МВС України

Харківський національний університет
внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Матеріали
Міжнародної науково-практичної конференції

м. Харків, 10 грудня 2013 р.

Харків 2013

УДК 343.98:[343.3/.7:004](477)(063)
ББК 67.9(4УКР)623.19я431
А43

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова – перший проректор з навчально-методичної та наукової роботи Харківського національного університету внутрішніх справ полковник міліції ***Головко Олександр Миколайович***;

Секретар – старший викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства капітан міліції ***Савчук Тетяна Іванівна***

Члени оргкомітету:

начальник факультету з підготовки фахівців для підрозділів слідства підполковник міліції ***Музичук Олександр Миколайович***; начальник факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми підполковник міліції ***Марков В'ячеслав Валерійович***; начальник відділу міжнародних зв'язків підполковник міліції ***Осятинський Станіслав Олександрович***; начальник кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства підполковник міліції ***Степанюк Руслан Леонтійович***; начальник кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми полковник міліції ***Тулупов Володимир Володимирович***; начальник кафедри кримінального процесу факультету підготовки фахівців для підрозділів слідства полковник міліції ***Юхно Олександр Олександрович***; начальник відділу матеріального забезпечення підполковник міліції ***Копаниця Олексій Вікторович***; начальник відділу організації наукової роботи підполковник міліції ***Мірошниченко Оксана Станіславівна***; начальник відділу організації служби підполковник міліції ***Тарасенко Віталій Миколайович***; начальник інформаційно-технічного відділу підполковник міліції ***Чесноков Вадим Валерійович***; начальник відділу зв'язків з громадськістю підполковник міліції ***Щербакова Ірина Василівна***; директор загальної бібліотеки ***Процких Тамара Олексіївна***

Друкується за рішенням оргкомітету відповідно до доручення Харківського національного університету внутрішніх справ від 10.09.2013 № 106.

Матеріали видано за підтримки Координатора проектів ОБСЄ в Україні.

Опубліковано Координатором проектів ОБСЄ в Україні в рамках «Проекту посилення боротьби з торгівлею людьми та кіберзлочинністю в Україні»

Україна, 01030, Київ, вул. Стрілецька, 16
www.osce.org/ukraine

ЗМІСТ

Шановні учасники конференції!

Від імені ректорату, Вченої ради Харківського національного університету внутрішніх справ і особисто від себе вітаю вас з початком роботи Міжнародної науково-практичної конференції «Актуальні питання розслідування кіберзлочинів»!

Конференція організована Харківським національним університетом внутрішніх за підтримки Головного слідчого управління МВС України, Управління боротьби з кіберзлочинністю МВС України, Державного науково-дослідного експертно-криміналістичного центру МВС України та Координатора проектів ОБСЄ в Україні.

Конференція викликала зацікавленість відомих вчених та працівників правоохоронних органів з України, Російської Федерації, Білорусі. Зокрема, правоохоронні органи представляють слідчі, судді, керівники підрозділів боротьби з кіберзлочинами системи МВС України, експертних підрозділів, фахівці Служби безпеки та Прокуратури України. Вищі навчальні заклади та науково-дослідні установи представляють вчені Національного університету «Юридична академія України імені Ярослава Мудрого», Харківського національного університету радіоелектроніки, Національного технічного університету «Харківський політехнічний інститут», національних університетів внутрішніх справ зі Львова, Одеси, Києва, Сум, Луганська, Донецька, Харкова, а також училищ професійної підготовки працівників міліції та навчальних центрів підготовки працівників органів внутрішніх справ з Полтави, Сум та Криму. Окрім того на запрошення відгукнулись фахівці Харківського банківського Союзу – регіонального представника Незалежної асоціації банків України, працівники банківських установ, державних органів та органів місцевого самоврядування Харківської області, громадських організацій, зацікавлених у підвищенні ефективності розслідування кіберзлочинів правоохоронними органами.

На сьогоднішній день проблеми виявлення, розслідування та запобігання кіберзлочинам є надзвичайно актуальними, що неодноразово наголошувалось Президентом України В. Ф. Януковичем, представниками вищих державних органів і міжнародних інституцій. Кіберзлочинність є відносно новим явищем, характерним для сучасного етапу розвитку суспільства. Проте вона поширюється надзвичайно стрімко,

що вимагає від юридичної науки активізації наукових досліджень з метою забезпечення ефективної протидії будь-яким злочинним проявам у кіберпросторі. Тому вважаю проведення цієї науково-практичної конференції своєчасним і корисним з точки зору як розвитку теоретичних уявлень, так і вдосконалення практичної діяльності у сфері протидії даному типу злочинності.

Конференція планується як науковий захід, на якому науковці і працівники правоохоронних органів, представники державних і приватних структур, зацікавлені у вдосконаленні стану протидії кіберзлочинності, обговорять сучасні проблеми розслідування кіберзлочинів; спільними зусиллями спробують знайти ефективні засоби вирішення кримінально-правових, процесуальних та криміналістичних проблем їх розслідування; сформулюють пропозиції та рекомендації, які можна буде використати в практичній діяльності правоохоронних органів, у науково-дослідній роботі та у навчальному процесі.

Робота конференції буде проводитися за такими напрямами, як процесуальні та криміналістичні проблеми розслідування кіберзлочинів; актуальні питання кваліфікації кіберзлочинів; досвід зарубіжних країн щодо їх розслідування; використання інформаційних технологій і технічних засобів у документуванні та розслідуванні кіберзлочинів тощо.

Сподіваюсь, що конференція дозволить розв'язати основні проблеми, які виникають під час розслідування кіберзлочинів, та віднайти шляхи подальшого удосконалення чинного законодавства, слідчої практики і процесу підготовки відповідних фахівців для органів внутрішніх справ.

Бажаю учасникам конференції «Актуальні питання розслідування кіберзлочинів» конструктивної праці, творчого натхнення та вагомих наукових напрацювань.

С. Гусаров,
ректор Харківського національного університету внутрішніх справ, доктор юридичних наук, член-кореспондент Національної академії правових наук України, заслужений юрист України, генерал-полковник міліції

РОЗДІЛ 1
ПРОБЛЕМИ ПРАВОВОГО, ОРГАНІЗАЦІЙНОГО ТА КАДРОВОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

УДК 343.98

Сергій Миколайович ГУСАРОВ,
ректор Харківського національного університету внутрішніх справ, доктор юридичних наук, член-кореспондент Національної академії правових наук України, заслужений юрист України

РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ОРГАНАМИ ВНУТРІШНІХ СПРАВ УКРАЇНИ: НАУКОВЕ ТА КАДРОВЕ ЗАБЕЗПЕЧЕННЯ

Кіберзлочинність є явищем міжнародного значення. Її рівень перебуває у прямій залежності від рівня розвитку та впровадження сучасних комп'ютерних технологій, мереж їх загального користування та доступу до них. Стрімкий розвиток інформатизації в Україні несе за собою потенційну можливість використання комп'ютерних технологій з корисливих та інших мотивів, що певною мірою ставить під загрозу не лише національну безпеку держави, а й особисті, майнові, немайнові та інші права і свободи громадян.

