МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЯРОСЛАВА МУДРОГО

КАФЕДРА КРИМІНОЛОГІЇ
ТА КРИМІНАЛЬНО-ВИКОНАВЧОГО ПРАВА

ЗЛОЧИННІСТЬ ЯК СУСПІЛЬНА ПРОБЛЕМА ТА ШЛЯХИ ЇЇ ВИРІШЕННЯ В УКРАЇНІ

Матеріали Всеукраїнської студентської наукової конференції

(Харків, 4 листопада 2016 року)

У двох томах

За редакцією *А. П. Гетьмана, Б. М. Головкіна*

Том 2

Харків
«Право»
2016

УДК 343.988
ББК 67.9(4УКР)61
З-68

З-68 **Злочинність** як суспільна проблема та шляхи її вирішення в Україні : матеріали Всеукр. студ. наук. конф., м. Харків, 4 листоп. 2016 р. : у 2 т. / за заг. ред. А. П. Гетьмана, Б. М. Головкіна. – Т. 2. – Х. : Право, 2016. – 194 с.

ISBN 978-966-937-086-0
ISBN 978-966-937-088-4 (т. 2)

ISBN 978-966-937-088-4 (т. 2)
ISBN 978-966-937-086-0

дефолту. У 2008 р. Міжнародний валютний фонд виділив один з найбільших кредитів у розмірі 11 млрд дол. на підтримку економічного становища України [3].

Таким чином, унаслідок дій «білих комірців» у США щодо зловживання в економічній сфері була заподіяна шкода, яка розповсюдилася по усьому світу та негативно вплинула на економічну ситуацію в Україні.

У 2016 р. було розпочато кримінальне провадження щодо народного депутата Олександра Онищенка як організатора корупційної схеми розкрадання державних коштів під час видобутку та продажу природного газу в рамках договорів про спільну діяльність з ПАТ «Укргазвидобування», у результаті якої державі було завдано збитків на суму близько 3 млрд грн, а загальна вартість арештованого майна Онищенка складає близько 315 млн грн [4]. Не можна оминути увагою судовий процес щодо одного з найбагатших українців Дмитра Фірташа, який підозрюється у підкупі чиновників Індії та ухиленні від сплати податків на суму близько 50 млн дол. [5].

Завдання державних органів полягає в тому, щоб запобігати вчиненню таких злочинів та забезпечувати невідворотне покарання для тих, хто їх скоїв. Проте найгірше, коли інтереси «білих комірців» спеціально залишаються непомітними з боку державних органів, чий обов'язок стримувати злочинність та протидіяти їй.

Необхідно погодитися з думкою Едвіна Сазерленда щодо приділення недостатньої уваги та ігнорування злочинів, скоєних заможними верствами населення.

Таким чином, загальна характеристика осіб, які підпадають під термін «білий комірець», є такою: як правило, це люди з вищою освітою, гарною репутацією, які представляють середній та великий бізнес і мають високий соціальний статус.

Список літератури

1. Сатерленд Э. Являются ли преступления людей в белых воротничках преступлениями? / Эдвин Сатерленд // Социология преступности (современные буржуазные теории) : сб. ст. / отв. ред. Б. С. Никифоров. – М., 1972. – 368 с.
2. Financial Crimes Report 2010–2011 [Електронний ресурс]. – Режим доступу: https://www.fbi.gov/stats-services/publications/financial-crimes-report-2010–2011.
3. Меморандум, Міжнародний документ «Меморандум про взаєморозуміння між Урядом України та Урядом Сполучених Штатів Америки» від 10.11.2008 № 840_139 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/840_139.
4. Національне антикорупційне бюро України [Електронний ресурс]. – Режим доступу: https://nabu.gov.ua/novyny/genprokuror-pidpysav-pidozru-shchodo-oleksandra-onyshchenka.
5. Ольга Байвидович [Електронний ресурс]. – Режим доступу: http://ua.korrespondent.net/world/3320604-firtash-ne-vnis-zastavu-za-zvilnennia-i-perebuvaie-pid-areshtom-u-vidni.
6. Шостко О. Ю. Кримінологічні проблеми дослідження злочинів у сфері службової діяльності : матеріали наук.-практ. семінару / О. Ю. Шостко. – К. ; Х. : Юрінком Інтер, 2005. – С. 101–103.

