документ гарантирует им права во взаимоотношениях с работодателями, устанавливает высокие стандарты техники безопасности и обитаемости на судах.

Наряду с Конвенциями СОЛАС, МАРПОЛ и ПДНВ новая конвенция МОТ должна стать «четвертым столпом» международного морского права» - подчеркнул генеральный директор российского морского регистра Н.Решетов.

Повышение уровня социальной защищённости моряков - один из важнейших элементов с точки зрения человеческого фактора, обеспечения безопасности на море, наряду с качественной профессиональной подготовкой.

«Морская профессия требует тщательной подготовки и не даёт права на ошибку, а неправильные действия могут привести к серьёзным последствиям», - заявил в своём докладе руководитель отдела «Оценка и экспертирование аспектов безопасности» Европейского агентства по безопасности на море (EMSA) г-н Хантер. В настоящее время морские учебные заведения и судовладельцы нацелены на разработку и совершенствование программ подготовки профессиональных кадров.

«Мы не должны, упускать ни одной возможности повысить престиж судоходства как живой индустрии - отметил А. Махапатра, руководитель отдела морской подготовки и человеческого фактора Управления безопасности мореплавания ИМО, - которая, не забывая соблюдать свои внутрикорпоративные обязательства в отношении социального обеспечения моряков, предлагает при этом выгодные в материальном отношении, способствующие профессиональному росту долгосрочные карьерные перспективы». [3, с. 29]

Литература

1. Международная конвенция по подготовке и дипломированию моряков и несении вахты 1978г. с поправками 1995г. (ПДМНВ 78/95).-55с.
2. Международный стандарт ДСТУ ISO 9001 -2001. Система менеджмента и качества. Требования.-12с.
3. Качественное судоходство и престиж морской профессии в XXI веке, // Морской флот.-2009г.-№1.

ПЕРЕДУМОВИ НЕОБХІДНОСТІ СТРАТЕГІЧНИХ ЗАХОДІВ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ БОРОТЬБИ З КІБЕРНЕТИЧНОЮ ЗЛОЧИННІСТЮ

Савінова Н.А.

Київський національний університет внутрішніх справ

На початку XX сторіччя необхідність правового забезпечення розвитку інформаційного суспільства (далі - ІС) сприймалася в Україні настільки гостро, що Верховною Радою України, навіть, озвучувалися думки щодо потреби у розробці проекту Інформаційного кодексу України[1]. Ця спірна з наукової точки зору ідея сама по собі була яскравим демонстратором того, що представники влади в Україні усвідомлюють необхідність запровадження ефективних норм правового забезпечення суспільних відносин в Україні в умовах розвитку ІС.

[1] **Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / За загальною редакцією д-ра юрид. наук, проф.. Бандурки О.М.: Монографія. - Харків: Вид-во Ун-ту внугр. Справ, 2000.- 368 с- С.190.**

у 1995 році СНД було започатковано розробку Концепції формування інформаційно простору СНД[2], у якій приймала участь і Україна. У цьому акті, зокрема, зазначалося, що учасниками прийняте рішення про віднесення діяльності по формуванню інформаційного простору до проблем і питань міждержавного рівня, рішення якого вимагає погоджених дій. Цей факт свідчить про те, що ще у листопаді 1995 року перед Україною постало питання щодо необхідності узгоджених дій щодо розбудови власного сегменту ІС (у контексті зазначеного Рішення СНД від 03 листопада 1995 року - "інформаційного простору"), проте, визнаючи необхідність вчинення власних правових рішень шодо формуванні ІС, і приймаючи участь у міжнародних актах з цього приводу, Україна фактично пасивно спостерігала за розвитком інформатизаційних і пов'язаних з ними глобалізаційних подій у світі.

9 січня 2007 року Україна зробила остаточний вибір щодо необхідності запровадження правового забезпечення у державі розвитку власного сегменту 1С, і Верховною Радою України був прийнятий Закон України № 537-V[3], яким було затверджено Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки (далі - Основні засади розвилку ІС в Україні), відповідно до яких одним з пріоритетів України відзначається "прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток ІС, в якому кожний міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя".

Розвиток ІС як у глобальному масштабі, так і його відповідні кооперативні та національні сегменти потребують на правове забезпечення всіх рівнів, адже розвиток суспільних відносин, як їх позитивна динаміка, не може відбуватися хаотично: відхилення від бажаного напрямку розвитку мають коригуватися за допомогою правових норм.