В останні роки набувають значного поширення кіберзлочини, пов'язані з використанням мережі Інтернет: використання віртуальних крамниць і фірм, що надають платні послуги з вилученням з рахунків і кредитних карток їх володільців «електронних» грошових коштів; організація азартних ігор (казино, лотерей, тоталізаторів, інтернет-аукціонів), фінансових пірамід, шлюбних агентств і т. п. шахрайства з викраденням грошових коштів обманутих громадян; вимагання під погрозою знищення чи модифікації інформаційних баз даних; комп'ютерне «піратство» (незаконна діяльність у сфері програмного забезпечення); інше використання комп'ютерних техніки та технологій (інформаційної системи) для вчинення злочинів (розповсюдження порнографічної продукції, матеріалів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, створення та розповсюдження шкідливих програм чи засобів тощо).

Підвищений інтерес злочинців до Інтернету не випадковий. Унікальність глобальної мережі полягає в тому, що вона не знаходиться у віданні конкретної фізичної особи, приватної компанії, державної чи громадської організації чи навіть окремої держави. Використання телекомунікаційних мереж дозволяє вчинити злочин не виходячи з дому, офісу, не покидаючи межі своєї країни, або одночасно з території декількох держав. Відсутні будь-які форми контролю за інформацією, що відкриває необмежені можливості для доступу до неї та використовується злочинцями. Зазначене обумовлює транснаціональний, організований, груповий характер багатьох кіберзлочинів.

Враховуючи значущість та гостроту проблем, що виникають у сфері боротьби із вказаним типом злочинності, окремі питання застосування заходів кримінально-правового характеру з метою протидії кіберзлочинності неодноразово були предметом наукових досліджень як теоретичного, так і прикладного характеру. Вагомим є і внесок учених Харківського національного університету внутрішніх справ.

Зокрема, фахівцями університету розроблено проект Закону України «Про внесення змін і доповнень до Кримінального кодексу України щодо посилення відповідальності за кіберзлочини», проект Закону України «Про внесення змін і доповнень до Кримінального процесуального кодексу України щодо надання органам розслідування повноважень, необхідних і достатніх для ефективної боротьби з кіберзлочинністю», надано зауваження та пропозиції до проекту Закону України «Про боротьбу з кіберзлочинністю», розробленого Управлінням боротьби з кіберзлочинністю МВС України, та запропоновано авторський проект Закону України «Про протидію кіберзлочинності». Також проаналізовано пропозиції МВС України щодо законопроекту про вдосконалення порядку отримання правоохоронними органами інформації про споживачів телекомунікаційних послуг та порядку придбання SIM-карт споживачами та підготовлено проект Закону України «Про внесення змін до деяких законодавчих актів України (щодо вдосконалення порядку надання телекомунікаційних послуг абонентам та отримання правоохоронними органами інформації про них)» тощо. Окрім того, досліджено питання регламентації заходів протидії кіберзлочинності як на національному, так і на міжнародному рівнях.

Проведений науково-практичний аналіз міжнародних нормативно-правових актів, якими регламентується співробітництво у боротьбі з кіберзлочинністю, дозволив зробити висновок, що основними напрямами вдосконалення національного законодавства слід визнати:

– узгодження термінології, що використовується у нормативно-правових актах міжнародного характеру та національному законодавстві України;

– здійснення чіткої класифікації злочинних посягань, які слід відносити до групи (категорії) кіберзлочинів;

– розробка та впровадження дієвого механізму взаємодії правоохоронних органів у рамках виконання зобов'язань України, взятих у зв'язку з ратифікацією 7 вересня 2005 року Конвенції про кіберзлочинність.

Харківським національним університетом внутрішніх справ проводяться семінари та науково-практичні конференції, в тому числі міжнародні, з питань боротьби з кіберзлочинністю. Науково-педагогічний склад та курсанти беруть активну участь й у науково-практичних конференціях та семінарах, що проводяться іншими вищими навчальними закладами та підрозділами системи МВС.

Належне кадрове забезпечення протидії кіберзлочинності органами внутрішніх справ передбачає організацію добору, навчання, розстановки, перепідготовки та підвищення кваліфікації працівників органів внутрішніх справ у сфері протидії кіберзлочинам. Основними завданнями в цій сфері є:

– впровадження у діяльність вищих навчальних закладів системи МВС України програм підготовки фахівців за спеціалізацією «протидія кіберзлочинам»;

– забезпечення взаємної інтеграції дисциплін юридичного і технічного спрямування відповідно у фахівців із технічного захисту інформації та підготовка фахівців-правознавців. Подібні заходи дозволять, по-перше, зміцнити технічну складову у підготовці слідчих та оперативних працівників ОВС, а по-друге – озброїти технічних спеціалістів необхідними юридичними знаннями;

– впровадження у програми підвищення кваліфікації працівників ОВС, які проводяться на базі вищих навчальних закладів, тем щодо протидії кіберзлочинам, їх виявлення, документування, особливостей розслідування;

– залучення до проведення практичних занять у вищих навчальних закладах провідних фахівців у сфері протидії шахрайствам у мережі Інтернет, захисту інформаційних даних з практичних органів внутрішніх справ, а також з інших установ і підприємств, які працюють у сфері інформаційних технологій та захисту інформації;

– забезпечення навчальних закладів МВС України необхідними технічними засобами і комп'ютерним обладнанням, які дозволять більш ефективно проводити підготовку у сфері попередження та розслідування кіберзлочинів;

– організація постійного обміну досвідом із провідними фахівцями правоохоронних органів та інших установ у сфері попередження комп'ютерної злочинності, захисту персональних даних, припинення випадків фінансових шахрайств у мережі Інтернет. У рамках такого обміну доцільною є організація стажування практичних працівників у відповідних правоохоронних органах та інших установах, організаціях, що спеціалізуються на цьому питанні.

На вирішення зазначених завдань на базі Харківського національного університету внутрішніх справ у 2013 році створений факультет підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми. На факультеті здійснюється навчання курсантів за напрямами підготовки «Системи технічного захисту інформації» (за спеціалізацією «боротьба з кіберзлочинністю») та «Правознавство» (спеціалізація – слідчі, що спеціалізуються на розслідуванні кіберзлочинів; оперативні працівники для підрозділів боротьби з кіберзлочинністю; оперативні працівники для підрозділів з протидії торгівлі людьми, злочинам проти моральності та у міжнародній сфері).

У 2013 році в університеті також відкрито на громадських засадах Навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору. Вказаний Центр виконує в першу чергу навчальні функції, адже призначений для проведення практичних і лабораторних занять з метою формування курсантами навичок пошуку, виявлення, фіксації, вилучення та дослідження слідів кіберзлочинів та їх носіїв – жорстких та гнучких магнітних дисків, дисків для лазерних системи зчитування, флеш-носіїв, мобільних телефонів та ін. У навчальному процесі використовуються технічні та програмні засоби, що знаходяться на оснащенні правоохоронних

органів України (апаратні та програмні засоби пошуку, виявлення, фіксації та дослідження речових доказів), а також зразки процесуальних документів, що складаються при проведенні відповідних слідчих (розшукових) дій в Україні. Подібне впровадження в навчальний процес практичної компоненти безумовно підвищує якість підготовки фахівців з розслідування окремих видів кіберзлочинів.

На базі центру післядипломної освіти Харківського національного університету внутрішніх справ свою кваліфікацію підвищують слідчі підрозділів боротьби з кіберзлочинами та експерти з комп'ютерно-технічної експертизи. Окрім того, теми щодо протидії кіберзлочинам, їх виявлення, документування, особливостей розслідування впроваджені у програми як підвищення кваліфікації інших категорій працівників ОВС, так і підготовки магістрів, які вивчають спеціальний курс з особливостей розслідування кіберзлочинів. До проведення практичних занять із курсантами та слухачами активно залучаються провідні фахівці у сфері протидії кіберзлочинам.

