стадіях кібернетичні злочини мали світове значення, і, як свідчить історія кіберзлочинності. Їх різноманітність стартувала від трансформації від загально кримінальної злочинності під впливом розвитку технологій.

Перші повідомлення про факти вчинення злочинів вчинених за допомогою ІКТ з'явилися у 70-х роках ХХ сторіччя. Вони мали ознаки традиційних розкрадань, але вчинених з використанням нової технології. Так, група студентів з метою безкоштовного телефонування, розпочала масове зламування місцевих і міжнародних телефонних ліній АТ&Т (США) з використанням т.з., «ВіеВох» („Блакитної коробки“), яка була сконструйована ветераном В'єтнамської війни Дж.Дрейпером. Секрет її виготовлення був необачно широко опублікований у ЗМІ, що призвело в подальшому до навали телефонних шахрайств.

80-ті роки ХХ сторіччя характеризувалися не лише сплеском хаотичних атак на комп'ютерні системи з метою розкрадань різного роду, а й популяризацією таких: у західній пресі набули особливої популярності "форуми" - стенди оголошень у пресі, велика кількість з яких була присвячена передачі знань та навичок щодо використання ІКТ для вчинення таких злочинів: шахрайства у телефонних мережах, підбору кодів для кредитних карток, звичайного хакінгу, які давали можливість розкратити та привласнювати гроші, належні іншим особам. Зокрема, з цього етапу починається культивування терміну "хакер" від (hacker (англ.) такий, що ламає).

"Хакерами" спершу називали себе члени групи студентів-практикантів Массачусетського технологічного університету (Бостон, США), які займалися модернізацією моделей залізниць та електропотягів та застосовували нові схеми перемикання колій. Інтерес окремих членів цієї групи був направлений на аналогічні маніпуляції з комп'ютерними програмами університетського комп'ютеру, за допомогою яких здійснювалося управління моделями локомотивів, а також - управління програмами моделювання залізничних шляхопроводів[1].

Термін „хакер" у первинному розумінні 70-х років ХХ сторіччя, насамперед, визначав індивідуума, який випробовує програмні та комунікаційні можливості комп'ютера [2]. Позитивне розуміння хакерства збереглося у професійному використанні фахівців з ІКТ. У загальному ж розумінні, термін "хакер" набув переважно негативного значення, яке пізніше набуло кримінологічного змісту, і під хакерами у правовій літературі стали розуміти осіб, які вчинюють злочини через комп'ютерні системи, використовуючи ІКТ [3, с. 786: 4, с. 104]. В цілому позитивне поняття набуло негативного значення з кількістю протиправних дій у віртуальному просторі[5. с. 570].

90-ті роки ХХ сторіччя характеризувалися трансформацією у кіберзлочини та «вдосконаленням» звичайних за змістом шахрайств та розкрадань. Гак, у серпні 1994 р. у США був затриманий Дж.Т.Пітерсон (AgentSteal) [6], який у 1993 р. спільно К.Паулсеном (DarkDante), блокували телефонну мережу конкурсу, внаслідок чого до ефіру доходили лише їх телефонні дзвінки, тому два призові автомобілі „Порше", турпоїздки і 20 000 доларів дісталися їм. Дж.Т.Пітерсон був затриманий ФБР за злам баз даних і проникнення у телефонну мережу та викрадення у фінансової корпорації HellenFinencia 150 тисяч доларів США, за що був засуджений у 1995 р.[7]. У 1995 р. у Великобританії був заарештований і притягнутий до кримінальної відповідальності за злам мережі Citibank і викрадення 10 мільйонів доларів США громадянин РФ В. Левін. [8]

Сучасні кіберзлочини-трансформери стають дедалі складнішими і більш «витонченими» через постійне ускладнення процедур атак. Так, у 2007 р. один з найкрупніших банків Швейцарії Nordea став жертвою російських хакерів [9], які викрали більше мільярда євро достатньо новим у порівнянні з іншими подібними злочинами способом: у якості "посередників" злочинцями були використані клієнти банку, на комп'ютери яких був завантажений комп'ютерний вірус Backdoor.Win32.Harddoor [10] типу "троянський кінь" [11]. Завантажений злочинцями комп'ютерний вірус через систему Інтернет-банкінгу [12, с. 133] потрапив до комп'ютерної системи банку Nordea, де зруйнував систему захисту персональних даних, внаслідок чого злочинці отримали доступ до пін-кодів та управління рахунками. А 600000 доларів СІЛА були викрадені українським хакером М.Ястремським спільно з громадянами Естонії та США також з використанням "посередника" — комп'ютерної системи мережі ресторанів "Busters" (США), зламавши яку злочинці отримали персональні дані клієнтів ресторану, необхідні і достатні для привласнення злочинцями грошей клієнтів з банківських рахунків [13].

