українському і міжнародному співтовариству.

Зазначені концептуальні ідеї знайшли розуміння і підтримку в органах влади нашої країни. Відповідно до рішення Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади від 6 жовтня 2000 року проект Концепції реформування законодавства України (щодо кодифікації) у сфері суспільних інформаційних відносин (далі Концепція) передано на обговорення до державних органів центральної виконавчої влади та до наукової громадськості за участю Академії правових наук України.

Ініціатива щодо розробки Концепції підтримана окремими народними депутатами України та фахівцями практиками.

Концепція розглянута на засіданні науково-технічної ради Національної програми інформатизації та Консультативної ради з питань інформатизації при Верховній Раді України.

Указом Президента України від 6 грудня 2001 року № 1193/2001 "Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" визначено Кабінету Міністрів у шестимісячний строк розробити пропозиції щодо кодифікації законодавства в галузі інформаційних відносин.

Запропоновані концептуальні положення є результатом спільної творчої праці ініціативної групи практиків органів влади та вітчизняних вчених: Академії правових наук України, Науково-дослідного центру правової інформатики, Київського регіонального центру Академії правових наук України, Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинністю при Президентові України, Національної академії внутрішніх справ, Національної юридичної академії ім. Я. Мудрого та інших наукових і вищих навчальних закладів України.

Інформація щодо Концепції розміщена в Інтернет за адресами: http://mndc.naiau.kiev.ua та www.bespeka.com

Література: 1. Виявлення та розслідування злочинів, що вчиняються з використанням комп'ютерних технологій. /заг.ред. Я. Ю. Кондратьєва. – К.: НАВСУ, 2000. – 64 с. 2. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Монографія /За заг. ред. д. ю. н. Калюжного Р. А. – Запоріжжя: "Просвіта", 2001. – 252 с. 3. Інформатизація соціального управління: теорія і практика (організаційно-правовий аспект). Посібник. Наукове видання. – Київ – Донецьк: Донецький інститут внутрішніх справ, 2001. – 190 с. 4. Інформаційне право та інформаційна безпека /Сучасний стан, поняття та визначення змістовної частини, інкорпорація нормативних актів з правових питань у сфері інформації та її захисту/ заг. ред. Р. Калюжного та В. Філонова – Київ – Донецьк: Донецький інститут внутрішніх справ МВС України. Інститут економіки та права "КРОК", 2001. – 230 с. 5. Комп'ютерна злочинність. Навчальний посібник. – Київ: "Атіка", 2002. – 240 с. 6. Інформаційне суспільство. Дефініції…/Брыжко В. М., Гальченко О. М., Цымбалюк В. С., Орехов О. А., Чорнобров А. М. /За ред. Р. А. Калюжного, М. Я. Швеця, – К.: "Інтеграл", 2002. – 220 с. 6. е-будущее и информационное право//Брыжко В. М., Цымбалюк В. С., Гальченко О. М., Орехов О. А., Чорнобров А. М./За ред. Р. А. Калюжного, М. Я. Швеця, – К.: "Інтеграл", 2002. – 264 с.

УДК 002.6+342.7

ЄВРОПЕЙСЬКА КОНВЕНЦІЯ З КІБЕРЗЛОЧИНІВ

Михайло Гуцалюк

Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю

Анотація: **Розглянуто проблеми комп'ютерної злочинності у контексті інтеграції України до європейського співтовариства. Пропонуються організаційні заходи щодо створення Міжвідомчого центру боротьби з комп'ютерною злочинністю.**

Summary: **The problem of computer crime in a context of integration of Ukraine in the European society is examined. The organizational measures of formation of Interagency center on combating computer crime are offered.**

Ключові слова: **Інформаційне суспільство**, **комп'ютерна злочинність, інформаційна безпека**.

І Вступ

В епоху інформаційної революції розвиток держави визначає насамперед рівень її досягнень у сфері обробки інформації.

Сьогодні Україна вибрала стратегічний шлях свого розвитку, що полягає в інтеграції в Європейське співтовариство. Як відомо, однією з особливостей цього співтовариства є побудова інформаційного суспільства, яке широко використовує досягнення нових інформаційних технологій і, зокрема, глобальної комп'ютерної мережі Internet.