В університеті також організоване стажування науково-педагогічного складу у підрозділах правоохоронних органів ГУМВС України в Харківській області, що спеціалізуються на розслідуванні кіберзлочинів.

Резюмуючи вищевикладене, слід констатувати, що проведення комплексних досліджень з метою поліпшення стану наукового забезпечення розслідування кіберзлочинів, удосконалення системи підготовки фахівців для підрозділів боротьби з кіберзлочинністю є запорукою підвищення ефективності практичної діяльності.

Одержано 19.11.2013

УДК 322.2;342.9:351.74

Володимир Миколайович ОЛІЙНИК,
народний депутат України VII скликання,
заступник голови Комітету Верховної Ради України
з питань законодавчого забезпечення правоохоронної діяльності,
кандидат історичних наук, заслужений юрист України

КІБЕРЗЛОЧИННІСТЬ ЯК УМОВА ПОРУШЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ УКРАЇНИ

Ми живемо в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людини і держави. Але людство, поставивши собі на службу телекомунікації і глобальні комп'ютерні мережі, не передбачало, які можливості для зловживання створюють ці технології. Сьогодні жертвами злочинців, що орудують у віртуальному просторі, можуть стати не лише люди, але і цілі держави. При цьому безпека тисяч користувачів може виявитися залежна від декількох злочинців. Кількість злочинів, що здійснюються в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, по оцінках Інтерполу, темпи зростання злочинності, наприклад, в глобальній мережі Інтернет, є найшвидшими на планеті [1, с. 98].

На XI Конгресі ООН із запобігання злочинності і кримінального правосуддя, який відбувся в квітні 2005 року, злочинності, пов'язаній з використанням комп'ютерів було приділено особливу увагу: це питання було включене до порядку денного і розглядалось в рамках проблеми ефективних заходів по боротьбі з транснаціональною організованою злочинністю. Експерти ООН в рекомендаціях, підготовлених до XI Конгресу, говорять про особливий характер кіберзлочинності і необхідності вживання комплексних підходів по боротьбі з нею, а також про невідкладні заходи по оновленню кримінального законодавства держав-учасників ООН, таких як уточнення або вилучення норм, що не відповідають ситуації, що склалася, або прийнятті норм, що стосуються нового вигляду кіберзлочинів.

Декларація Бангкока, яка стала результатом діяльності XI Конгресу ООН по запобіганню злочинності і кримінальному правосуддю, також свідчить про актуальність проблеми кіберзлочинності.

У Декларації наголошується, що в період глобалізації швидкий розвиток інформаційних технологій і нових систем телекомунікацій і комп'ютерних мереж супроводжується зловживанням цими технологіями в злочинних цілях, а також підкреслюється необхідність розробки національних заходів та розвитку міжнародної співпраці по протидії кіберзлочинності [2].

Небезпека кіберзлочинності як для всього світу, так і для України визнають і вітчизняні правоохоронні органи. Так, на наш погляд, кіберзлочинність (злочинність у сфері високих технологій) в даний час є однією з найбільш серйозних погроз національній безпеці України в інформаційній сфері.

Кіберзлочинність за своєю суттю набагато ширше за комп'ютерну злочинність, і включає цілий спектр протиправних діянь. Під кіберзлочинністю в даній роботі розуміється сукупність злочинів, що здійснюються в кіберпросторі з допомогою або за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Відповідно, кіберзлочин – це винне протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, здійснені з допомогою або за допомогою комп'ютерів, комп'ютерних мереж і програм, а також з допомогою або за допомогою інших пристроїв доступу до модельованого за допомогою комп'ютера інформаційного простору.

Кіберзлочинність володіє підвищеною громадською небезпекою унаслідок можливості спричинення крупного збитку при мінімальних витратах й невисокому ризику. Крім того, кіберзлочинність характеризується високою латентністю, внаслідок чого статистика правоохоронних органів не відображає достовірної картини стану кіберзлочинності як на рівні держави, так і на загальносвітовому рівні. Для оцінки стану кіберзлочинності необхідно використовувати інші способи здобуття даних і оцінки ситуації: огляди, інтерв'ювання, методи реєстрації звернень.

Зростання кіберзлочинності, що сталось останніми роками, відзначають і фахівці правоохоронних органів держав, і співробітники організацій, що займаються дослідженнями за

допомогою альтернативних методів збору статистичних даних. При цьому фінансові втрати від кіберзлочинності обчислюються мільйонами доларів. В Україні зростаюча загроза кіберзлочинності вже визнається на рівні вищих посадових осіб, які говорять про неї як про можливу загрозу безпеці держави. Офіційна ж статистика України повідомляє всього про декілька тисяч комп'ютерних злочинів. Ця проблема характерна для багатьох держав. Оскільки кіберзлочинності є відносно «новим» видом злочинної діяльності, а виявлення і розслідування злочинів ускладнюється їх трансграничним характером, статистичні дані ще дуже довго не відображатимуть достовірну картину електронних посягань не лише на глобальному рівні, але і на рівні окремо узятої держави.

Проте, не дивлячись на невисокі показники офіційної статистики в багатьох державах, проблемою кіберзлочинності вже заклопотана як чимала кількість країн, так і міжнародні організації. Через трансграничний характер цього явища, кримінально-правова боротьба з ним стає глобальною проблемою. Для ефективної боротьби з кіберзлочинами необхідне як прийняття відповідних кримінально-правових норм на національному рівні, так і вироблення єдиних міжнародних стандартів. Однією з необхідних умов дієвості заходів, що робляться, є криміналізація хоч би мінімального набору протиправних діянь, що здійснюються за допомогою комп'ютерних технологій у всіх державах світу.

Тенденція зростання кіберзлочинності і тенденція «відставання» соціально-правового контролю над нею ув'язуються в якийсь порочний круг, розірвати який можна лише шляхом органічного поєднання кримінально-правових і криміналістичних стратегій боротьби з цим видом злочинів.

Для боротьби із загрозою кіберзлочинності, яка, безумовно, зростатиме з подальшим розширенням сфери використання інформаційних технологій, надаючи великі можливості для протиправної діяльності як індивідуумам, так і злочинним групам, необхідна постійна міжнародна співпраця. Контролювати кіберзлочинність і боротися з нею на рівні окремої держави практично неможливо. Прийняття міжнародних норм і стандартів повинне супроводжуватись внесенням змін до національного законодавства держав. Координація зусиль держав необхідна для забезпечення швидкого реагування на розвиток комп'ютерних технологій і прийняття відповідних

норм. В даний час у формуванні міжнародної стратегії боротьби з кіберзлочинністю задіяні більше сорока країн світу, і процес цей обіцяє бути досить довгим. Проте, не дивлячись на всі складнощі, очевидно, що міжнародному співтовариству необхідно прийти до вирішення проблем уніфікації законодавства. Інакше, з врахуванням трансграничності кіберзлочинності, певні невідповідності в законодавстві і нескоординованість кримінальної політики дозволять особам, що зробили суспільно небезпечні дії, уникати відповідальності і ускладнювати розслідування злочинів і переслідування правопорушників.

