**Реферат на тему:**

**Тероризм та інформаційні технології**

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.

Наша країна історично має вагомі внески у цій галузі. Наприклад, усім відомо про створення саме в Україні у 1949 р. першої в Європі електронно-обчислювальної машини С.А. Лебедєва (так звана мала електронно-обчислювальна машина - МЕОМ). На жаль, у дев'яності роки в силу відомих історичних подій, в Україні як і в усіх країнах СНД, був певний спад у даному напряму.

У даний час у нашій країні відзначається інтенсивне використання як готових закордонних програмних продуктів, так і виробництво вітчизняних. Збільшується кількість користувачів глобальної комп’ютерної мережі Internet (більше 1 млн.) та кількість провайдерів, хоча значна їхня частина знаходиться в Києві. На форумі HI-TECH індустрії, що проходив у Києві 21 лютого цього року, були відзначені наступні тенденції вітчизняної комп’ютерної індустрії: перехід від кодування по специфікаціях до надання бізнесів-рішень і готових продуктів на зовнішньому ринку; розвиток інвестиційних процесів у сфері розробки програмного забезпечення (ПЗ); початок реальної протидії правопорушенням у сфері інтелектуальної власності (ліцензійне використання ПЗ); формування нових компаній, як основна ознака становлення української індустрії програмного забезпечення (за даними Держкомстату України 56 українських компаній зареєстрували іноземні інвестиції на суму 7,616 млн. грн.); зростання конкурсу на вступних іспитах у вузах відповідного профілю - досягнув рівня 1991 року - близько 7 абітурієнтів на місце [1].

Однак, зазначені прогресивні досягнення мають і зворотний бік медалі. Як відомо, з поширенням використання інформаційних технологій в 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, використанні 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, поширені у банківсько-кредитній сфері, де активно використовуються автоматизовані системи [2]. Слід зазначити, що в Україні ріст комп'ютерних злочинів відповідає світовій тенденції, що полягає в пропорційності росту даного виду правопорушень масштабам використання засобів обчислювальної техніки. Особливе занепокоєння викликають факти використання нових інформаційних технологій терористичними групами. У січні 2002 року на території аеропорту м. Одеси пролунав вибух у кафе. Одночасно до начальника аеропорту надійшло повідомлення електронною поштою з вимогою виплати одного мільйону гривень та детальними вказівками щодо подальших дій, включаючи використання засобів масової інформації для реклами терористичної групи "Піночет". Зокрема сповіщалося, що на літаку з пасажирами, який щойно взяв курс в одну з європейських держав, знаходиться вибуховий пристрій з складною системою контролю (дистанційне управління з землі, самоліквідація при відсутності такого контролю, залежність від висоти польоту та ін.). У випадку невиконання вказівок, літак погрожували підірвати, а начальника аеропорту ліквідувати. Для передачі викупу за життя пасажирів пропонувалося використати систему Інтернет-банкінгу одного з комерційних банків України.

Внаслідок проведення оперативно-розшукових заходів, в першу чергу з залученням фахівців відділу по боротьбі з правопорушеннями у сфері високих технологій ДСБЕЗ МВС України, зловмисника вдалося виявити і нейтралізувати. Ним виявився колишній військовий, який захотів розпочати новий "бізнес".

гідно Кримінального кодексу України терористичним актом вважається "застосування зброї, ... вчинення дій, які створюють небезпеку для життя чи здоров'я людини або заподіюють значну майнову шкоду чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення або з метою впливу на прийняття рішень чи вчинення або не вчинення дій органами державної влади чи органами місцевого самоврядування, ... або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів терориста". На Самміті Тисячоліття у вересні 2000 року в Нью-Йорку Президент України Л.Д. Кучма у своїй доповіді на пленарному засіданні відмітив, що "роль зброї, здатної завдавати нищівних ударів по безпеці народів і держав, переходить до такого величного творіння людського розуму, як комп’ютер" і виступив з ініціативою про розробку Міжнародної конвенції про боротьбу з комп’ютерним тероризмом [3].

Кібертероризм пов’язаний з діяльністю екстремістських організацій націоналістичного, релігійного, політичного характеру тощо. Спектр застосування засобів електронної зброї найрізноманітніший, особливо він стає небезпечним по мірі розвитку міжнародної системи Інтернет, інтеграції її з супутниковими та радіо зв’язком, стільниковою телефонією. У Шрі-Ланці в травні 1998 року "тигри звільнення Тамілу" вперше серед терористичних груп провели кібернетичну атаку, яка була спрямована проти посольств у столиці [4].

Надзвичайної шкоди кібератаки здатні завдати комп’ютерним системам на особливо важливих об’єктах, таких як системи управління повітряним флотом, атомних електростанцій, правоохоронних органів, медичного забезпечення тощо. Адже вони можуть завдавати збитків, що значно перевищують розміри від "традиційних" терористичних актів. А поєднані у часі теракти та кібератаки утворюють особливо небезпечний акумулятивний ефект.

Значної економічної шкоди, аж до повного знищення інформаційної інфраструктури, можуть завдавати, на перший погляд, безвинні комп’ютерні віруси. Випадки масового розповсюдження вірусів, атаки на інформаційні ресурси, отримання небажаної кореспонденції вже стають звичним явищем в українському сегменті мережі Інтернет. Як приклад, можна привести резонансне зараження 16 листопада 2001 року вірусом "Nіmda" комп'ютерної мережі Укртелеком (провідного оператора зв’язку в Україні). Вірусна атака серйозним чином вплинула на працездатність обчислювальної мережі Генеральної дирекції ВАТ "Укртелеком", яка налічує більше 700 комп'ютерів та десятки серверів. Як наслідок, це спричинило тимчасове відключення комп'ютерів від Інтернету, а також вивело з ладу систему корпоративної електронної пошти. За попередніми підрахунками, збитки від атаки складають більше 1млн. грн.

Поштовий комп’ютерний вірус SirCam "викрадав" документи з органів державної влади, в тому числі адміністрації Президента України. Відомі також спроби знищення офіційного web-сайту Президента України. У цьому аспекті слід відзначити, що розслідування злочинів, пов'язаних з розробкою шкідливих програм, досить складний процес і неможливий без тісного міжнародного співробітництва.

Боротьба з кібертероризмом вимагає насамперед відповідної правової бази, функціонування спеціальних підрозділів по боротьбі з комп'ютерною злочинністю, широкого співробітництва з громадськістю, державними, комерційними підприємствами, тісної міжнародної взаємодії.

У новому Кримінальному кодексі України, що вступив в дію 1 вересня 2001 року, передбачена відповідальність за комп'ютерні злочини. Зокрема, у розділі XVI Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж передбачені наступні статті: ст. 361. Незаконне втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж; ст. 362. Використання, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем; ст. 363. Порушення правил експлуатації автоматизованих електронно-обчислювальних систем.

Водночас, існують певні питання щодо практичного використання XVI розділу КК у правоохоронній діяльності [6]. Як відомо, особливістю комп'ютерних злочинів, які вчиняються через Internet, є відсутність кордонів, що ускладнює розслідування і затримку правопорушників. Розуміючи яке значення в цьому зв'язку має тісне міжнародне співробітництво та уніфікація відповідного законодавства, Україна 23 листопада 2001 року підписала разом з 30 іншими країнами Європейську Конвенцію про кіберзлочини. 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 "комп'ютерному тероризму", 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. N 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" [7].

Сьогодні боротьба з комп'ютерними злочинами ведеться створеним у 2001 році Управлінням по боротьбі зі злочинами в сфері високих технологій при МВС України. За час функціонування підрозділом порушено 40 кримінальних справ (для порівняння до створення такого підрозділу в 2000 році було порушено 7 кримінальних справ по ст. 198-1 Кримінального кодексу, що діяв раніше). У той же час, приймаючи до уваги, що дозволений законом моніторинг систем зв'язку є одним з важливих засобів захисту національної безпеки і розслідування тяжких злочинів у відповідності до Резолюції Ради ЄС від 17 січня 1995 року "Про законний моніторинг телекомунікацій" (96/С 329/01), органам правопорядку необхідно здійснювати постійний моніторинг телекомунікацій у реальному часі. Службові дані, що мають відношення до повідомлень, також повинні надаватися в реальному часі. Якщо надати дану інформацію в реальному часі немає можливості, то вона повинна бути отримана максимально швидко після закінчення з'єднання для передавачі розмови, що перехоплюються, у відповідний моніторинговий центр.

Разом з тим, у зв’язку з міжнародним характером кіберзлочинів, актуальною залишається взаємодія правоохоронних органів різних країн з метою кримінального переслідування злочинців – адже саме кіберторористи частіше всього користуються відсутністю кордонів та митних служб у кіберпросторі. У зв’язку з викладеним, невідкладним завданням на сьогодні є створення Міжвідомчого центра по боротьбі з комп'ютерними злочинами, 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 оперативної допомоги жертвам, 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 МЦКБКЗ не виділити достатніх фінансово-матеріальних ресурсів – завтра втрати економіки держави від комп’ютерної злочинності будуть набагато більшими.

У цілому, основні напрям щодо протидії комп’ютерній злочинності, у тому числі і кібертероризму знайшли своє відображення в відображення у проекті Концепції стратегії і тактики боротьби з комп'ютерною злочинністю в Україні, яка розроблена у Міжвідомчому науково-дослідному центрі з проблем боротьби з організованою злочинністю та розміщена на сайті http://mndc.naiau.kiev.ua . Зазначене дозволить підтримувати в Україні необхідний рівень інформаційної безпеки, сприяти входженню нашої держави до світового інформаційного суспільства з усіма його перевагами.

**Список використаної літератури:**

1. В. Спиридонов Украинская индустрия ПО: достижения, проблемы, перспективы // http: www.bezpeka.com.

2. Б.Романюк, М.Гуцалюк Інтернет і злочин // Міліція України. – 2001. - № 11. – С. 22-23.

3. Виступ Президента України Леоніда Кучми на пленарному засіданні Генеральної асамблеї ООН // Крок. – 2000. вересень. - № 17-18. – С. 2.

4. International Police Review. – 1998. – November/December.

5. О. Реріх Вірус поцупив у Кучми секретний розклад // Дзеркало тижня. – 2001. - № 29(353).

6. М. Гуцалюк Кримінальний кодекс та комп’ютерна злочинність // Новий Кримінальний кодекс України: питання застосування і вивчення. Матер. міжнар. наук.-практ. конф. [Харків] 25-26 жовт. 2001 р. – К. = Х.: "Юрінком. Інтер", 2002, - С. 163-166.

7. Постанова КМ України від 14 грудня 2001 р. N 1694 Про затвердження Програми реалізації положень Варшавської конференції щодо спільної боротьби проти тероризму.