Однак, зазначені прогресивні досягнення мають і зворотний бік медалі. Як відомо, з поширенням використання інформаційних технологій у сфері управління, технологічних процесів зростає їх вразливість щодо вчинення правопорушень з використанням засобів комп'ютерної техніки. Об'єктивно це пояснюється зниженням рівня захищеності інформаційних систем, зростанням кількості антисоціальних проявів внаслідок поширення користувачів глобальних комп'ютерних мереж, використання наукових та технічних досягнень криміналітетом. Інтереси організованих злочинних груп і окремих правопорушників спрямовані на відмивання «брудних коштів», поширення неправдивої інформації, фінансові махінації, і в першу чергу, порушення у банківсько-кредитній сфері, де активно використовуються автоматизовані системи.

Слід зазначити, що в Україні ріст комп'ютерних злочинів відповідає світовій тенденції, яка полягає в пропорційності росту даного виду правопорушень масштабам використання засобів обчислювальної техніки [1]. Зазначеній проблемі приділяється значна увага як окремих країн, так і міжнародних організацій, таких як ООН, Рада Європи та ін. 23 листопада 2001 роки у Будапешті проходила міжнародна конференція по проблемах боротьби з кіберзлочинністю, де представники 30 країн підписали Європейську конвенцію про кіберзлочинність.

ІІ Зарубіжний досвід боротьби з комп'ютерною злочинністю

Розглянемо досвід боротьби з комп'ютерною злочинністю в деяких країнах.

Статистика таких злочинів ведеться з 1958 року. Тоді під ними розуміли випадки псування і розкрадання комп'ютерного устаткування; крадіжка інформації; шахрайство або крадіжка грошей, зроблені з застосуванням комп'ютерів; несанкціоноване використання комп'ютерів або крадіжка машинного часу. Записи велися в Стенфордському дослідницькому інституті і довгий час не мали великого інтересу. До речі, у 1966 році комп'ютер уперше був використаний як інструмент для пограбування банку. Сталося це в Міннесоті. У 1968 році у Сполучених Штатах Америки було зафіксовано 13 злочинів; у 1978 році – 85, а в 1975 році інститут припинив ведення і публікацію статистики через складність визначення вірогідності подій, число яких швидко росло [2].

І сьогодні, з кожним роком проблема комп'ютерної злочинності постійно ускладнюється. Військові, фінансові, промислові структури наче магнітом притягують зловмисників. У 2001 році було зареєстровано понад 20 тис. проникнень в інформаційні комп'ютерні системи.

Тому з 1984 року в США діє перший закон, присвячений комп'ютерним правопорушенням, який в подальшому багато разів редагувався. З'явилися й інші нормативні акти, присвячені цій проблемі. Проте, не дивлячись на прийняті закони, проблема не стала менш гострою.

ФБР і департамент юстиції в 1991 році створили відділи, що займаються комп'ютерними злочинами (The Criminal Division, Computer Crime & Intellectual Property Section, U.S. Department of Justice. Секретні служби, що є частиною фінансового департаменту, також створили свій відділ комп'ютерних злочинів – Electronic Crimes Branch. Відділ ФБР, відомий як National Computer Crime Squad, є частиною Washington Metropolitan Office ФБР).

Після інциденту з вірусом в Internet у 1988 р. комп'ютерне суспільство прийшло до висновку про необхідність заснувати організацію, яка була б здатна швидко реагувати на погрози безпеки Internet, можливі в майбутньому. Під егідою Управління перспективних дослідницьких проектів Міністерством оборони був створений Координаційний центр групи реагування на екстренні ситуації, які пов'язані з комп'ютерами (CERT – Computer Emergency Response Team). Центр у кооперації з громадськими та приватними комп'ютерними мережами допомагає організаціям реагувати на напади і поширює інформацію про них.

Нижче в табл. 1 представлені види комп'ютерних атак за інформацією CSI/FBI 2000 Computer Crime and Security Survey.