Список використаних джерел:

1. Номоконов В. А. Глобализация информационных процессов и преступность / В. А. Номоконов // Інформаційні технології та безпека : зб. наук. праць. – Вип. 1. – К., 2002. – С. 95–103.

2. Бангкокская декларация «Взаимодействие и ответные меры: стратегические союзы в области предупреждения преступности и уголовного правосудия» [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/decl_conv/declarations/bangkok_declaration.shtml.

Одержано 14.11.2013

УДК 65.012.8+004

Олександр Миколайович ГОЛОВКО,
доктор юридичних наук, професор,
перший проректор з навчально-методичної та наукової роботи
Харківського національного університету внутрішніх справ

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ У СФЕРІ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Підготовка фахівців для підрозділів МВС України, задіяних у сфері боротьби з кіберзлочинністю, на сьогоднішній день є одним з актуальних завдань правоохоронної діяльності. Значущість цього питання обумовлено не лише щорічним зростанням високотехнологічної злочинності в Україні та світі, але й поступовим зміщенням акцентів злочинних інтересів у бік кіберпростору.

Як зазначив начальник Управління боротьби з кіберзлочинністю М. Ю. Літвінов, протягом 2012 року правоохоронцями

зареєстровано 2011 злочинів, вчинених із використанням високих технологій. У першому півріччі 2013 року до ЄРДР внесено 1878 заяв та повідомлень про злочини даної категорії, а їх розкриття складає близько 50 %.

Важливим елементом боротьби з кіберзлочинністю є ефективна міжнародна взаємодія, одним з напрямів якої є обмін досвідом та допомога у підготовці фахівців відповідної категорії. Харківський національний університет внутрішніх справ приділяє цьому питанню підвищену увагу.

У навчальному процесі викладаються сучасні міжнародні методики протидії кіберзлочинності, залучаються іноземні спеціалісти в цій сфері, проводяться круглі столи та вебінари.

За поточний рік було налагоджено взаємодію з низкою міжнародних інституцій, серед яких можна виділити наступні:

Американська асоціація юристів «Ініціатива з верховенства права» (ABA ROLI – Україна)

U.S. Dept. of Justice International Criminal Investigative Training Assistance Program (ICITAP) Ukraine Mission

Організація безпеки та співробітництва в Європі

The Society for the Policing of Cyberspace (POLCYB)

Зокрема, у період з 8 до 10 серпня 2013 року на базі Харківського національного університету внутрішніх справ Американською асоціацією юристів «Ініціатива з верховенства права в Україні» в рамках виконання проекту «Зміцнення потенціалу МВС в розслідуванні справ про кіберзлочини» було проведено регіональний практичний тренінг з працівниками підрозділів боротьби з кіберзлочинністю та слідчих підрозділів ОВС України на тему «Особливості проведення тимчасового доступу до речей і документів при розслідуванні справ про кіберзлочини: процесуальні та технічні аспекти».

Одним з останніх міжнародних заходів, які відбулися в університеті у рамках підготовки фахівців для підрозділів боротьби з кіберзлочинністю, став візит представників Посольства США та Міжнародної програми підвищення кваліфікації для органів кримінального розслідування Департаменту юстиції США (ICITAП).

Серед учасників делегації був М. Роджерс – професор університету Пердью штату Індіана США. У рамках проведеного круглого столу з курсантами та викладачами університету він окреслив загальний порядок встановлення особи за її мережними ідентифікаторами в США, документування доказової інформації, яка зберігається за допомогою хмарних технологій, розповів, як вдалося довести винуватість особи у потрійному вбивстві за допомогою комп'ютерно-технічної експертизи, під час якої було змодельовано декілька процесів, та досліджено так звані «флеш-куки». Наостанок М. Роджерс запропонував курсантам Харківського національного університету внутрішніх справ взяти участь у спеціалізованих змаганнях у сфері протидії кіберзлочинності разом з його студентами.

Як показала практика такі заходи сприяють практичній підготовці курсантів та виробленню в них системного підходу у протидії високотехнологічним злочинам.

Не оминає увагою університет і взаємодію з вищими навчальними закладами інших країн у сфері наукового забезпечення протидії кіберзлочинності. Так, у травні поточного року делегація університету взяла участь у міжнародній науково-практичній конференції «Протидія злочинам у сфері інформаційних технологій» на базі Бєлгородського юридичного інституту МВС Росії. Під час конференції розглядалися важливі питання, пов'язані з оперативно-розшуковими заходами в інформаційному просторі, та проблемами протидії злочинам, що вчиняються з використанням телекомунікаційних систем. За словами заступника начальника інституту з наукової роботи А. Озерова, ця зустріч сприятиме розвитку міжнародної співпраці правоохоронних органів щодо протидії злочинам у сфері інформаційних технологій та позитивно позначиться на спільній роботі у формуванні цілісної системи протидії кіберзлочинам.

Підбиваючи підсумки зазначимо, що вжиті університетом заходи щодо покращення міжнародної взаємодії у підготовці

фахівців відповідної категорії вже сьогодні дають позитивний результат. Курсанти не лише підвищують рівень теоретичної грамотності, але й беруть участь у реальних заходах з виявлення кіберзлочинів та розшуку злочинців з використанням комп'ютерних технологій. Маючи певні практичні напрацювання, вдається більш ефективно консультуватися з зарубіжними колегами та вживати належні заходи протидії кіберзлочинності.

Одержано 15.11.2013

УДК 343.3/.7

Николай Витальевич КАРЧЕВСКИЙ,
доктор юридических наук, доцент,
первый проректор по учебно-методической и научной работе
Луганского государственного университета внутренних дел
имени Э. А. Дидоренко

«КОМПЬЮТЕРНОЕ ПРЕСТУПЛЕНИЕ», «КИБЕРПРЕСТУПЛЕНИЕ», «ПРЕСТУПЛЕНИЕ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Одним ключевых вопросов уголовно-правового регулирования в сфере информатизации является определение понятий «преступление в сфере использования информационных технологий», «компьютерное преступление», «киберпреступление» и т. д. Как отмечалось ранее, обеспечение уголовно-правового стимулирования положительных и минимизации негативных социальных последствий информатизации, предполагает определение в качестве самостоятельного объекта уголовно-правовой охраны системы общественных отношений, обеспечивающих реализацию информационной потребности. Для обозначения этой системы предлагается использовать термин «информационная безопасность», ее структуру составляют отношения в сфере формирования информационного ресурса, обеспечения доступа к информации, а также отношения в сфере использования информационных технологий. При этом социальная значимость отношений информационной безопасности, а следовательно и целесообразность их уголовно-правовой охраны, определяются значимостью тех отношений, в пределах которых возникает информационная потребность. В свою очередь, информационная тех.-нология представляет собой организованную совокупность

информационных процессов с использованием средств вычислительной техники, которые обеспечивают высокую скорость обработки данных, быстрый поиск информации, передачу данных, доступ к источникам информации независимо от места их расположения [5]. Таким образом, преступления в сфере использования информационных технологий, являясь одним из видов преступлений в сфере информационной безопасности, представляют собой *предусмотренные законодательством об уголовной ответственности, общественно опасные, виновные, совершенные субъектом преступления деяния, причиняющие вред обеспеченным средствами вычислительной техники отношениям в сфере реализации информационной потребности.* Анализ действующего УК позволяет прийти к выводу, что к таким преступлениям следует относить посягательства, предусмотренные *ч. 11, 12 ст. 158, ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1 УК.*

Наряду с предлагаемым понятием («преступление в сфере использования информационных технологий») достаточно активно используются следующие: «компьютерное преступление», «киберпреступление», «интернет-преступление» и т. д. Объем данных понятий определяется по-разному. Тем не менее, наиболее распространенным является отнесение к компьютерным преступлениям всех общественно опасных посягательств, при совершении которых компьютеры используются как технические средства [2, с. 11; 4, с. 14; 3, с. 35–40; 1, с. 72]. Такой подход широко используется и в зарубежной научной литературе [7; 5; 8].