Кримінально-правове забезпечення розвитку ІС має відігравати одну з найважливіших функцій правового забезпечення в цілому, адже сфера її спрямування охоплює найбільш суспільно-небезпечні відхилення у суспільних відносинах. Саме кримінально-правове забезпечення реалізує політику боротьби зі злочинністю в спектрі кримінально-правової політики. Розуміння ж кримінально-правового забезпечення, як ролі держави у впорядкуванні та розвитку суспільних відносин у сфері убезпечення останніх від суспільно небезпечних посягань - злочинів та кримінальних проступків, особливо актуалізується в умовах трансформації суспільних відносин на шляху до ІС. Руйнування старої системи суспільних цінностей, неврегульованість відносин, що відбуваються з приводу цінностей ІС, стан аномії суспільства та глобальна популяризація негативу, яка здійснюється з урахуванням впливу ЗМІ на свідомість аудиторії, а також зростання вірогідності здійснення злочинів дистанційно тощо обумовлюють переосмислення підходів до кримінально-правового забезпечення розвитку СІ у напрямках, які обумовлюють такий розвиток: розвиток і безпеку інформації, знань, ІКТ, комунікацій, спілкування.

Усвідомлення сутності інформаційної безпеки у ІС необхідно потребує оцінки загроз та переростання їх у безпосередні випливи. Оскільки ж інформація, знання та ІКТ

[2] Рішення про розробку проекту Концепції формування інформаційного простору Співдружності Незалежної Держави № 997 в82 від 11.03.1995 р. // Збірник чинних міжнародних договорів України 2006р, № 5, (№№ Книга 2 ст. Д-196), стор. 675.

[3] Закон України "Про Основні засади розвитку інформаційного суспільства в Україні" від 9 січня 2007 року № 537-V // Відомості Верховної Ради України від 23.03.2007. - 2007 р., № 12, стор. 511, стаття 102.

використовуються у всіх сферах суспільного життя, логічним є твердження, що і відповідні загрози у ІС спрямовуються на всі сфери життєдіяльності, а впливи на інформацію, знання та ІКТ руйнівно впливають на суспільні відносини у відповідних сферах.

З точки зору політико-правових заходів і цілісного правового забезпечення розвитку ІС, слід виявляти та попереджувати ті загрози, які потенційно переростають, або вже переросли у впливи, окреслити такий перелік і визначити, які саме з них лишились лише загрозами і можуть бути усунуті політико-правовими заходами запобігання, а які саме з них вже мають визнаватися впливами, і, відповідно, потребують активної протидії - боротьби. Важливим фактором оцінки подібних негативних явищ є оцінка їх суспільної безпечності, яка відносить делінквентні прояви до категорії злочинів, і які, відповідно, потребують політико-правових заходів, генерація яких покладається на політику у сфері боротьби зі злочинністю.

Спектр загроз і потенційних впливів розвитку ІС, які можуть виникати внаслідок протиправних дій у ІС, а також, відповідно, щодо розвитку ІС, може коливатися від мінімальних, на перший погляд, втручань, до дій, які мають наслідками катастрофи світового масштабу[4]. „За усіх позитивів, - пише М.Головатий, - особливо для країн, які за рахунок інтенсивного розвитку і використання інформації вступили у так звану інформаційну еру, інформаційне суспільство має все ж і багато проблем, несе певні загрози, \...\, може сприяти появі так званої інформаційної диктатури, розпалюванню інформаційних війн тощо".[5] У контексті розвитку ІС слід усвідомлювати спектр загроз, який здатний до переходу у впливи, що здатні заподіяти шкоду розвитку суспільних відносин у ІС, шляхом посягання на інформаційний простір та комунікаційну інфраструктуру як в цілому, так і окремим складовим інформаційного простору або відповідної інформаційної інфраструктури.

Прогнози С. Лема, зроблені в середині XX сторіччя стосовно непередбачуваності і негативів, поряд із позитивами розвитку технологій[6] повною мірою відображені у сьогоденному стані відносин у ІС, коли „роздвоєння" досягнення цілей призвело до співіснування суспільно-корисних відносин у ІС та кібернетичної злочинності[7], спрямованої на такі відносини, та блага з приводу яких такі відносини виникають.