За повідомленнями BraunResearchInc, станом на 2006 р., майже 60 % американських компаній були впевнені у тому, що кіберзлочинність завдає їм більшу шкоду, ніж звичайна злочинність [14]. За даними ФБР США щодо статистики скарг, які поступали протягом 2006 р. до Центру дослідження комп'ютерної злочинності у мережі Internet у складі ФБР США від громадян, які постраждали від дій хакерів, поступило 200 тисяч заяв, а збитки, яких зазнали громадяни США від дій шахрайства у Internet склали майже 200 мільйонів доларів [15, с. 69]. а британці бояться кібернетичних злочинців більше, ніж звичайних грабіжників [16].

При цьому у більшості постраждалих від кіберзлочинців відсутнє бажання своєчасно повідомляти про факти кіберзлочинів правоохоронним органам, така тенденція характерна як для країн, що розвиваються, так і для розвинутих країн: у США лише 20% компаній повідомляють поліції про кіберзлочини [17]. Така тенденція спостерігалася і раніше, про що ще у 2001 р. вказували В.О.Голубев та його колеги-співавтори, досліджуючи ступінь латентності кібернетичних злочинців через фактичну відсутність належної реакції з боку постраждалих від них. Так, аналізуючи реакцію на такі кіберзлочини з боку постраждалих суб'єктів господарювання, якими на той час, як і зараз, були, переважно банки, вони зазначали: «через небажання підриву репутації потерпіла сторона неохоче повідомляє правоохоронним органам про факти і вчинення злочинів, якщо робить це взагалі» [18, с. 83].

Від кіберзлочинності зазнають інформаційні агенції всього світу, які постійно відчувають інформаційні втручання [19; 20; 21]. Яскравим прикладом таких дій може слугувати втручання у роботу дитячого телеканалу DisneyChannel у США у 2007 р., на якому, за повідомленнями News.uaclub.net, у ранковий час, коли канал переглядали діти, хакерами була "продемонстрована" порнографія. [22]

Кіберзлочини характеризуються здебільшого індивідуальною спрямованістю, за виключенням випадків використання ретельної (мережевої) комунікації [23, с. 86], направленої на невизначену кількість реципієнтів.

До кібернетичних злочинів Конвенція про кіберзлочинність [24] та Додатковий протокол до неї [25] відносять лише низку суспільно-небезпечних діянь, які безпосередньо посягають комп'ютерні системи та комп'ютерну інформацію, а також злочини, які посягають на інші предмети, проте можуть бути вчинені з використанням комп'ютерних систем. Така уніфікація, очевидно, була викликана потребою термінового реагування на виклики кібернетичної злочинності. Недоцільно тоді було здійснювати і аналіз та співставлення безпосередніх об'єктів таких посягань.

Натомість, сьогодні вже вбачається, що об'єктами посягань більшості злочинів, що вчинюються з використанням комп'ютерних систем та інших ІКТ є не комп'ютерні системи та комп'ютерна інформація, а ті суспільні відносини, які такими системами та комунікацією забезпечуються: державна (зокрема, інформаційна) безпека, відносини у сфері державної, банківської, комерційної таємниці та персональних даних, виборчих прав, моральності та низки інших родових (з точки зору теорії вітчизняного кримінального права) об'єктів.

У той же час, саме злочини, спрямовані на комп'ютерні системи, стають ніби «посередниками» при вчиненні «кінцевих» суспільно-небезпечних діянь - викрадень, дискредитації органів влади, втручання в діяльність ЗМІ тощо.