Необходимо отметить, что зарубежный опыт несомненно должен изучаться и быть использованным. В тоже время, безоглядный перенос западных стандартов регулирования политических, экономических и социальных процессов без учета исторических и национальных особенностей далеко не всегда приводит к положительным результатам. Представляется, что в случае с определением компьютерных преступлений и использованием данного понятия в отечественном уголовно-правовом дискурсе имеет место как раз такая ситуация.

При описанном понимании, любое преступление, совершенное с использованием компьютерной техники (мошенничество, шпионаж, незаконное распространение наркотических средств и т. д.), должно считаться компьютерным. Хотя абсолютно очевидно, что вышеперечисленные общественно

опасные деяния не являются преступлениями нового вида. Такие действия, несмотря на использование для их совершения компьютерной техники, остаются государственной изменой, шпионажем, кражей, мошенничеством, незаконным сбором сведений, которые составляют коммерческую тайну и т. д. Средство не меняет сути преступления.

Сказанное вовсе не означает, что расширение сферы применения компьютерных технологий не привело к появлению преступлений нового вида, не всегда общественно опасное посягательство, совершенное с использованием компьютерной техники, можно рассматривать как традиционное преступление, усложненное применением новых средств. Как быть, например, с квалификацией распределенной атаки отказа от обслуживания, совершенной с использованием ботсети? В терминах какого из традиционных преступлений можно описать незаконные множественные рассылки электронных сообщений (спам)?

Таким образом, уместное в пределах зарубежного уголовно-правового дискурса определение компьютерных преступлений имеет весьма ограниченную ценность для национальной науки уголовного права. Как известно, в зарубежной уголовно-правовой доктрине материально-правовые проблемы рассматриваются в неразрывной связи с процессуальными. В таких условиях критикуемый подход к определению компьютерных преступлений имеет смысл и несомненно оправдан. В свою очередь, попытка исследования проблем национального уголовно-правового отражения тенденций информатизации на основе такого же подхода, как представляется, не имеет перспективы.

Понятия «компьютерное преступление» и «киберпреступление», в общепризнанном понимании, могут быть эффективно использованы при проведении криминологических, уголовно-процессуальных, криминалистических исследований. Что же касается национального уголовно-правового дискурса, то здесь их применение следует ограничить, и использовать предложенное понятие «преступление в сфере использования информационных технологий».

Список использованных источников:

1. Азаров Д. С. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д. С. Азаров // Право України. – 2000. – № 12. – С. 69–73.

2. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юрид. лит., 1991. – 157 с.

3. Голубєв В. О. Правові проблеми захисту інформаційних технологій / В. О. Голубєв // Вісник Запорізького юридичного інституту. – 1997. – № 2. – С. 35–40.

4. Калюжный Р. А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. … д-ра юрид. наук : 12.00.02 / Калюжный Ростислав Андреевич. – К., 1992. – 47 с.

5. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луг. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.

6. Brenner S. Cybercrime: criminal threats from cyberspace / Susan W. Brenner. – Praeger, 2006. – 281 p.

7. Jewkes Y. Cybercrimes / Yvonne Jewkes // The Sage Dictionary of Criminology / comp. and ed. by Eugene McLaughlin, John Muncie. Third Edition. – Sage Publications, 2013. – 536 p.

8. Leukfeldt R. High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands [Электронный ресурс] / Rutger Leukfeldt, Sander Veenstra, Wouter Stol // International Journal of Cyber Criminology. – Vol. 7. – Is. 1. – 2013. – Режим доступа: http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf.

Одержано 19.11.2013

УДК 343.1

Олександр Олександрович ЮХНО,
доктор юридичних наук, професор,
начальник кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ І ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ ОРГАНІВ ВНУТРІШНІХ СПРАВ

Стрімкий та динамічний розвиток інформаційних технологій кожен день все більше змінює аспекти економічного, політичного і соціального життя у всіх країнах світу. В середині п'ятдесятих років минулого століття телевізор був рідкістю, а тепер він є майже в кожній родині. В середині

сімдесятих років того ж століття персональний комп'ютер був рідкістю, а на сьогоднішній день комп'ютером навряд чи кого здивуєш. Вказане призвело до розвитку програмного забезпечення, підвищення професіональної підготовки користувачів, збільшенню потреб підприємств, установ і організацій в удосконаленні технології обробки інформації і даних, значно поширило сферу застосування комп'ютерів і мережі Інтернет, до яких також стало все частіше підключатись широкі верстви населення. Активно поширюється автоматизована обробка бухгалтерської і іншої виробничої та службової документації, зокрема «безпаперових» технологій. Комп'ютер став обов'язковим елементом робочого місця не тільки керівників, але й виконавців. Не обійшло це і слідчу діяльність. За чинним КПК України діє Єдиний реєстр досудового розслідування, створюється Реєстр адвокатів України тощо. За даними «Nua Internet Surveys» кількість користувачів глобальної мережі Інтернет із 80 тисяч у 1988 році зросла до 2,7 мільярдів у 2013 році. Кожен службовий персональний комп'ютер слідчого чи оперативного працівника має підключення до глобальної мережі Інтернет, що надає працівникам правоохоронних органів низку сучасних інформаційних інструментів для проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій. Зростання кількості персональних комп'ютерів та користувачів мережі Інтернет впливає на криміналізацію дій, пов'язаних з його використанням та збільшення кількості злочинів, що все більше вчиняються з використанням сучасних інформаційних технологій і призвело до доцільності законодавчо регламентувати кримінальну відповідальність за вчинення кримінальних правопорушень у цій сфері. У національному законодавстві встановлено відповідальність за шістьма статтями КК України. Так, в Україні у 2002 році було зареєстровано всього 30, в 2009 році вже 217 таких видів злочинів, а щорічне їх зростання складає 27 відсотків, враховуючи велику латентність, недосконалість чинного законодавства тощо. Так, за оцінкою окремих вітчизняних і зарубіжних дослідників рівень латентності комп'ютерних кримінальних правопорушень складає біля 90 %, а із залишених 10 %, виявлення й розкриття вже вчинених складає лише один відсоток. За результатами практики розслідування інших видів злочинів, вчинених з використанням комп'ютерів і інформації з них, встановлено, що висунути підозру особі у кримінальних провадженнях дозволяє у 50 %

випадках, а в 35 % надає суттєву допомогу у викритті й розшуку таких злочинів, по яких достеменно встановлено обставини вчинення кримінального правопорушення.

