є намір особи розпорядитися викраденим, як власним, на свій розсуд – використати особисто, передати іншим особам (не лише близьким), знищити тощо. Отже, злочинець може використати викрадене як для задоволення індивідуальних потреб (не лише життєво потрібних), так і для потреб іншої особи чи групи осіб. Головним, на наш погляд, тут є саме незаконний характер дій винного щодо отримання та подальшого розпорядження майном, власником якого він не являється.

Саме тому, вважаємо за доцільне запропонувати визначення корисливого мотиву, як прагнення задовольнити індивідуальну потребу винного або іншої особи шляхом завідомо протиправного, передбаченого кримінальним законом заволодіння чужим майном чи чужими майновими правами, або шляхом звільнення від майнових зобов'язань та зменшення витрат. На наш погляд, таке доповнення більш детальніше розкриває основні ознаки та соціальну сутність корисливих мотивів злочинів та за умов подальших ґрунтовних наукових досліджень буде сприяти проникненню в природу злочинності в цілому.

Література

1. Албул С.В. Корисливо-насильницькі злочини відносно іноземців в Україні: кримінологічний аналіз: монографія / С.В. Албул. – Одеса: Видавець Букаєв В.В., 2009. – 144 с.

2. Албул С.В. Кримінальне право України : навч.-метод. посіб. / С.В. Албул, Д.О. Балабанова, А.А. Березовський та ін.; за ред. В.О. Тулякова. – Одеса : Фенікс, 2010. – 456 с.

3. Бабенко А.М. Запобігання злочинності в регіонах України: концептуально-методологічний та праксеологічний вимір: монографія / А.М. Бабенко. – Одеса: ОДУВС, 2015. – 416 с.

4. Зелинский А.Ф. Корысть: опыт криминологического и психологического анализа // Государство и право. – № 3. – 1993. – С. 23-28.

5. Зелинский А.Ф. Криминальная психология. научно-практическое издание. – Х.: Юринком Интер, 1999. – 212 с.

6. Лунеев В.В. Преступность XX века. Мировой криминологический анализ. – М.: Норма, 1999. – 856 с.

7. Савченко А.В. Класифікація мотивів злочину // Режим доступу: http://www.naiau.kiev.ua

8. Сайт Корысти // Режим доступу: http://www.korist.ru

9. Словарь по этике / Под ред. И.С. Кона. – 4-е изд. – М.: Политиздат, 1981. – 388 с.

10. Тищенко В.В. Корыстно-насильственные преступления: криминалистический анализ: Монография. – Одесса: Юрид. л-ра, 2002. – 258 с.

11. Фуко М. Наглядати і карати. – К.: Основа, 1998. – 392 с.

Албул С.В.
кандидат юридичних наук,
доцент
перший проректор ОДУВС

Холостенко А.В.
кандидат юридичних наук,
доцент
директор ННІЗДН ОДУВС
Надійшла до редакції: 16.11.2015

УДК 343.123.12

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ – ПРОБЛЕМА ТРАНСНАЦІОНАЛЬНОГО МАСШТАБУ

Андрусенко С. В.

У статті розглянуті питання поширення кіберзлочинності на транснаціональному рівні та протидія правоохоронних органів різних держав світу в боротьбі з міжнародною кіберзлочинністю.

***Ключові слова**: комп'ютери, злочин, транснаціональність, співробітництво, взаємодія, кіберзлочинність, правоохоронні органи.*

В статье рассмотрены вопросы распространения киберпреступности на транснациональном уровне и противодействие правоохранительных органов различных государств мира в борьбе с международной киберпреступностью.

***Ключевые слова**: компьютеры, преступление, транснациональность, сотрудничество, взаимодействие, киберпреступность, правоохранительные органы.*

The article focuses on the cybercrimes' spreading at the transnational level and law enforcement agencies' reaction of different countries in the world onto the combating international cybercrimes.

Keywords: computers, crime, transnationality, cooperation, interaction, cybercrimes, law enforcement agencies.

Стрімкий розвиток інформаційних і телекомунікаційних технологій призвів до того, що сучасне суспільство значною мірою залежить від управління різними процесами за допомогою комп'ютерної техніки – електронної обробки, зберігання, доступу й передачі інформації. Використання інформаційних технологій розширює свою дію на всі нові сфери людської діяльності: від контролю за повітряним і наземним транспортом до вирішення проблем національної безпеки. Інформація як один з основних елементів цього процесу відіграє все більш істотну роль як у житті окремої людини, так і в житті всього суспільства й кожної держави. У зв'язку з цим інформаційна безпека є однією зі складових національної безпеки держави [1].