Підсумовуючи наведене вище, з урахуванням дослідженої генези кіберзлочинності, очевидно, що *кібернетичні злочини це суспільно-небезпечні діяння, які трансформувалися зі звичайних злочинів під впливом виникнення і розвитку ІТ, зокрема - ІКТ, і посягають на комунікації та інші суспільні відносини, які здійснюються при посередництві комунікацій. При цьому вони спрямовуються насамперед на комп'ютерні системи (у т.ч. телекомунікаційні) і завдають їм шкоди, або завдають шкоди даним в таких системах, або змісту чи власнику таких даних.*

Сучасні кібернетичні злочини спрямовуються, як вже вказувалося, фактично на всі сфери діяльності, у яких беруть участь комунікаційні системи, тобто — на всі основні сфери життєдіяльності людини. Такі трансформовані злочини вже навряд чи доцільно вважати кібернетичними - адже в такому випадку у недалекому часі всі злочини, що описані в законі про кримінальну відповідальність (за виключенням убивств та тяжких тілесних ушкоджень) можна буде віднести до «кіберзлочинів», через можливість їх вчинення з використанням віддалених комунікацій...

Кібернетичні злочини слід відрізняти від інших злочинів, що трансформувалися під впливом ІКТ у інформаційному суспільстві, які першочергово спрямовані на завдання шкоди іншим об'єктам без ознак активного впливу на комп'ютерні системи. Це, наприклад, поширення порнографії, шахрайства, погрози, створення злочинних організацій або незаконних воєнізованих формувань, тощо вчинені з використанням мереж та телекомунікаційних систем.

1. Балда Т. Коротка історія хакерства // http://www.universum.org.ua/sp/2002/haker_3.html
2. Хакеры как профессионалы и кракеры как вид [Електронний ресурс]/ FreeTimeClub / режим доступу до ресурсу: <http://www.freetime.com.ua/972>
3. Науково-практичний коментар до Кримінального кодексу України: За станом законодавства і Постановою Пленуму Верховного суду України на 1 грудня 2001 р. /За ред. С.С.Яценка. - К: А.С.К., 2002.
4. Голубев В. Кримінологічна характеристика злочинів в сфері використання комп'ютерних технологій // Підприємництво, господарство і право. - 2002. - № 11.
5. Гаврилов М.И. Информатика и информационные технологии: учебник для студентов вузов / М.И. Гаврилов. —м.: Гардарики, 2007. — 655 с. с: ил.
6. История „кибертеррориста № 1“. Computer Crime Research Center // <http://www.crime-research.org/Burgl.html>
7. Сетевые террористы. 10 самых опасных хакеров планеты / корреспондент. - 2007. - № 15 (254). - С. 68-69.
8. Владимир Левин [Електронний ресурс] /Люди.Ru. / Режим доступу до ресурсу: <http://www.peoples.ru/state/criminal/computer/liviv/>
9. Российские хакеры ограбили Швейцарский банк на 1.000.000 евро.[Електронний ресурс] / SecurityLabbyPositiveTechnologies / Режим доступу до ресурсу :<http://www.securitylab.ru/news/288287.php>
10. Лабораторія Касперського. Ваксаоог.іVin32.Нагаоог// SecurityLab by Positive Technologies // <http://www.securitylab.ru/virus/212405.php>
11. Термінологічний довідник з питань технічного захисту інформації / Коженеуський Р.С., Кузнецов Г.В., Хорошко В.О., Чернов Д.В. / За ред. проф. В.О. Хорошка. - К.: ДУІКТ, 2007.
12. Брижко В.М., Цимбалюк В.С., Орехов А.А., Кальченко О.Н.. е-будущее и информационное право / Под редакцией доктора наук, профессора Р.А. Калюжного, доктора экономических наук, профессора М.Я Швеца. — К. : «Интеграл», 2002.
13. Украинский хакер взломал американский ресторан на 600 тысяч долларов [Електронний ресурс] / Комсомольская правда Украины от 14.05.2008 // Режим доступу до ресурсу: <http://kr.ua/daily/140508/411773>
14. Киберпреступность крепнет [Електронний ресурс] / Режим доступу до ресурсу :СЮWorld'/<http://www.cjoworld.ru/analytics/258907/>
15. Трибушная Е. Зомбированная сеть // Корреспондент. — 2007. - № 15(254). -С. 69.
16. Британцы боятся онлайн-преступников больше, чем обычных грабителей / [Електронний ресурс]/ Viruslist.com Интернет-безопасность / Режим доступу до ресурсу: <http://www.viruslist.com/ru/news?id^201571768>
17. Американские компании укрывают кибератаки [Електронний ресурс] / Reuters / Режим доступу до ресурсу: <http://www.reuters.com/newsArticle/jhtml?type=internetNews&storyID=7666955> "target^ "blank"
18. Голубев О.В., Говловський В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинністю у сфері використання комп'ютерних тех-

нологій / За заг. ред. д-ра, професора Р.А. Калюжного. - Запоріжжя: Про-
світа, 2001.