Науковий керівник – д-р юрид. наук, проф. О. Ю. Шостко

М. В. Плеханов,
студент 16 групи 5 курсу Інституту прокуратури та кримінальної юстиції Національного юридичного університету імені Ярослава Мудрого, м. Харків

ДЕЯКІ АСПЕКТИ ТЕНДЕНЦІЙ РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

З початком нового тисячоліття суспільство зазнало стрімкого розвитку, особливо ми це побачили у сфері інформаційних технологій. На сьогодні навіть у країнах «третього світу» техно-

логії потрапили в кожен дім, та без них вже зараз неможливо уявити світ. З одного боку, використання сучасних телекомунікаційних мереж, сучасного обладнання, персональних комп'ютерів забезпечує феноменальний розвиток таких галузей, як медицина, освіта, правоохоронна діяльність, сфера надання банківських послуг і т. д., але, з іншого боку, створює суттєву загрозу в обличчі кіберзлочинності.

Актуальність цього питання демонструють прийняття Радою Європи «Конвенції про кіберзлочинність», відведення цілого розділу в Кримінальному кодексі України, розробка закону «Про кібернетичну безпеку України», який, на жаль, не був прийнятий, Указ Президента України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», який мав розробити питання інформаційної безпеки, посилити захист інформації, розробити нове, а також вдосконалити існуюче законодавство у сфері кібербезпеки, впровадити категоріально-понятійний апарат. Але чіткого визначення кіберзлочинності наше національне законодавство так і не отримало, а в кримінальному законодавстві воно взагалі не використовується. На мою думку, на цьому етапі розробки законодавства в цій сфері необхідно використовувати визначення, запропоноване у проекті «Стратегії забезпечення кібернетичної безпеки України», розробленої Національним інститутом стратегічних досліджень: «кібернетичний злочин (кіберзлочин) – передбачене кримінальним законом суспільно небезпечне винне діяння, що полягає в протиправному використанні інформаційних та комунікаційних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність» [1, с. 85–86].

Перейдемо до кримінологічної характеристики цієї групи злочинів. Найбільшою особливістю кіберзлочинів є їх латентність. На думку Б. М. Головкіна, рівень латентності цих злочинів сягає 90–95 %, тому статистичні дані не відбивають повною мірою ситуацію з кіберзлочинністю в Україні [2, с. 335].

Відповідно до статистичних даних, наданих Генеральною прокуратурою України, рівень злочинності у цій сфері за 2014 р. склав 418 зареєстрованих злочинів, за 2015 р. – 561, за 2016 р. (по вересень місяць) – 779, таким чином, ми можемо побачити бурхливий процес розвитку кіберзлочинності. Також важливим є те, що протягом останніх 3 років було обліковано понад 20 кібернетичних злочинів, учинених групою осіб, що вказує на підвищення рівня складності та небезпечності відповідних злочинів. Найбільшу питому вагу на 2014–2016 рр. складають злочини щодо несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, передбачені диспозицією ст. 361 КК України, – приблизно 80 %, ще приблизно 15–17 % складають несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України). Усі інші статті, передбачені у розділі «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», зустрічаються вкрай рідко.

Що стосується особи злочинця, то найчастіше кібернетичні злочини у 2016 р. вчиняли особи у віці від 18 до 39 років (понад 90 %). Особливим також є те, що понад 95 % злочинців мали вищу або професійно-технічну освіту, це вказує на збільшення досвідченості серед кіберзлочинців порівняно з минулими роками, так, на 2012 р. кількість злочинців у цій сфері з вищою освітою складала лише 77–78 %. Наостанок хочу звернути увагу на швидке зростання кількості жінок, які вчиняють кіберзлочини, якщо на 2012 р. їх кількість складала лише 15–18% від загальної кількості, то на 2016 р. ми маємо цифру 33%.