Розширення виробництва технічних засобів і сфери застосування комп'ютерної техніки, розвиток інформаційних технологій, а головне – наявність людського фактору у виді задоволення власних амбіцій чи з корисливою метою породили новий вид суспільно небезпечних діянь, в яких неправомірно використовується комп'ютерна інформація або вона сама стає об'єктом зазіхання. Подібно багатьом революційним технологіям глобальна мережа Internet несе із собою величезний потенціал як для прогресу, так і для зловживань.

Технологічна еволюція одночасно з позитивом породжує нові проблеми й загрози інформаційній безпеці

держав, посилюючи існуючи. В умовах глобальної конкуренції інформаційний тиск стає дієвим та ефективним методом вирішення міждержавних конфліктів. Усе інтенсивніше використовуються можливості глобальних інформаційно-комунікаційних мереж екстремістськими й терористичними організаціями для пропаганди і популяризації своєї ідеології, розповсюдження радикальних ідей, залучення все більшого числа однодумців та їх навчання, підтримки контактів і фінансування. Інформаційні системи держав піддаються загрозі комп'ютерних атак, які є одним зі способів терористичної діяльності. Організовані транснаціональні злочинні групи все активніше використовують сучасні інформаційно-комунікаційні технології в кримінальних цілях. Змінюється динаміка кіберзлочинності – для неї характерна стійка тенденція зростання [5].

Основною проблемою боротьби зі злочинністю в мережі Інтернет є транснаціональність самої мережі й відсутність механізмів контролю, необхідних для правозастосування. Мережа Інтернет створювалася технологічно як структура без ієрархії та без якогось "ядра", зруйнувавши які можна було б паралізувати її роботу, і навряд чи хтось міг уявити масштаби розвитку проекту, спочатку не призначеного для широкої аудиторії. Основною метою створення цієї мережі була стійкість до атак ззовні, і важко було передбачити подальший масштаб її розвитку, її економічну та соціальну роль у майбутньому. Саме відсутність розроблених механізмів контролю мережі зсередини вкупі з її доступністю й легкістю використання стало однією з глобальних проблем інформаційного співтовариства: децентралізована структура мережі та відсутність національних кордонів у кіберпросторі зумовили можливості для росту злочинності та на роки відклали розроблення механізмів правового та соціального контролю у сфері використання інформаційних мереж для вчинення злочинів [4].

Особливість кіберзлочинів полягає в їх високій латентності, появі нових, витончених способів учинення злочинів, доказування яких сильно ускладнено відсутністю необхідних правових, організаційних і технічних інструментів. Тому боротьба з кіберзлочинністю обумовлює потребу відповідного оперативного реагування, спільних скоординованих дій правоохоронних органів.

Атаки в мережі, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, корпоративне шпигунство та поширення дитячої порнографії – ось тільки деякі зі злочинів, що вчиняються в мережі Internet.

Такі протиправні діяння вже сьогодні складають для нашої держави, як і для багатьох інших країн світу, певну суспільну небезпеку, реально загрожуючи інформаційній безпеці – складовій національної безпеки.

Національна інфраструктура держави вже сьогодні щільно пов'язана з використанням сучасних комп'ютерних технологій. Щоденна діяльність банківських та енергетичних систем, керування повітряним рухом, транспортна мережа, навіть швидка медична допомога перебувають у повній залежності від надійної й безпечної роботи автоматизованих електронно-обчислювальних систем.

На теперішній час можна сміливо прогнозувати подальше зростання залежності життєдіяльності національної інфраструктури від процесів інформатизації та входження України в єдиний інформаційний простір, поширення криміногенних процесів, пов'язаних з протиправним використанням комп'ютерних технологій.

Розвиток науково-технічного прогресу, пов'язаний з упровадженням сучасних інформаційних технологій, призвів до появи нових видів злочинів, зокрема до незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж, викрадення, привласнення, вимагання комп'ютерної інформації, які узагальнені в небезпечному антисоціальному явищі, що отримало назву "кіберзлочинність" [3].

Поняття "кіберзлочинність" уперше з'явилось в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних. Кіберзлочинність (англ. cybercrime) – це поняття, яке охоплює комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо [2].