Інформація і ІКТ виступають основними ресурсами ІС, і тому кожне з них, або їх сукупність, слід розглядати як потенційний предмет спрямування злочинної діяльності або злочинності в цілому. При цьому надто важливо, сприймаючи інформацію та ІКТ, розуміти їх як такі, які можуть зазнавати злочинного впливу і у сукупності, і по одинак[8], ІКТ можуть бути і предметом злочину і знаряддям його вчинення[9] або засобом[10] вчинення

[4] Останні, як їх характеризував С.Лем, можуть "досягати апокаліптичних розмірів". (Лем С. Сумма технологии: Сомнения и антиомы: Пер. с польского. / С.Лем. - М.: ООО «Издательство АСТ»; СПб.: Тепа Fantastika, 2004. - 668, [4] с. - (Philosophy). - С. 23.)

[5] Політологічний словник: Навч. посіб. для студ. вищ. навч. зал. / За ред. М.Ф.Головатого іа О.В. Антонюка, - К.: МАУП. 205. - 792 с. - С. 341

[6] Лем С. Сумма технологии: Дилеммы: Пер. с польского. / С.Лем. М.; ООО «Издательство АСТ»; СПб.: Terra Fantastika. 2004. 668, [4] с. - (Philosophy). - С. 22.

[7] Тузов. Цивилизация «юзеров». - Корреспондент. - 2007 - № 3 (243). - С. 24

[8] Розенфельд Н.А. КримІнально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дисертація канд. юрид. наук: 12.00.08 / НАН України ; Інститут держави і права ім. В.М.Корецького. - К., 2003. 222 с. - 73, 77.

[9] Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дисертація канд. юрнд. наук: 12.00.08 / НАН України ; Інститут держави і права їм. В.М.Корецького. - К, 2003. - 222 с. - С. 103.

злочинів у ІС. Враховуючи те, що процес такої переорієнтації не відбувається водномить, найочевиднішим є саме перехід відомої раніше злочинності - трансформація злочинності у інформаційний простір, спостерігається з кожним роком все активніше. Доречно у цьому контексті навести висловлення Л.І.Бачило, яка зазначає: "Якщо інформаційні технології дають скорочення часу у області контактів контрагентів у глобальних мережах, то інші компоненти будуть відстоювати свої позиції"[11].

Особлива увага дослідників та практиків приділяється „новітнім" суспільно-небезпечним діянням, які, по суті, містять ознаки діянь, що визнавалися злочинами протягом десятків, або, навіть, сотень років, а вчинення таких, внаслідок розвитку ІКТ та ІТ, набуло нових можливостей, або, навіть - розмаху: підроблення [комп'ютерних] паролів і кодів, викрадення [електронних] грошей, викрадення [комп'ютерної інформації], пошкодження [комп'ютерної інформації або системи], вимагання шляхом загрози поширення відомостей [у вигляді комп'ютерної інформації], поширення порнографії [у мережі Internet], акт [кібер]тероризму тощо. Проте, і це слід підкреслити, що така трансформація відбулась внаслідок не лише використання досягнень розвитку ІКТ злочинцями, а, насамперед, через відповідну трансформацію певних благ у віртуальний простір: виникнення „віртуальних грошей", електронного підпису, телекомунікацій, мережевих спільнот, електронного маркетингу тощо.

Отримавши можливість використання сучасних ІКТ, і, відповідно можливість отримувати інформацію, у т.ч. знання, без обмежень часом, відстанню та кордонами, людство стало більш уразливим від злочинності, яка, користуючись тими ж ІКТ, не обмежена відстанню до предмету посягання, не стримується кордонами. Розвиток ІКТ і відносин, що відбуваються при їх використані, породив паралельний розвиток новітньої кібернетичної злочинності, спрямованої на відповідний предмет, який має нове вираження і не завжди є матеріальним[12], і визначатися, відповідно, як віртуальний[13] [14], під яким розуміється предмет об'єктивного світу, який створений за допомогою спеціальних методів та (або) засобів, фізично відсутній, але має зовнішнє представлення, або може набути такого представлення за допомогою спеціальних методів та способів впливу.[15]

Такі раніше відомі суспільно-небезпечні діяння, які трансформувалися у кібернетичний простір з реального у зв'язку з розвитком ІКТ та переходом певних благ кібернетичний простір, і зберігли, при цьому, ознаки раніше відомих злочинів, що відносяться до загальнокримінальної злочинності[16]: розкрадання певних благ, або їх пошкодження чи зміни їх первинного стану, поширення порнографічної, расистської, ксенофобної інформації та інформації, що культивує насильство та жорстокість, відомі

[10] Розенфельд Н.А. Кримиїально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дисертація канд. юрид. наук: 12.00.08 / НАН України ; Інститут держави і права ім. В.М.Корецького. - К , 2003. 222 с. -С. 114.

[11] Информационное право: основы пракшческий информатики. Учебное пособие/И.Л.Бачило. М:,2003.- 352с.-С.319.