Таблиця 1 – Динаміка збитків від комп'ютерних злочинів в США

Види атак	Кількість респондентів, що підтвердили фінансові втрати				Загальна кількість втрат у рік в тисячах $			
	1997	1998	1999	2000	1997	1998	1999	2000
Крадіжка інформації	21	20	23	22	20048	33545	42496	66708
Саботаж даних в мережі	14	25	27	28	4285	2142	4421	27148
Перехоплення інформації	8	10	10	15	1181	562	765	991
Несанкціонований доступ	22	19	28	29	2912	1637	2885	7104
Зловживання персоналу	55	67	81	91	1006	3720	7576	27984
Фінансове шахрайство	26	29	27	34	24892	11239	39706	55996
Відмова в обслуговуванні	-	36	28	46	-	2787	3255	8247
Зміна інформації	4	-	-	-	512	-	-	-
Віруси	165	143	116	162	12498	7874	5274	29171
Несанкціонований доступ персоналу	22	18	25	20	3992	50565	3567	22554
Мережеві шахрайства	35	32	29	19	22660	17256	773	4028
Активне перехоплення	-	5	1	1		245	20	5000
Крадіжки портативних ЕОМ	165	162	150	174	6132	5250	13038	10404
Загальні щорічні збитки					**100118**	**136822**	**123776**	**265335**

Загальна сума збитків понад $ 626 млн.

У Великобританії на створення спеціального підрозділу по боротьбі з комп'ютерними злочинами National High-tech crime Unit на 2001 рік виділено $ 35 млн.

У Турції з 1999 року в Загальному Управлінні безпеки було створено новий підрозділ "Робоча група по боротьбі зі злочинами в інформатиці" (Work Group for Crimes on Informatics), якою щорічно порушується біля 50 кримінальних справ.

Щорічно поліція Словенії порушує понад 500 кримінальних справ, де так чи інакше використовувались комп'ютерні технології.

У Швеції у 2000 році Національна Рада з попередження злочинності провела дослідження щодо комп'ютерних правопорушень в 1564 організаціях. Висновок дослідження – кількість даного виду правопорушень збільшилась на 40–80 відсотків. Для боротьби з правопорушеннями на центральному рівні у Національному Департаменті кримінального розшуку створено Команду по боротьбі зі злочинами у сфері інформаційних технологій – Information Technology Crime Squad.

В Японії кількість правопорушень зросла в двічі з 229 у 1990 до 461 у 1999 році. Кількість заарештованих осіб у 2000 році було 559, з яких 484 використовували комп'ютерні мережі. Було зареєстровано 106 випадків несанкціонованого доступу в комп'ютерні мережі, з яких 25 були з-за кордону. У квітні 2001 року Національне поліцейське агентство створило Офіс по боротьбі з кібертероризмом – Cyber Terrorism Technology Office – для зменшення збитків від кібертероризму. Поліцейські для подібних справ наймають системних інженерів та інших фахівців, що мають досвід використання комп'ютерної техніки. З 2001 року широко використовується система Cyber-Crime для технологічного обміну інформацією серед поліцейських агентств Китаю, Індонезії, Кореї, Малайзії, Філіппін, Сінгапуру, Таїланду.

У Польщі інциденти в глобальній мережі реєструє спеціально створена група Network Security Team по спеціальному телефону 0202122, яка працює з 1998 року. В останній час кількість таких інцидентів зросла у геометричній прогресії – з 1000 у 1998 році до 20000 у 2001. Це пояснюється різким зростанням користувачів Інтернет та впровадженням у суспільство е-бізнесу. Створений в 1998 у Варшаві спеціальний підрозділ – Police Computer Crime Unit порушив за час свого існування понад 600 кримінальних справ, з яких 400 – пов'язані з кредитними картками, що використовуються в он-лайн сервісі, 200 – з несанкціонованим доступом. Додатково розслідувалися 100 випадків дитячої порнографії. Більшість правопорушень було пов'язано з польським доменом. Біля 40 випадків надійшло з-за кордону. З питань інформаційної безпеки утворено багато комерційних та наукових установ, зокрема CERT-Poland.

У Португалії утворено спеціальний підрозділ для боротьби з комп'ютерними правопорушеннями, юрисдикція якого поширюється на всю територію країни. У Словенії для інформації щодо комп'ютерних загроз та проведення наукових робіт у цьому напряму створено Sl-CERT. В інших країнах світу також налагоджується система заходів щодо протидії кіберзлочинам [3].

Після утворення національних груп CERT, кожна з яких мала свої цілі та фінансування, постала необхідність утворення координуючого органу, який би вирішував питання взаємодії груп, які знаходяться в

різних часових поясах та використовують різні мови спілкування. Такою організацією стала FIRST – форум команд реагування на інциденти, яка була створена на початку 90-х років та об'єднує 80 бригад реагування з 19 країн світу [4].