Основною метою кіберзлочинця є комп'ютерна система, яка керує різними процесами, і інформація, що циркулює в них. На відміну від звичайного злочинця, що діє в реальному світі, кіберзлочинець не використовує традиційну зброю – ніж і пістолет. Його арсенал – інформаційна зброя, всі інструменти, що використовуються для проникнення в мережі, злому й модифікації програмного забезпечення, несанкціонованого одержання інформації або блокування роботи комп'ютерних систем. До зброї кіберзлочинця можна додати: комп'ютерні віруси, програмні закладки, різноманітні види віддалених атак, що дозволяють отримати несанкціонований доступ до комп'ютерної системи. В арсеналі сучасних комп'ютерних злочинців не лише традиційні засоби, а й найсучасніша інформаційна зброя та обладнання, яке дає можливість вчиняти злочини проти любої країни світу, тому ця проблема вже давно перетнула кордони держав і стала проблемою міжнародного масштабу.

На теперішній час визначають основні категорії кіберзлочинців.

Інсайдери – особи, що мають доступ до внутрішньої інформації. Вони частіше всього настроєні негативно проти своїх роботодавців, інсайдер (працюючий або звільнений співробітник компанії) є потенційним злочинцем.

Хакери також складають велику небезпеку, іноді вони зламують мережі просто заради гострих відчуттів або заради завоювання авторитету в хакерських колах. Але нерідко вони зламують системи й з метою фінансової наживи та інших злодіянь. Як правило, хакери – прекрасні знавці інформаційної техніки, які мають неординарні здібності, тому їм не складно маніпулювати комп'ютерними системами на відстані.

Творці вірусних програм. Ще одним видом комп'ютерної злочинності є протиправне пошкодження комп'ютерної системи або мережі з метою порушення функціонування комп'ютерів або глобальних телекомунікаційних систем за допомогою вірусів. Творці таких програм складають на сьогодні серйозну загрозу для користувачів.

Кримінальні угруповання. Останнім часом спостерігається тенденція росту вчинення комп'ютерних злочинів кримінальними групами, що діють із метою викрадання грошових коштів, частіше всього з банківських установ.

Терористи. Терористичні організації все частіше використовують нові інформаційні технології та Internet зі злочинними намірами, поповнення коштів, проведення пропаганди або передачі секретної інформації.

Шахрайство в (за допомогою) Internet. Використання

Internet з метою шахрайства є, мабуть, сьогодні одним із найпоширеніших видів кіберзлочинів, з яким уже зіштовхнулися як приватні, так і державні структури всього світу.

Жодна держава сьогодні не здатна протистояти цьому злу самостійно. Нагальною є потреба активізації міжнародного співробітництва в цій сфері. Вагоме місце в такому співробітництві належить, безумовно, міжнародно-правовим механізмам регулювання. Але, зважаючи на те, що в сучасних умовах значна частка засобів боротьби з кіберзлочинами, як і з іншими злочинами міжнародного характеру, належить до внутрішньої компетенції кожної окремої держави, необхідно паралельно розвивати й національне законодавство, спрямоване на боротьбу з комп'ютерними злочинами, узгоджуючи його з нормами міжнародного права та спираючись на існуючий світовий позитивний досвід.

Безперечно, ефективне міжнародне співробітництво в боротьбі з кіберзлочинністю неможливо, якщо в законодавстві однієї країни діяння вважається злочином, а в іншій – кримінальної відповідальності за це діяння не передбачено. Відсутність однаковості в національному кримінальному законодавстві країн може негативно вплинути на розвиток методів ефективної боротьби з кіберзлочинністю – явищем, для якого не існує державних кордонів. Наявність глобальних інформаційних мереж стирає межі інформаційного простору, а "віртуальні" кордони між державами легко перетинаються кіберзлочинцями, які орудують в будь-якому місці кіберпростору, незалежно від юрисдикції держав, з допомогою комп'ютера й доступу в Інтернет. Ефективне протистояння кіберзлочинності, враховуючи її транскордонний характер, неможливе, якщо розслідування злочинів, видача правопорушників, їх переслідування в суді ускладненні або взагалі нездійсненні через невідповідності національного кримінального законодавства окремих країн. Фактично, ці відмінності огороджують кіберзлочинців від переслідування, слугуючи своєрідним "бар'єром", дозволяють уникнути відповідальності, залишаючи безкарними їх діяння [5; 6].

Також кваліфікована кадрова забезпеченість сфери інформаційної безпеки є одним з основних факторів, який впливає на результативність боротьби з кіберзлочинністю. Крім цього, необхідне вдосконалення процесів і методики навчання, підвищення кваліфікації фахівців, зайнятих у сфері забезпечення інформаційної безпеки та боротьби з кіберзлочинністю.