З метою підвищення ефективності протидії і запобіганню таким кримінальним правопорушенням, в системі МВС України створено спеціальні підрозділи щодо протидії кіберзлочинам, що напрацьовують практику з цього напряму організаційної, слідчої, оперативно-розшукової та іншої діяльності. Невипадково такі види злочинів ще у 1992 році були внесені ООН до списку 14 видів транснаціональних організованих злочинів, поставивши їх в один ряд із «незаконним відмиванням» грошей, терористичною діяльністю, організованим наркобізнесом, крадіжками витворів мистецтв, інтелектуальної власності, незаконною торгівлею зброєю, захватом повітряних суден, морським піратством, заволодінням наземного транспорту, шахрайством, екологічними злочинами, торгівлею людьми і людськими органами. Крім цього в Європі ще у 2001 році було підписано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, яка в нашій країні більш відома під назвою «Конвенція про кіберзлочинність», що була ратифікована Україною у 2005 році. Якщо в соціальній сфері використання новітніх технологій, особливо мережі Інтернет невпинно зростає і використовується населенням різного, починаючи з дошкільного віку, то в діяльності правоохоронних органів і, зокрема органів внутрішніх справ, у зв'язку з обмеженням фінансування, їх застосування та вирішення питань ліцензування, здійснюється досить повільно. В той же час автори навчального посібника «Використання сучасних інформаційних технологій працівниками ОВС при проведенні негласних слідчих (розшукових) дій Д. О. Максимус і О. О. Юхно, що репрезентований на наступній науково-практичній конференції, вивчивши наявну систему новітніх інформаційних технологій і, зокрема мережі Інтернет, прийшли до висновку, що в ній є невикористані можливості, у тому числі технічні, що нададуть допомогу працівникам підрозділів досудового розслідування та оперативних підрозділів ОВС, без використання додаткових матеріальних витрат удосконалити діяльність досудового розслідування направлену на запобігання й протидію кримінальних правопорушень у сфері сучасних інформаційних технологій та мережі Інтернет, значно підвищити ефективність такої діяльності а також щодо інших видів зло-

чинів. Вказане дозволить продовжити дослідження не тільки по технічним, але й правовим питанням, по розширенню можливостей, напрацюванню пропозицій та рекомендацій щодо удосконалення кримінального процесуального і кримінального законодавства України, оперативно-розшукової діяльності та ін. Нагальність вказаних проблем сьогодні досить гостро відчувають як вчені, так і слідчі, оперативні працівники, фахівці органів прокуратури та інших правоохоронних органів.

Враховуючи невеликий досвід діяльності слідчих і оперативних підрозділів у вказаній сфері та з метою удосконалення досудового розслідування і оперативно-розшукової діяльності вважаємо за доцільне : 1) напрацьовувати дослідження й теоретичні методики і рекомендації для практики щодо удосконалення збору і процесуального закріплення доказів при досудовому розслідуванні кіберзлочинів; 2) вносити пропозиції щодо удосконалення національного законодавства про кримінальну відповідальність щодо криміналізації при виявленні нових видів кіберзлочинів; 3) з метою підвищення ефективності протидії і запобіганню створити при підрозділах ОВС по протидії кіберзлочинам сектори аналітичної і технічної розвідки, із забезпеченням їх потужними комп'ютерними і іншими сучасними інформаційно-технічними засобами; 4) продовжити введення обов'язкової спеціалізації слідчих із розслідування кіберзлочинів, у тому числі в підрозділах ГУБОЗ; 5) з метою поширення технічних і процесуальних знань щодо сучасних досягнень інформаційних і інших інформаційних технологій, можливостей мережі Інтернет тощо включати в плани роботи МВС України підвищення кваліфікації працівників підрозділів досудового розслідування і оперативних підрозділів по протидії кіберзлочинам та інших підрозділів; 6) керівництву МВС України розглянути питання про створення при навчальних закладах спеціалізованих науково-дослідних лабораторій щодо напрацювання методик розслідування і викриття кіберзлочинів та розробки проблемних питань чинного КПК України. Втім підняті питання не є остаточними і потребують окремого дослідження або наукового вивчення. Пропоную учасникам конференції прийняти участь у обговоренні наданих пропозицій.

Одержано 15.11.2013

УДК 65.012.8+004

Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент,
начальник кафедри захисту інформації
факультету підготовки фахівців для підрозділів
боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ФАХІВЦІВ ІЗ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ У ХАРКІВСЬКОМУ НАЦІОНАЛЬНОМУ УНІВЕРСИТЕТІ ВНУТРІШНІХ СПРАВ

У Міністерстві внутрішніх справ України на постійному контролі перебуває питання щодо підготовки, підвищення кваліфікації та спеціалізації фахівців по боротьбі з кіберзлочинністю. Кіберзлочинність є одним з нових видів негативних соціальних явищ, яке на сьогодні кидає виклик національній безпеці України.

З метою забезпечення сучасних потреб слідчих та оперативних підрозділів фахівцями по боротьбі з кіберзлочинністю Наказом МВС України «Про організацію підготовки кадрів у Харківському національному університеті внутрішніх справ» від 20.11.2012 № 1062 було утворено факультет підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ. На факультеті здійснюється підготовка фахівців за напрямами підготовки «Системи технічного захисту інформації» та «Правознавство» спеціалізації «боротьба з кіберзлочинністю» та «боротьба з торгівлею людьми».

На виконання рішень керівництва МВС щодо підготовки, підвищення кваліфікації та спеціалізації фахівців по боротьбі з кіберзлочинністю з початку 2012 року університетом були впроваджені наступні заходи:

– проведено курси підвищення кваліфікації з працівниками Управління боротьби з кіберзлочинністю ГУМВС України в Харківській області;

– проведено курси підвищення кваліфікації працівників НДЕКЦ МВС, ГУМВС, УМВС, які спеціалізуються на проведенні комп'ютерно-технічної експертизи та старших слідчих в особливо важливих справах, старших слідчих, слідчих СУ ГУМВС, УМВС, які закріплені за розслідуванням злочинів у сфері кіберзлочинності;

– проведено курси підвищення кваліфікації працівників управлінь, відділів, секторів боротьби з кіберзлочинністю ГУМВС, УМВС;

– проведено курси підвищення кваліфікації працівників НДЕКЦ ГУМВС, УМВС, які спеціалізуються на проведенні експертиз у сфері інтелектуальної власності.

Організація навчального процесу здійснювалася на підставі розроблених центром післядипломної освіти та кафедрами Харківського національного університету внутрішніх справ навчальних та тематичних планів за участю представників практичних підрозділів ГУМВС України в Харківській області.

В ході проведення курсів підвищення кваліфікації було проведено анкетування слухачів щодо підвищення ефективності діяльності правоохоронних органів з протидії кіберзлочинності.

Варто відзначити, що на базі Харківського національного університету внутрішніх справ проводять низку важливих тренінгів, семінарів, конференцій та інших заходів з обміну передовим досвідом фахівців у сфері боротьби з кіберзлочинністю. Зокрема у серпні 2013 року в рамках виконання Проекту «Зміцнення потенціалу МВС в розслідуванні справ про кіберзлочини» Американською асоціацією юристів Ініціатива з верховенства права в Україні був проведений регіональний практичний тренінг з працівниками підрозділів боротьби з кіберзлочинністю та слідчих підрозділів ОВС України на тему «Особливості проведення тимчасового доступу до речей і документів при розслідуванні справ про кіберзлочини: процесуальні та технічні аспекти».