Враховуючи активність криміналітету у сфері економічних та інших галузей суспільних відносин, які мають вплив на економічні процеси в Україні, для посилення протидії даній категорії злочинів, у структурі ДСБЕЗ МВС України у червні 2001 року створено Управління по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій, у складі якого сформовано відділ по боротьбі з правопорушеннями у сфері високих технологій.

Сьогодні співробітниками відділу по боротьбі з правопорушеннями у сфері високих технологій проводиться збір та аналіз оперативної інформації по основним напрямам діяльності: боротьба зі злочинами у сферах комп'ютерної інформації, електронних платежів, телекомунікацій, протидія легалізації («відмиванню») грошових коштів та іншого майна, здобутих злочинним шляхом, що здійснюються за допомогою високих інформаційних технологій.

З часу вступу в дію нового Кримінального кодексу України підрозділами Управління викрито понад 50 злочинів, вчинених особами за допомогою комп'ютерних технологій та в системах електронних платіжних систем (для порівняння: до створення такого підрозділу в 2000 році було порушено 7 кримінальних справ за ст. 198-1 Кримінального кодексу, що діяв раніше).

Аналізуючи кримінальні справи, можна зробити висновок, що основним об'єктом комп'ютерної злочинності залишається кредитно-фінансова сфера, а саме банківські установи. Головним напрямом злочинної діяльності у цій сфері, яка вже набула широкого розповсюдження, є шахрайство з використанням пластикових платіжних карток. Перш за все, це зумовлено переходом банківських та фінансових структур на розрахунки з використанням електронних платіжних систем.

У зв'язку з міжнародним характером кіберзлочинів, актуальною залишається взаємодія правоохоронних органів різних країн з метою кримінального переслідування злочинців – адже саме кібертерористи частіше всього користуються відсутністю кордонів та митних служб у кіберпросторі. У зв'язку з цим необхідно, щоб кримінальне право не відставало від швидких змін у технології передачі даних, які використовують злочинці для протиправної дії у кіберпросторі. Важливою вимогою Конвенції про кіберзлочини є уніфікація національних законодавств та вирішення процедурних питань щодо виявлення місцезнаходження злочинців у кіберпросторі, зберігання комп'ютерних доказів та виконання інших технологічних заходів, наприклад, перехоплення електронної інформації, яка надходить з систем обробки незаконної інформації (дитяча порнографія, расистські заклики та ін.).

III Міжвідомчий центр по боротьбі з комп'ютерною злочинністю

6 грудня 2001 року Президент України підписав Указ № 1193/2001, який передбачає внесення змін у законодавство, що регулює питання боротьби з кіберзлочинами.

З метою організації протидії кіберзлочинності, в тому числі поширенню через глобальні та національні мережі зв'язку ідеології тероризму, пропаганди насильства, війни і геноциду Постановою Кабінету Міністрів України від 14 грудня 2001 р. № 1694 заплановано розробити з урахуванням рекомендацій Парламентської Асамблеї Ради Європи щодо боротьби з міжнародним тероризмом проекти Законів України "Про моніторинг телекомунікацій", "Про захист інформації в мережах передачі даних", "Про регулювання українського сегменту мережі Інтернет" [5].

З кожним роком все небезпечнішими стають комп'ютерні віруси. Значне їх поширення можна пояснити тим, що на відміну від більшості вірусів 90-х, сучасні використовують як основний канал розповсюдження – мережу Інтернет. За оцінками деяких експертів вірусні атаки заблокують роботу електронної пошти вже до 2010 року. Слід відзначити, що українські інформаційні системи привабливі для вірусів не менше, чим зарубіжні. Для прикладу можна навести резонансне зараження 16 листопада 2001 року вірусом "Nimda" комп'ютерної мережі Укртелеком (провідного оператора зв'язку в Україні).

Сьогодні, в зв'язку з викладеним вище, невідкладним завданням є створення Міжвідомчого центру боротьби з комп'ютерними злочинами (МЦБКЗ), що передбачено Указом Президента України Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України". На базі МЦБКЗ слід організувати контактний пункт для отримання повідомлень про кіберзлочини та надання оперативної допомоги жертвам кіберзлочинів, створити базу даних для статистичних, кримінологічних та криміналістичних досліджень, лабораторію для проведення комп'ютерних експертиз. Центр може стати місцем для організації семінарів, практикумів у системі підготовки суддів, прокурорів, слідчих. Якщо сьогодні на створення та функціонування МЦБКЗ не виділити достатніх фінансово-матеріальних ресурсів – завтра втрати економіки держави від комп'ютерної злочинності будуть набагато більшими.