19. *Защита информации [Электронный ресурс] / Режим доступа до ресурсу: <http://informationsecurity.ru/keywords.php?keyword...>*
20. *Китайские хакеры перенесли дату атаки на сайт CNN [Электронный ресурс] / Защита информации, ' Режим доступа до ресурсу: <http://informationsecurity.ru/keywords.php?keyword...>*
21. *Азербайджанский хакер взломал пять армянских сайтов [Электронный ресурс] // Day.Az // Режим доступа до ресурсу: <http://www.day.az/news/hitech/68996.html>*
22. *Американским детям показали порнографию на КаньеDisney [Электронный ресурс] / Центр Исследования компьютерной преступности // Режим доступа до ресурсу: <http://www.crime-research.ru/news/04.05.2007/3444/>*
23. *Корнев М.Н., Коваленко А.Б. Социальная психология: учебник. — К., 1995.*
24. *Конвенция Рады Европы Про киберзлочинність від 23.11.2001 [Электронный ресурс] / Официальный сайт Верховной Рады Украины / Режим доступа до ресурсу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_575*
25. *Додатковий протокол до Конвенції про киберзлочинність, який стосується дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 [Электронный ресурс] / Официальный сайт Верховной Рады Украины / Режим доступа до ресурсу: http://zakon1.rada.gov.ua/laws/show/994_687*

Савинова Н. А. Киберзлочинність: витоки та тенденції детермінації в умовах розвитку Глобального інформаційного суспільства

Стаття присвячена проблемі детермінації киберзлочинності під впливом розвитку інформаційного суспільства, окремим епізодам історії такої динаміки. У статті акцентується увага на відмінності суто кібернетичної злочинності від інших видів злочинності, що трансформувалася під впливом розвитку і можливостей ІКТ.

Ключові слова: киберзлочинність, інформаційне суспільство, кримінально-правове забезпечення розвитку інформаційного суспільства, безпека інформаційного простору, трансформація злочинності.

Савинова Н. А. Киберпреступность: обзор динамики в условиях развития Глобального информационного общества

Статья посвящена проблеме детерминации киберпреступности под воздействием развития информационного общества, отдельным эпизодам истории такой динамики. В статье акцентируется внимание на отличии сугубо кибернетической преступности от иных видов преступности, трансформировавшейся под воздействием развития информационного общества.

Ключевые слова: киберпреступность, информационное общество, уголовно-правовое обеспечение развития информационного общества, безопасность информационного пространства, трансформация преступности.

Savinova N.A. «Cybercrime: an overview of the dynamics interim of development of the Global Information Society».

The article is devoted to the determination of cybercrime under the influence of the information Society, the individual episodes in the history of such dynamics. The article focuses on the distinction purely cybercrime from other types of crime, transformed under the influence of the Information Society.

Keywords: cybercrime, information society, criminal law to ensure the information society, security of information space, the transformation of crime.

ТКАЧУК І.С.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА КОЛІЗІЙ ЯК ОКРЕМОГО ВИДУ ВЗАЄМОЗВ'ЯЗКІВ НОРМ КРИМІНАЛЬНОГО ТА КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНОГО ПРАВА

УДК 343.2.01:343.13(477)

Актуальність. Законодавство України <: високоорганічованою цілісною системою, якій повинні бути притаманні такі ознаки, як точність і несуперечність усіх її елементів. Слід зазначити, що на сьогодні зміни в законодавстві спричинили збільшення і виникнення невідомих раніше колізій правових актів. У зв'язку із цим необхідне теоретичне осмислення причин виникнення, шляхів усунення і подолання цих протиріч. Звичайно, досконалої системи законодавства, позбавленої колізій загалом і колізій правових актів зокрема, бути не може. Поява у сфері правового регулювання суперечностей неминуха через природний розвиток суспільних відносин. Але в Україні причини виникнення правових колізій характеризуються низкою обставин, таких як незавершеність правової реформи, невисока якість нормативних актів, що приймаються та ін.

Постановка проб. ими. У судовій практиці при вирішенні коїткретних справ виникають такі ситуації, коли виконання приписів процесуальних норм тягне за собою порушення норм матеріального права і навпаки. Про це кримінально-процесуальним законом не передбачено, як повинен діяти в таких випадках суд. У результаті, зустрічаючись з подібними колізіями, суди чинять по-різному, але в більшості випадків судова практика надає перевагу процесуальному закону.