Курсанти та науково-педагогічний склад кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС протягом 2013 року приймали участь у заходах, які сприяють підвищенню рівня професійної майстерності, а саме у:

– Міжнародній науково-практичній конференції «Протидія кіберзлочинності в фінансово-банківській сфері» (Харківській національний університету внутрішніх справ);

– XVI-й Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (Державна служба спеціального зв'язку та захисту інформації);

– засіданні науково-методичної комісії МОН України з інформаційної безпеки (галузь знань 1701 «Інформаційна безпека»);

– Міжнародній науково-практичній конференції «Протидія злочинам у сфері інформаційних технологій» (Бєлгородський юридичний інститут Міністерства внутрішніх справ Російської Федерації);

– щорічній Міжнародній конференції банківських офіцерів «Безпека карткового бізнесу» (Національний центр підготовки банківських працівників України);

– тренінгу «Особливості застосування комп'ютерних технологій при розслідуванні кіберзлочинів (Американська асоціація юристів Ініціатива з верховенства права» (ABA ROLI) в Україні);

– VI-й східноєвропейській конференції «ЄМА» з протидії шахрайствам (Українська міжбанківська Асоціація членів платіжних систем «ЄМА»);

– науково-практичному семінарі на тему «Сучасні технічні засоби для спеціальних підрозділів міліції» (Державний науково-дослідний інститут МВС України);

– Міжнародній науковій конференції «Євразійська регіональна співпраця з метою розвитку криміналістики та судової експертизи» (Департамент юстиції США – ICITAP);

– Міжнародній науковій конференції «ДНК та електронні докази у кримінальному процесі» (Департамент юстиції США – OPDAT);

– семінарі-нараді «Комп'ютерно-технічні експертиза: проблема та розвиток» (Державний науково-дослідний експертно-криміналістичний центр МВС України).

Одержано 21.11.2013

УДК 343.98

Анатолій Миколайович КЛОЧКО,
доктор юридичних наук, доцент,
проректор по службі
Харківського національного університету внутрішніх справ

ПРОБЛЕМНІ ПИТАННЯ ТРАНСНАЦІОНАЛЬНОЇ КІБЕРЗЛОЧИННОСТІ

Кіберзлочини стали одним з найбільш небезпечних видів злочинних посягань: злочинці дуже швидко усвідомили масштаби можливостей Інтернету та телекомунікацій.

Сьогодні не існує загальноприйнятого визначення терміну «кіберзлочин», що характеризується експертами як злочин, здійснений із застосуванням високих інформаційних технологій. Злочин може бути здійснений засобами телекомунікаційних систем і мереж, в телекомунікаційній системі або мережі, або проти телекомунікаційної системи або мережі.

Інколи посилаються на категорії кіберзлочинів, до яких відноситься будь-яка незаконна дія, що проведена за допомогою будь-яких електронних засобів, котра має на меті впливати на засоби комп'ютерної безпеки або дані, що обробляються або зберігаються в комп'ютерній системі. В рамках даної категорії можуть розглядатися другорядні або непрямі погрози, такі як підготовка до серйозніших атак: передача комп'ютерних паролів, ключів кодування, кодів доступу тощо.

З врахуванням всіх міжнародних телекомунікаційних мереж, що існують сьогодні в світі менш вірогідним стає те, що всі елементи кіберзлочинності будуть обмежені територією однієї держави. Залежно від стосунків між зацікавленими державами, характеру відповідної інформації та інших чинників може виникнути потреба в розробці повноважень і процедур в міжнародних угодах та стандартах.

Здійснення відповідно до статей Європейської Конвенції про взаємодопомогу по кримінальних справах між державами-учасниками Європейського Союзу загальні дії при розслідуванні транснаціональних злочинів ускладнюються по таких причинах:

– традиційні форми співпраці передбачають письмові клопотання про надання правової допомоги, а це пов'язано з втратою часу в разі розслідування кіберзлочинів, та втрату доказів унаслідок знищення «історичних даних» (слідів);

– виявлення, закріплення, вилучення «історичних даних» (слідів) є можливим відносно двох держав (держави - місця знаходження потерпілого і держави, в якій знаходиться злочинець). Якщо комп'ютерна інформація проходить через три і більше держав, то надання правової допомоги може затягнутися на довгий час, внаслідок чого існує значна вірогідність зміни або знищення «історичних даних» (слідів);

– законами однієї держави проводяться розмежування між пошуком і перехопленням даних в процесі їх передачі або пошуку, які зберігаються, тоді як в правових системах інших держав чітке розмежування відсутнє.

Аналіз основних міжнародних документів правового регулювання інформаційних технологій дозволяє зробити висновок, що для ефективної діяльності по розслідуванню транснаціональних кіберзлочинів необхідно:

– уніфікувати кримінальне і кримінальне процесуальне законодавство кожної держави щодо протидії кіберзлочинам;

– усунути норми подвійного права;

– удосконалити протокол офіційної правової допомоги для ефективного розслідування злочинів і вирішення проблем оперативного отримання з-за кордону вилученої або збереженої на час надання правової допомоги комп'ютерної інформації – в документованому вигляді для використання її у якості доказу;

– передбачити канал зв'язку для забезпечення обслуговування невідкладних запитів в будь-який проміжок часу у всіх часових поясах з метою удосконалення системи слідчих і оперативно-розшукових заходів, особливо відносно кримінальних справ, які зачіпають інтереси декількох держав;

– ввести системи ідентифікації для сприяння пошуку кіберзлочинця за декілька секунд з метою здобуття безперечних доказів його злочинної діяльності;

– забезпечити обмін адресами операторів мереж/постачальників послуг у мережі.

Тому слід визначити що, існують різні погляди на злочини на національному рівні, що входять в загальну юрисдикцію. По-перше, існування різних принципів, більшість з яких суперечать один одному, показують, що проблеми юрисдикції не нові в сучасному міжнародному праві, а Інтернет і телекомунікаційні системи лише розширюють спектр потенційних проблем та загроз національній безпеці держави. По-друге, слід зазначити очевидне протиріччя «глобалізації» і «безмежності» Інтернету принципам юрисдикції, а це вносить певні зміни в концепції загальної юрисдикції.

Таким чином, проблеми, які створюються сучасними технологіями, можуть вирішуватися за допомогою тих же технологій. І, відповідно, поняття територіальності може стати фундаментальним у формуванні концепції «кіберправа». Експерти у сфері інформатики відзначають: «інформаційне суспільство» не має політичних, соціальних і економічних меж.

Одержано 07.11.2013

УДК [351.743:343.8]:004

Валерій Дмитрович ПЧОЛКІН,
доктор юридичних наук, професор,
професор кафедри кримінально-правових дисциплін
факультету права та масових комунікацій
Харківського національного університету внутрішніх справ

ШЛЯХИ ВДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ ОВС ЩОДО ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Проблема протидії кіберзлочинності набула глобального масштабу. Найбільш уразливою сферою суспільного життя від кіберзлочинів є фінансовий сектор економіки, а саме банки та їх послуги. Кібернетична злочинність все більше посягає на банківські рахунки як компаній чи організацій, так і пересічних громадян. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв. Серед поширених злочинів в банківській сфері є шахрайство з використанням платіжних карток та їх реквізитів і шахрайство з використанням дистанційного банківського обслуговування (система «клієнт-банк»).

