

КІБЕРЗЛОЧИННІСТЬ: ПОТЕНЦІЙНА ЧИ РЕАЛЬНА ЗАГРОЗА ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВУ?

Ключові слова: кіберзлочинність, комп'ютерний вірус, інформація, протидія.

Keywords: cybercrime, computer virus, information, opposition.

Анотація: Розглянуто природу кіберзлочинності, основні джерела небезпеки та наслідки, що спричиняються. Розкрито реальну загрозу кіберзлочинів на прикладі нещодавніх подій.

Annotation: The nature of cybercrime, the main sources of danger and the consequences that are caused is considered. The real threat of cybercrime is revealed on the example of recent events.

Сучасний розвиток інформаційно-комп'ютерних технологій стрімко зростає. Неможливо уявити наше життя без гаджетів з вільним доступом до мережі Internet. Так, кількість користувачів «світової павутини» постійно збільшується, а комп'ютерні програми, що забезпечують такий доступ постійно розробляються або оновлюються, враховуючи потреби споживача. Особа, яка користується послугою інтернет-банкінгу або онлайн магазину, може навіть і не підозрювати, що в цей самий час відбувається злочин, шляхом несанкціонованого доступу до її персональних даних, або використання коштів на банківському рахунку в інтересах кіберзлочинця.

Дійсно мережа Internet створила для людства безкордонні можливості реалізації його потреб, значно скоротила час для виконання операцій, що донедавна потребували великих людських, матеріальних та часових затрат. Але чи є така зручність запорукою безпеки?

Голіна В.В. зазначає, що обговорення цього питання серед кримінологів актуалізувалося понад 17 років тому. І вже тоді вчені констатували, що зростання комп'ютерних протиправних засіхань перестало бути далекою перспективою. Проблема комп'ютерної злочинності набуває яскраво вираженого міжнародного характеру. Виникає необхідність міжнародного співробітництва, створення спеціалізованих підрозділів або цілеспрямованих сил, що володіють професійними знаннями, досвідом, владними повноваженнями для найкращого вирішення завдань в цій сфері [1].

Зважаючи на те, що Україна, яка перебуває в постіндустріальному періоді розвитку та процесі лібералізації економіки, проблема кіберзлочинності актуалізується з кожним роком [2].

Важко не погодитись із позицією дослідників, адже зовсім нещодавно, влітку 2017 року, українські підприємства зазнали найбільшої кібер атаки з боку вірусу «Петя А.». Внаслідок цього була паралізована робота багатьох провідних державних і комерційних підприємств, зокрема мережі крупних супермаркетів, державних банків «Мегабанк», «Ощадбанк» та інші. Ця атака

привела до справжнього хаосу та великих втрат капіталу, адже розробники вірусу висунули вимоги саме майнового характеру. У цій ситуації ми відчули усі прогалини вітчизняного законодавства щодо регулювання питання безпеки інформаційного простору України, та неспроможність новоствореного Департаменту кіберполіції Національної поліції України попередити такі атаки.

Зазначаючи проблемні питання законодавчого регулювання питання кібербезпеки в Україні слід відзначити такий підзаконний нормативний акт як Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року "Про Стратегію кібербезпеки України". Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Цей документ досить широко визначає проблемні аспекти кібербезпеки в Україні, основні напрямки діяльності системи правоохоронних органів для їх подолання. До того ж у прикінцевих положеннях зазначається необхідність урахування положень Стратегії при розробці нормативно-правових актів у сфері боротьби із кіберзлочинністю [3].

В силу Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 року та Закону України «Про національну поліцію» від 2 липня 2015 року було затверджено наказом Національної поліції від 10.11.2015 № 85 Положення про Департамент кіберполіції НП України, який є міжрегіональним територіальним органом Національної поліції України відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції [4].

На жаль, на сьогодні не можна з точністю сказати, що утворений Департамент функціонує належним чином та ефективно виконує покладені на нього завдання. На мою думку, це пов'язано із законодавчою неврегульованістю, адже проєкт Закону «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері» досі не прийнятий. А зважаючи на різку критику положень цього проєкту, не робиться спроб доопрацювати або переробити його. Ще одним чинником є брак фінансування, адже із розвитком інформаційних технологій необхідним є забезпечення Департаменту відповідним обладнанням та професійними кадрами.

Підсумовуючи вище викладений матеріал, слід зазначити, що на перший погляд безпечний кібер простір не є таким. Правоохоронні органи, комерційні та звичайні користувачі все частіше фіксують спроби втручання сторонніх в їх персональні дані з метою заволодіння і використання в особистих цілях. На жаль ця тенденція тяжіє до зростання, зважаючи на стрімкий технічний і програмний розвиток інформаційно-комп'ютерної сфери. Як правило, законодавець не в змозі своєчасно врахувати такий швидкий технічний прогрес, тому законодавство нашої країни потребує постійного вдосконалення, а відповідні правоохоронні органи повинні мати належне технічне, фінансове і кадрове забезпечення для ефективного функціонування і виконання покладених на них завдань. Тому, варто наголосити на тому, що кіберзлочинність є реальною загрозою, адже її наслідки пронизують усі сфери суспільного життя, та завдають руйнівних втрат.

Список використаних джерел:

1. Голина В.В. Проблеми в комп'ютерній преступності / В.В Голина, В.В. Пивоваров // Фінансова злочинність: зб.матеріалів Міжнар. наук-практ. семінару, Харків 12-13 лют. 1999 р. / редкол.: В.І. Борисов (голов. ред.) та ін.- Х.: Право, 2000. - с. 62.
2. Пивоваров В.В. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання / В.В. Пивоваров, С.Ю. Лисенко// Право і суспільство. – 2016. - №3, ч. 2.
3. Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року "Про Стратегію кібербезпеки України", № 96/2016.
4. Положення про Департамент кіберполіції НП України, затвердженого наказом Національної поліції від 10.11.2015 № 85.

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. Головкина*

Харків
«Право»
2017

УДК 343.9.01:005.44
ББК 67.61я431
3-68

Редакційна колегія:
проф. А. П. Гетьман;
проф. Б. М. Головкін;
канд. юрид. наук, доц. О. В. Ткачова,
канд. юрид. наук, ас. О. В. Таволжанський,
канд. юрид. наук, ас. Н. В. Сметаніна,
канд. юрид. наук, ас. К. Д. Кулик,
канд. юрид. наук, ас. О. О. Шуміло,
ст. лаб. К. С. Остапко

3-68 **Злочинність** у глобалізованому світі : матеріали XVI Всеукр.
кримінол. конф. для студентів, аспірантів та молодих вчених (м. Хар-
ків, 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

© Національний юридичний університет
імені Ярослава Мудрого, 2017
© Оформлення. Видавництво «Право», 2017