Таким чином, проаналізувавши статистичні дані за останні роки, я дійшов висновку, що кіберзлочинність отримує все більший розвиток, а відповідні кіберзлочини щодалі стають все більш складними та зухвалими, навіть незважаючи на те, що більшість даних неможливо отримати через дуже високий рівень латентності. Важливим та актуальним також є низький рівень законодавчого закріплення питань інформаційної безпеки та боротьби з кіберзлочинністю. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямом протидії кіберзлочинності я вважаю організацію взаємодії і координацію зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою, а також міжнародну співпрацю.

Список літератури

1. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. – К. : ВБ «Аванпост-Прим», 2012. – 214 с.
2. Кримінологія: Загальна та Особлива частини : підручник / В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська, О. В. Лисодєд та ін. ; за ред. В. В. Голіни і Б. М. Головкіна. – Х. : Право, 2014. – 440 с.

Науковий керівник – канд. юрид. наук, асист. О. В. Новіков

Д. А. Познякова,
студентка 6 групи 5 курсу Слідчо-криміналістичного інституту
Національного юридичного університету імені Ярослава Мудрого,
м. Харків

КІБЕРЗЛОЧИННІСТЬ ТА ЗАСОБИ ПРОТИДІЇ

Комп'ютерний вік приніс нові можливості для злодіїв і шахраїв. Реакцією злочинців на виявлені нові можливості, а також залежність сучасного суспільства від технологій стала поява кібершахрайства та кіберзлочинності.

Кіберзлочинці шантажують компанії, виявляючи слабкі місця в їх мережах. Вони займаються розкраданням комерційної таємниці компаній через прогалини в їх системах безпеки. Зростають шахрайство в системах інтернет-банкінгу, несанкціонований переказ грошових коштів, проводяться атаки комп'ютерних мереж роздрібних магазинів, страхових компаній, банків і філій з метою розкрадання баз даних з інформацією банківських карт клієнтів. Швидкими темпами зростає напрям, пов'язаний з крадіжкою персональних даних, розповсюдженням комп'ютерних вірусів, викраденням комп'ютерної інформації та порушенням правил експлуатації автоматизованих електронно-обчислювальних систем – це далеко не повний перелік подібних злочинів.

В Україні кіберзлочинність регулюють такі нормативно-правові акти: Конвенція про кіберзлочинність, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Кримінальний кодекс України.

Основною причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість. Величезні суми грошей з'являються в кишенях злочинців у результаті окремих великих афер, не говорячи вже про невеликі суми, які йдуть потоком. Друга причина росту кіберзлочинності як бізнесу – те, що успіх справи не пов'язаний з більшим ризиком. У реальному світі психологічний аспект злочину припускає наявність деяких коштів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв, будь то окремі люди або цілі організації, яких вони вибрали для атаки. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше.

Останнім часом рівень кіберзлочинності швидко зростає в Україні. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Росією, Бразилією, Китаєм та меншою мірою – Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування [1].

Аналіз даних статистичної звітності за останні п'ятнадцять років свідчить про тенденцію стабільного та стрімкого зростання рівня кіберзлочинів. Їх середньорічний рівень в інтервалі 2002–2016 рр. склав 225 злочинів. У той же час лише у 2016 р. абсолютна кількість зареєстрованих кіберзлочинів сягнула близько 600, що на 35% більше, ніж у 2015 р.

На підставі аналізу та узагальнення експертних оцінок, матеріалів наукових досліджень встановлено, що рівень латентності кіберзлочинів складає близько 95%, що дозволяє віднести їх до категорії високолатентних. Серед факторів їх латентності виділено три основні групи: 1) фактори, що обумовлюють природну латентність, у силу яких про вчинений кіберзлочин відомо лише самому винному; 2) фактори, пов'язані з негативною поведінкою жертви (очевидців) злочину та їх