Для ефективної протидії кіберзлочинності потрібно правове забезпечення інформаційної сфери на державному рівні.

На сучасному етапі важливу роль у боротьбі з кіберзлочинністю відіграють спеціалізовані міжнародні угоди. Так, у ряді міжнародних документів визнано, що кіберзлочинність сьогодні загрожує не тільки національній безпеці окремих держав, а й безпеці людства та міжнародному порядку [7, с. 3]. Стурбованість міжнародного співтовариства щодо розвитку кіберзлочинності знайшла відображення, зокрема, у таких міждержавних угодах, як Резолюція Ради ЄС "Про законний моніторинг телекомунікацій" (96/З 329/01) від 17 січня 1995 р. та Конвенція Ради Європи "Про кіберзлочинність" від 23 листопада 2001 р., Бангкокська декларація з попередження злочинності та кримінального правосуддя (2005 р.), Бухарестська декларація про міжнародне співробітництво в боротьбі з тероризмом, корупцією і транснаціональною організованою злочинністю (2006 р.). У цих документах йдеться про спільне протистояння кіберзлодіям, шляхом прийняття відповідних законодавчих актів, які не будуть суперечити ні законам окремої держави, ні пунктам договорів, які ратифікувала ця держава.

Що стосується України, слід відмітити такі негативні чинники, що стримують активну боротьбу з кіберзлочинами й не дозволяють нашій державі на рівноправній основі включитися у світове інформаційне суспільство:

- відсутність достатньої державної фінансової підтримки фундаментальних і прикладних вітчизняних досліджень у сфері попередження й боротьби з кіберзлочинністю;
- практично відсутній розвиток вітчизняного виробництва конкурентоспроможних засобів інформатизації і зв'язку, їх захисту;
- інформатизація державних і комерційних структур здійснюється переважно на базі закордонної технології та комп'ютерної техніки (стратегічна технічна і технологічна залежність від інших держав);
- недостатні професійні знання працівників правоохоронних органів (особливо МВС) у сфері боротьби з інформаційними злочинами.

Таким чином, кіберзлочинність – це проблема, з якою зіштовхнулась планета у 21 столітті і яка обіцяє рости та поглинати все більше коштів. Незважаючи на всі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників і зменшуючи вміст кишень пересічних громадян. Тому сьогодні особливо важливо переглянути всі існуючі заходи та активно розробляти нові, що принесуть більшу користь і надійніший захист від кіберзлочинців.

Ефективний контроль за кіберзлочинністю вимагає більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності.

Література

1. Лісайчук А.А. Проблеми боротьби із кіберзлочинністю на міжнародному рівні // Матеріали Міжнародної науково-практичної Інтернет-конференції "Актуальні проблеми країнознавчої науки", 09 жовтня 2014 (36). [Електронний ресурс]: https://internationalconference2014.wordpress.com/2014/10/09/проблеми-боротьби-із-кіберзлочинніс/

2. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби / Н.В. Савчук // Теоретичні та прикладні питання економіки: зб. наук. праць. – К.: Видавничо-поліграфічний центр "Київський університет", 2009. – Вип. 19. – С. 338-342.

3. Шакирова З.Х. Киберпреступность как масштабная проблема / З.Х. Шакирова // Современные научные исследования и инновации. – 2013. – № 8. – [Электронный ресурс]: http://web.snauka.ru/issues/2013/08/25764.

4. Ben-Itzhak Y. Organized Cybercrime [Electronic source] / Y. Ben-Itzhak // ISSA Journal. – October 2008. – Access mode: https://dev.issa.org/Library/Journals/2008/October/Ben-Itzhak-Organized%20Cybercrime.pdf.

5. Джансараева Р.Е., Аратулы К. Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ / Р.Е. Джансараева, К. Аратулы // Криминологический журнал ОГУЭП. – 2012. – № 3 (21). – [Электронный ресурс]: http://cj.isea.ru/pdf.asp?id=13289http://web.snauka.ru/issues/2013/08/25764.

6. Албул С.В. Кваліфікація комп'ютерних злочинів / Упорядники: В.О. Туляков, С.В. Албул, В.М. Підгородинський // ОНЮА – Одеса: Фенікс, 2007. – 28 с.

Андрусенко С.В.,
кандидат юридичних наук, доцент,
професор кафедри оперативно-розшукової
діяльності ОДУВС
Надійшла до редакції: 05.11.2015