IV Висновок

Підписання Україною Конвенції про кіберзлочини стало важливим етапом на шляху до інтеграції в Європу. Наступним логічним кроком має стати ратифікація зазначеної конвенції Верховною Радою України та практичні рішення щодо її реалізації. У зв'язку з цим слід зазначити, що розробка ефективних заходів протидії злочинам у сфері високих технологій вимагає співробітництва між державою і комерційними підприємствами, що працюють на ринку Інтернет-послуг. Держава може тільки тоді ефективно боротися з кіберзлочинами, коли діє в партнерстві з підприємцями, що здійснюють свою діяльність в глобальних інформаційних мережах. Відповідно до цього, правоохоронним органам слід організувати співробітництво з Інтернет-провайдерами, контент-провайдерами, фінансовими компаніями, що надають послуги в мережі Інтернет, а також з електронними магазинами по реалізації спільної протидії комп'ютерній злочинності, особливо в частині, що стосується виявлення та ідентифікації злочинців.

Література: 1. М. В. Гуцалюк Проблеми протидії комп'ютерній злочинності // Бюлетень з обміну досвідом роботи. Науково-практичне видання: МВС. – 2001. № 135. – С. 26-31. 2. Компьютерные террористы: Новейшие технологии на службе преступного мира./Автор- составит. Т. И. Ревяко. - Мн.: Литература, 1997. – 640 с. 3. Комп'ютерна злочинність. – К.: Атіка. – 2002. – 240 с. 4. М. Вест-Браун, К. Коссаковский Международная инфраструктура за глобальную безопасность и реагирование в сфере информационных технологий. – 1999 // http://bezpeka.com. 5. Указ Президента України від 6 грудня 2001 року № 1193/2001 Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України". 6. Постанова КМ України від 14 грудня 2001 р. № 1694 Про затвердження Програми реалізації положень Варшавської конференції щодо спільної боротьби проти тероризму.

УДК 681.3

КОМЕНТАР ДО СТАТЕЙ 361 – 363 КК УКРАЇНИ

Петро Андрушко
Київський Національний Університет України ім. Т. Шевченка

Анотація: **Дається науково-практичний коментар до статей 361 – 363 нового КК України, які встановлюють відповідальність за вчинення комп'ютерних злочинів.**
Summary: **This article is dedicated commenting the articles 361 – 363 of the new Crime Code of Ukraine, which dispose responsibility for committing computer crimes.**
Ключові слова: **Злочинність, кримінальний кодекс, злочин, автоматизовані електронно-обчислювальні машини (комп'ютери), їх системи та мережі, відповідальність, інформація.**

"Комп'ютерна" злочинність стала однією з міжнародних проблем, що зумовлено створенням міжнародних інформаційних систем, таких, наприклад, як мережа "Інтернет", яка об'єднує обчислювальні центри і системи більш як 70 країн і забезпечує обмін даними між різноманітними джерелами і користувачами, яких десятки мільйонів. В розвинених країнах "комп'ютерна" злочинність завдає величезних збитків власникам і користувачам автоматизованих систем, примушує їх витрачати значні кошти на розробку і впровадження програмних, технічних та інших засобів захисту від несанкціонованого доступу до інформації, її перекручення чи знищення. Останнім часом і в Україні спостерігається стрімке зростання злочинів, пов'язаних з втручанням в роботу автоматизованих систем, зокрема, в систему банківських електронних платежів. Як правило, втручання в їх роботу здійснюється з метою вчинення інших, більш тяжких злочинів: розкрадання майна; його вимагання під погрозою знищення чи спотворення інформації, яка обробляється чи зберігається в автоматизованих системах; ознайомлення з такою інформацією, її викрадення, знищення тощо.

Новий КК України від 05. 04. 2001 р. містить 3 статті, що передбачають відповідальність за вчинення так званих "комп'ютерних злочинів" – втручання до роботи автоматизованих електронно-обчислювальних машин (комп'ютерів, АЕОМ), їх систем та мереж: ст. 361, 362, 363 КК України.

Статтею 361 передбачена відповідальність за дві самостійні форми незаконного втручання в роботу автоматизованих електронно-обчислювальних машин (комп'ютерів), їх систем чи комп'ютерних мереж (КС): 1) незаконне втручання в роботу КС, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації; 2) розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних