Бабич О. О.,
студент 5 курсу, 7 групи, Інститут прокуратури та кримінальної юстиції Національного університету ім. Ярослава Мудрого

ДО ПРОБЛЕМИ КІБЕРЗЛОЧИННОСТІ

Анотація: розглянуто деякі проблемні питання у сфері запобігання кіберзлочинності.
Abstract: Some problems in the field of cybercrime prevention were considered.
Ключові слова: кіберзлочинність, кібербезпека, кіберзлочинець, кібертероризм, комп`ютерні мережі.
Keywords: cybercrime, cyber security, cybercrime, cyberterrorism, computer networks.

У сучасному світі все більше виробництв і послуг спираються на інформаційні технології. Виробництво і постачання енергії, очищення і постачання питної води, керування транспортом, освітлення міст, зв'язку, доступ людей до інформації, охорона здоров'я, оплата товарів і послуг, волевиявлення під час виборів і референдумів, і навіть електронне урядування – все це реалії нашого життя. Ми залежимо від безперервності та коректності функціювання комп'ютерних систем об’єктів критичної інфраструктури, і атаки з боку та засобами кіберпростору на такі системи спричиняють реальні загрози для безпеки людей і суспільства. Частіше за все кіберзлочинність носить латентний характер тому вкрай важко виділити ознаки особи злочинця який завдає шкоду охоронюваним законом суспільним правам та свободам.

На мою думку, найбільшою проблемою у сфері кібербезпеки є недостатнє правове регулювання цього питання на міжнародному рівні. Так, на сьогодні існує лише один міжнародний нормативно правовий акт у цій сфері – це Конвенція про кіберзлочинність, яка була підготовлена та представлена на підпис 23 листопада 2001 року. З року в рік проводиться дедалі більше конференцій, круглих столів з питань кібербезпеки, однак вони приводять лише до поодиноких угод між країнами у цій сфері. Провідні держави світу витрачають чималі кошти зі своїх бюджетів задля запобігання та виявлення кіберзлочинів, проте кіберзлочинці якщо не випереджають то йдуть в ногу з спеціально створеними органам, що протидіють їм.

Історії відомий випадок коли у 1998 році 12-річний хакер проник у комп’ютерну систему, яка контролювала водоспуск води дамби Теодора Рузвельта в Арізоні. Небезпека його дій

полягала у тому, що у разі відкриття зливних воріт дамби вода могла затопити міста із загальною чисельністю населення у 1 млн. осіб. Саме після цього випадку з'явився такий термін як «кібертероризм». Взагалі майже усі види кіберзлочинів почали з'являтися у 90-ті роки минулого століття. Взагалі під поняттям «кіберзлочинність» розуміють сукупність злочинів, що вчиняють у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, ком'ютерних мереж і комп'ютерних даних. Виходячи з цього поняття можна зрозуміти, що такі злочини вчиняються у кіберпросторі за допомогою комп'ютерної техніки, а специфіка використання такого обладнання передбачає доволі високий освітній рівень, саме тому серед кіберзлочинців найчастіше зустрічаються люди з вищою або середньою спеціальною освітою. Дослідники стверджують, що віковий діапазон кіберзлочинців від 11 до 45 років. 11 річні правопорушники займаються злочинами з використанням телефонних мереж, кредитних карток та автоматів з видачі готівки. Злочинці у старшому віці займаються хакерством та шпигунством з використанням комп'ютерних систем. Зазвичай усі ці злочини вчиняються із корисливих мотивів. Характерною особливістю кіберзлочинців є нестандартність мислення і поведінки, обережність та уважність [1, с. 5].

Кіберзлочинці це «головна біль» правоохоронних органів, особливо в тих державах де урегулюванню проблеми кібербезпеки приділяється мало уваги, де відсутні спеціальні, окремо створені органи, адже ці злочини вкрай важко виявити. Кіберзлочинність і надалі буде залишатися великою проблемою тих держав, де не буде врегулювана вся діяльність, пов'язана з використанням комп'ютерних систем. Однак варто зазначити, що деякі держави світу приділяють достатню увагу цьому питанню, проте роблять вони це у власних інтересах і замість того, щоб боротися з кіберзлочинністю самі стають на вершині цієї злочинної піраміди. Наприклад, за даними ФБР на сьогоднішній день армія хакерів КНР складає близько 180 тисяч осіб, які щорічно здійснюють близько 90 тисяч атак проти комп'ютерів Міністерства оборони США. Варто зазначити, що до кібервійськ КНР входять не лише спеціально підготовлені особи, а й цивільні хакери, співробітники IT-компаній, які на замовлення держави здійснють шпигунство та кібератаки на різні підприємства, установи та організації. Кіберкомандування США (U.S Cyber Command) налічує штат у 30 тисяч осіб діяльність яких нічим не відрізняється від китайських колег. З вищенаведеного можна зробити висновок, що в той час коли більшість держав світу намагається завадити розвитку кіберзлочинності, провідні держави на офіційному рівні санкціонують діяльність кіберзлочинців та надають їм засоби для діяльності у власних інтересах та для ведення «кібервійн». Через цю діяльність держав кіберзлочинність характеризується латентністю, адже про вчинення злочину відомо правоохоронним органам, проте вони не вчиняють дій до його розслідування [2, с. 5].

До недавніх пір кіберзлочинності була притаманна певна особливість – злочини здійснювались індивідуально, однак дедалі частіше фіксуються випадки вчинення кіберзлочинів у складі організованих злочинних угрупувань. За статистикою 62% таких злочинів вчиняються у складі групи, інші 38% індивідуально.

Характерною ознакою злочинців, що діють у віртуальному просторі є їх технічне оснащення. Професійні хакери є добре оснащеними тому їх діяльність дуже важко виявити, діяльність тих осіб що оснащені досить слабко виявити легше, тому вони вчиняють незначні злочини з використанням ком'ютерних систем, щоб нести незначну відповідальність [3, с. 174–175].

Кіберзлочинцем може бути будь-хто з нашого оточення, наприклад, в Україні за даними Української антипіратської асоціації станом на січень 2017 р. кількість користувачів піратських сайтів з онлайн відео посиланнями (streaming video link sites) склала 59,6 млн. користувачів. Зважаючи на таку негативну статистику, державні органи України почали діяти і результатом цієї діяльності на сьогодні є прийнятий в жовтні 2017 року Закон України «Про основні засади кібербезпеки в Україні», а також розроблена Радою національної безпеки і оборони України «Стратегія кібербезпеки України». В цих нормативно-правових актах розкриті усі терміни пов'язані з використанням кіберпростору, визначені суб'єкти забезпечення кібербезпеки, зазначені пріоритети та напрями забезпечення кібербезпеки в Україні. На мою думку, прийняття наведених вище нормативно-правових актів є позитивним явищем для нашої країни, що вплине на стан кібербезпеки в Україні в майбутньому.

Список використаних джерел:

1. Дзюндзюк Б. В. «Поява і розвиток кіберзлочинності» [Електронний ресурс] / Б. В. Дзюндзюк, В. Б. Дзюндзюк. – Режим доступу: www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf/
2. Дубов Д. В. Кібербезпека: світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – Київ: НІСД., 2011. – 30 с.
3. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Дніпропетровськ. - №3 2016. – 172 – 177с.

Міністерство освіти і науки України

**Національний юридичний університет
імені Ярослава Мудрого**

ЗЛОЧИННІСТЬ У ГЛОБАЛІЗОВАНОМУ СВІТІ

Матеріали XVI Всеукраїнської кримінологічної конференції для студентів, аспірантів та молодих вчених

(м. Харків, 12 грудня 2017 р.)

За загальною редакцією
професора *А. П. Гетьмана* і професора *Б. М. Головкіна*

Харків
«Право»
2017

УДК 343.9.01:005.44
ББК 67.61я431
З-68

Злочинність у глобалізованому світі : матеріали XVI Всеукр.
З-68 кримінол. конф. для студентів, аспірантів та молодих вчених (м. Харків, 12 груд. 2017 р.) / за заг. ред. А. П. Гетьмана і Б. М. Головкіна. – Харків : Право, 2017. – 420 с.

ISBN 978-966-937-307-6

ISBN 978-966-937-307-6