На наш ПОГЛЯД, якщо з якихось причин виникає колізія між процесуальним і матеріальним правом, то повинна діяти певна субординація юридичних норм, ніщо не повинно заважати здійсненню правосуддя чи викривляти суть справи.

Важливість цієї проблеми привертала увагу багатьох ВІДОМИХ науковців. Вона досліджувалась у роботах С. Алексеева, В. Андрейцева, Ф. Бурчака, М. Власенка, Д. Гончарова, П. Свграфова, А. Зайця, О. Зайчука, М. Козюбри, В. Копейчикова, В. Кудрявцева, М. Марченко, М. Матузова, О. Миронска, С). Мурашина, З. Незнамової, Н. Оніщенко, В. Опришка, П. Рабіновича, В. Селіванова, В. Сіренка, О. Скакун, В. Тація, Ю. Тихомирова, Ю. Тодики, І. Усенка, К). Шемшученка та ін.

У вітчизняному правознавстві причини виникнення колізій правових актів поки що висвітлені частково, в основному з позиції того, що колізія руйнує єдність правового регулювання, внутрішню узгодженість системи права, негативно впливає на правову політику, що проводиться в державі, породжує протиріччя в правозастосуванні. Зазначене зумовлює необхідність загальнотеоретичного аналізу питань щодо змісту, видів, шляхів виявлення та подолання колізій у законодавстві.

Міністерство освіти і науки,
молоді та спорту України
Прикарпатський національний університет
імені Василя Стефаника

Юридичний інститут

Збірник наукових статей

**Актуальні проблеми вдо-
сконалення чинного зако-
нодавства України**

Випуск ХХVIII

м. Івано-Франківськ, 2012

ББК 67.9 (4Укр)

А 43

Редакційна колегія: д.ю.н., доц. Васильєва В.А. (*головнийредактор*); акад. АПрНУ, д.ю.н., проф. Луць В.В.; акад. АПрНУ д.ю.н., проф.Костицький М.В.; акад. АПрНУ, д.ю.н., проф. Погрібний О.О.; акад. АНВШУ, д.ю.н., проф. Дзера О.В.; д.ю.н., проф. Фріс П.Л.; д.ю.н., доп. Галянтич М.К.; д.ю.н., доц. Стефанчук Р.О.; д.ю.н., проф. Коссак М.В.; д.ю.н., проф. Майданик А.Р.; д.ю.н., проф. Кириченко О.А.; к.ю.н., доц. Кобецька П.Р.; к.ю.н., доц. Вівчаренко О.А.; к.ю.н., доц. Логвінова М.В.; к.ю.н., доц. Ославський М.І.; к.ю.н., доц. Пристані Л. Г.; к.ю.н., доц. Багай І.О.; к.ю.н., доц. Заїрський О.Б.; к.ю.н., доц. Микитин Ю.Л. (*відповідальний секретар*).

A43 Актуальні проблеми вдосконалення чинного законодавства України
[текст] : *Збірник наукових статей*. Випуск 28. - Івано-Франківськ : Прикарпатський національний університет імені Василя Стефаника, 2012. - 274 с.

У збірнику досліджуються актуальні проблеми державного будівництва, питання теорії та історії держави і права, правової реформи в Україні, екології, боротьби зі злочинністю. Вносяться та обґрунтовуються пропозиції щодо вдосконалення ряду інститутів конституційного, цивільного, кримінального та інших галузей права.

Для науковців, викладачів, аспірантів, здобувачів, студентів, слухачів, курсантів юридичних інститутів та факультетів, юристів-практиків.

Actual problems in the field of the formation of the Ukrainian State, questions of theory and history of state and law, law reforms in Ukraine, ecology, struggle against criminality are researched in this issue. The propositions on the perfection of some institutions of constitutional, civil, criminal and other spheres of law are submitted and analyzed.

Good for scientists, professors, post-graduate students, students of law departments, practising lawyers.

Реєстраційне свідоцтво: серія КВ №4150. Видається з 1996 року.

Адреса редколегії: 76018, м.Івано-Франківськ, вул. Шевченка, 44а. Юридичний інститут Прикарпатського національного університету імені В.Стефаника. Тел./факс (0342) 50-87-60.

ISSN 2218-1849

ББК 67.9 (4 Укр)

© Юридичний інститут Прикарпатського національного університету імені Василя Стефаника, 2012