[12] Голубев В. Комп'ютерна злочинність // Юридичний вісник України. 2002. - № 6. - с. 1,4. - С. 1

[13] Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дисертація канд. юрид. наук: 12.00.08 / НАН України ; Інститут держави і права ім. В.М.Корецького. - К., 2003. - 222 с. - С. 196.

[14] Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Автореферат дис. ... канд.. юрид, «аук:12.00.08. - Київ. Ін-т держави і права НАН України. - Київ, 2003. - С. 9.

[15] Розенфельд Н.А. Віртуальний предмет злочинів, пов'язаних з порушенням авторського права і суміжних |трав // Право України. - 2008. - № 5 - С.с. 105-108 - С. 106.

[16] Криминология. Учебник для юридических вузов. Под общей редакцией доктора юридических наук профессора А.И.Долгановой - М: Издательская группа ИНФА-М-НОРМА, 1997. - 784 с. - С. 463.

раніше, у зв'язку з їх трансформацією, на світовому рівні отримали назву „кібернетичні злочини" або, скорочено, - „кіберзлочини", а явите, що характеризується сукупністю кіберзлочинів - „кіберзлочинність". Виходячи з розуміння основних ресурсів ІС, злочини що на них посягають не завжди є новітніми, а багато з них належать взагалі до загальнокримінальної злочинності, саме трансформація злочинності у інформаційному просторі здебільшого відбувається внаслідок переходу звичайних злочинів[17] у злочини кібернетичні.

Трансформація загальнокримінальної злочинності під впливом розвитку ІКТ, може спрямовуватися на будь-які об'єкти суспільних відносин, які цікавлять злодія, оскільки всі сфери життєдіяльності суспільства сьогодні інформатизовані. Проте, кібернетичні злочини можуть вчинюватися виключно з використанням ІКТ, одночасно, сучасний рівень динаміки ІКТ забезпечує широкий доступ до ресурсів фінансових, комунікаційних і інформаційних центрів, синтезує нові технології, і, відповідно, стимулює подальшу трансформацію злочинності.

Сьогодні вже очевидно, що навіть на первинних стадіях кібернетичні злочини мали світове значення, адже відбувалися паралельно з розвитком ІС, користуючись усіма зручностями і можливостями ІКТ. Проте варто звернути увагу на перші прояви трансформації загальнокримінальної злочинності у кібернетичну, з метою усвідомлення сутності останньої як явища, яке могло відбутися лише у ІС. З метою усвідомлення сутності трансформації і переходу звичайної злочинності у кіберзлочинність, проведемо огляд найгучніших з таких злочинів за останні 50 років.

Від кіберзлочинності зазнають інформаційні агенції всього світу, які постійно відчувають інформаційні втручання[18] [19] Яскравим прикладом може слугувати втручання у роботу дитячого телеканалу Disney Channel у CUJA у 2007 році, на якому, як повідомляє News.uaclub.net, у ранковий час, коли канал переглядають діти, була "продемонстрована" хакерами жорстка порнографія.[20] Очевидно, що від подібного втручання зазнає, насамперед аудиторія каналу, яка отримує неочікувану, а у продемонстрованому випадку - руйнівну для психіки дитини інформацію.

Загалом, злочини проти моральності, зокрема - поширення порнографії, культу насильства та жорстокості, процвітають у Internet: пошукова система GOOGLE[21] станом на 20 березня 2008 року видавала за пошуком "порно" - 14 200 000 посилань (лише російськомовних), за пошуком - "видео сцена изнасилования" - 494 000 посилань, "сексуальне извращения" - 255 000, "видео пыток» - 564 000 посилань, «порно с подростками» - 1 790 000 посилань. Жахливим є те, що серед "сценарованийх" зйомок подібної продукції наявні також і дійсні факти ґвалтувань і знущань, зняті з метою розміщення у Internet.

Хоча саме через виникнення і модифікації кібернетичних злочинів відбувається вплив злочинності на ресурси ІС, не лише кіберзлочини становлять загрозу для

[17] Для зручності відмежування злочинів, які були відомі до виникнення злочинів кібернетичних у подальшому дослідженні буде застосовуватися прикметник „звичайні", і, відповідно стосовно явища, які утворюють такі злочини, у якості термінупоняття застосовуватиметься словосполучення „звичайна злочинність".

[1S] Китайские хакеры перенесли дату атаки на сайт CNN / Зашита информации// http://informationsecurity.ru/keywords php?keyword…

[19] Азербайджанский хакер взломал пять армянских сайтов/ Day. Az//http://www.day.az/news/hitech/68996.html

[20] Американським детям показали порногорафию на канале Disney //Центр Исследования компьютерной преступности / http://www.crime-research.ru/news/04.05.2007/3444/

[21] GOOFLE.com / http//:www.google.com

останнього. Кібернетичні злочини можуть бути спрямовані на ресурси, які використання яких здійснюється через комп'ютерних систем, або які самі містяться у таких системах, при чому лише під час безпосередньої роботи останніх. Ресурси ж ІС - інформація, у т.ч. знання, та ІКТ можуть перебувати і поза межами комп'ютерних систем, не втрачаючи при цьому своєї цінності для ІС, як стадії розвитку людства. Так, для ІС, без урахування їх значення для історії та кільтури, рівною мірою цінні знання, зазначені на папірусі, викладені у монографії, чи розміщені у Інтернет. Останні лише більше уразливі для кібернетичного протиправного посягання, а у разі, якщо перші два також будуть розміщені у Internet, вони стануть такими ж уразливими, оскільки йдеться про сам зміст, наповнення такого знання, а засоби його носія не мають значення. Саме на зміст такого знання направляється злочин - злочинець може намагаєгься отримати таке знання з повним спектром мотивації: від банальної корисливої мети до виконання замовлення по шпіонажу[22]

Підсумовуючи наведене вище, з урахуванням дослідженої ґенези 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. Кіберзлочини характеризуються здебільшого індивідуальною спрямованістю, за виключенням випадків використання ретеальної (мережевої) комунікації[23], направленої на невизначену кількість реципієнтів.[24]

Необхідно зазначити, що кібернетичні злочини є злочинами, що становлять не меншу загрозу для суспільства, ніж їх попередники - звичайні злочини. Ще у 2003 році підкреслювалось, що кібернетичні злочини становлять особливу суспільну небезпечність, яка обумовлюється інтенсивністю впровадження технологій в усі сфери життєдіяльності та наявності широкого кола осіб які володіють достатніми знаннями та технічними навичками для вчинення злочинів у кібернетичному просторі[25]. Якщо друга причина, з наведених автором раніше збереглася повною, то перша причина через ступінь розвитку ІС і перехід економіки розвинутих країн світу у мережеві стосунки, просто втратила актуальність в частині інтенсивного запровадження, яке замінилося на сталий стан використання ІКТ, який постійно модернізується.

Підкреслимо, що окремим і необмеженим важелем ескалації кіберзлочинів у світі є їх популяризація через ЗМІ, у т.ч. web-сайти у Internet, а також через художні фільми, у яких хакерів наділяють героїчними рисами, в той час, як насправді вони вчинюють злочинні дії.

У той же час на державному рівні попри участь України у всіх прогресивних заходах міжнародної спільноти у протидію кіберзлочинності та активної роботи у напрямку реалізації Концепції реформування кримінальної юстиції, зокрема, в контексті підвищення ефективності протидії злочинності, ефективних законодавчих заходів кримінально-правової протидії злочинності не здійснюється. Діяння у кібернетичному просторі, соціальна обумовленість яких вимагає криміналізації, до цього часу у КК не включаються, що створює постійну трансформацію і ескалацію кібернетичної злочинності.

[22] Г. Балда. Коротка історія гакерства// http://www/universum.org.ua/sp/2002/haker 3.html

[23] Корнєв М.Н., Коваленко А.Б. Соціальна психологія: підручник. - К., 1995. - 304 с. - С. 86.

[24] Виключенням у цьому випадку є безадресне розповсюдженням через мережу певних знарядь або засобів суспільно-небезпечних діянь: розповсюдження порнографії та предметів. що містять культ насильства та жорстокості, пін-кодів. расистських закликів, тощо.

[25] Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Дис. канд.. юрид. аук. Інститут держави і права їм.. В.М.Корецького НАН України, 2003. р. - 222 с. - С. 16.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МИКОЛАЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

НАУКОВІ ПРАЦІ

СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО - ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

СПЕЦІАЛЬНИЙ ВИПУСК

МИКОЛАЇВ - 2010

МИКОЛАЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

СПЕЦІАЛЬНИЙ ВИПУСК

СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

В збірник ввійшли матеріали, представлені і обговорені під час проведення 2-ої Всеукраїнської науково-практичної конференції «СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ» 15-17 вересня 2010р., в с. Коблево Миколаївської області

МИКОЛАЇВ - КОБЛЕВО
2010

ЗМІСТ