За даними Нацбанку України, у 2012 р. в Україні зафіксовано 139 випадків шахрайства з використанням системи «клієнт банк» на загальну суму 116 млн грн, проте 75 % цих коштів було повернуто постраждалим особам. У цілому за офіційними даними Нацбанку України загальна кількість шахрайських операцій за минулий рік збільшилась на 47 %, а сума збитків на 20 %. У 2012 р. 40 % від загальної кількості українських банків постраждали від кібернетичних злочинів. На початку 2013 р. було виявлено 14 кіберзлочинів на загальну суму близько 20 млн грн, із яких було повернуто 88 %. Слід зазначити, що ці кіберзлочини вчиняються як хакерами, які не мають жодного відношення до банку, так і співробітниками банків, які мають доступ до персональних даних клієнтів. Так звані інсайдери досить часто зливають конфіденційну інформацію шахраям, отримуючи за це частку від награбованих коштів. Найбільшу небезпеку для суспільства, держави становить транскордонна організована кіберзлочинність: комп'ютерний тероризм; диверсії, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з комп'ютеризованих баз даних та порушення

права інтелектуальної власності на комп'ютерні програми; шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська сфера) і т. ін.

Законодавство України на теперішній час є ще недосконалим у сфері боротьби з кіберзлочинністю[1; 2]. У вітчизняному законодавстві є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерних систем та мереж електрозв'язку. У Кримінальному кодексі України окремі види комп'ютерних злочинів (кіберзлочинів) виділено в окремий розділ VI Особливої частини – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» (ст. 361, 361, 363 КК). Деякі види злочинів, у яких комп'ютерні продукти визначено як засіб злочину, розміщені в інших розділах Особливої частини – розділі V «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» (ст. 163, 176, 177 КК), розділі VII «Злочини у сфері господарської діяльності» (ст. 200 КК) [3].

Треба відзначити, що організовані злочинні угрупування, намагаючись діяти конспіративно, забезпечують високий рівень власного захисту і одночасно постійну готовність до активної протидії органам внутрішніх справ у виявленні й розслідуванні злочинів. Але практика свідчить, що діяльність оперативно-розшукових і слідчих підрозділів органів внутрішніх справ постійно збагачується певним практичним досвідом у тому числі і в протидії кіберзлочинності. Для протидії кіберзлочинам створюються спеціальні підрозділи і структури. Їхні повноваження постійно розширюють, а технічні можливості посилюють. Слід зазначити, що в Україні Департамент по боротьбі з кіберзлочинністю МВС України було створено у грудні 2011 р., а відповідні територіальні підрозділи почали створюватися лише на початку 2012 р. Специфіка роботи зазначеного підрозділу полягає не тільки у знанні правових аспектів і законодавчих норм, які є підставами для притягнення до відповідальності за кіберзлочини, а й глибоке знання технічної сторони діяння. Дана обставина вказує на необхідність удосконалення тактики проведення негласних слідчих (розшукових) дій, шляхом більш активного застосування оперативно-технічних заходів. Цьому сприяє впровадження нового Кримінального процесуального кодексу

України, а також розроблені МВС України нові нормативно-правові акти.

Для вдосконалення організації діяльності оперативних підрозділів ОВС на стадіях документування злочинних дій, реалізації оперативних матеріалів, кримінального провадження та судового розгляду видано наказ МВС України від 14.08.2012 № 700 «Про організацію взаємодії органів досудового розслідування з іншими органами та підрозділами внутрішніх прав України у попередженні, виявленні та розслідуванні кримінальних правопорушень» [4], в якому вимагається своєчасна реєстрація в ЄРДР матеріалів оперативно-розшукової діяльності, використання фактора раптовості під час затримки кіберзлочинців «на гарячому», а також приховання ступеня поінформованості про подальші плани розслідування. В процесі розслідування кримінальних правопорушень щодо діяльності організованих груп кіберзлочинців доцільно здійснювати проведення негласних слідчих (розшукових) дій:

а) введення в середовище співучасників, що залишилися на свободі, а також у коло їх корумпованих зв'язків інформаторів, що мають відповідні особисті й професійні якості для продовження активної оперативної розробки;

б) оперативне розроблення затриманих і заарештованих членів злочинної групи, починаючи з ІТТ і СІЗО;

в) візуальне спостереження у середовищі учасників кримінального процесу, їх службового і побутового оточення;

г) застосування оперативно-технічних засобів для контролю за поведінкою розроблюваних і документуванням їх діяльності щодо протидії здійсненню кримінального судочинства;

ґ) збереження об'єктів – носіїв доказової інформації [5].

Практика боротьби з кіберзлочинністю показала, що орієнтація тільки на технічні та технологічні засоби забезпечення інформаційної безпеки (технічного захисту інформації) в умовах інформатизації, у тому числі профілактики кіберзлочинів, не має значного успіху. Кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, проте на відміну від традиційних крадіжок і шахрайства, вона постійно удосконалюється і йде в ногу з технологіями, що у свою чергу ускладнює виявлення та протидію зазначеним протиправним діям.

Список використаних джерел:

1. Про оперативно-розшукову діяльність : закон України від 18.02.1992 №2135-XII // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.
2. Про організаційно-правові основи боротьби з організованою злочинністю : закон України від 30.06.1993 № 3341-XII // Відомості Верховної Ради України. – 1993. – № 35. – Ст. 358.
3. Кримінальний кодекс України [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14. – Редакція від 04.07.2013.
4. Про організацію взаємодії органів досудового розслідування з іншими органами та підрозділами внутрішніх прав України у попередженні, виявленні та розслідуванні кримінальних правопорушень : наказ МВС України від 14.08.2012 року № 700 [Електронний ресурс] – Режим доступу: http://document.ua/pro-organizaciyu-vzaemodiyi-organiv-dosudovogo-rozsliduvannj-doc119907.html.
5. Пчолкін В. Д. Особливості розкриття злочинів у кредитно-банківській сфері / В. Д. Пчолкін // Вісник Львівського інституту внутрішніх справ. – 1999. – № 2 (10). – С. 77–88.

Одержано 06.11.2013

УДК [347.132:347.53]:004

Євген Олександрович МІЧУРІН,
професор кафедри охорони інтелектуальної власності, цивільно-правових дисциплін факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ БОРОТЬБИ З КІБЕРЗЛОЧИНАМИ

Майже класичною стала фраза, що будь-який злочин має економічну підставу. Склади злочинів чимало в чому базуються на економічній зацікавленості осіб, що їх скоюють у кримінальному (що підпадає під склад злочину) результаті – незаконному заволодінні майном чи результатами інтелектуальної власності, інформацією. Цивільне право у свою чергу дозволяє дійти висновку, чи існує база для злочину, чи має місце саме порушення права власності або права інтелектуальної власності, права на інформацію, інших охоронюваних прав та інтересів особи. Адже якщо підставою для переходу права на інформацію, об'єкт права інтелектуальної власності, майно є не протиправне заволодіння ними, а належним чином укладений цивільний договір, той казати про злочин у

ряді випадків не доводиться. Отже, цивільне право є підґрунтям для встановлення норм права, що регулюють економічні відносини у державі. Економічні, що врегульовані правом відносини можуть виходити за межі приватних, коли вони грубо порушуються (незаконне заволодіння чужою власністю, інтелектуальною власністю). Тоді вони переходять у публічну сферу і підпадають під кримінальне, адміністративне законодавство. Якщо у цивільному праві захист прав є справою особи, права якої порушені, у сфері публічних правовідносин правоохоронні органи держави охороняють її інтереси, до яких зокрема належить стабільність відносин інтелектуальної власності, приватної та державної власності. Отже, цивільне право є базисом для того, щоб вірно класифікувати наявність чи відсутність порушення законодавства, що підпадає під публічне правове регулювання, відповісти на запитання, чи є заволодіння власністю безпідставним, чи навпаки за наявності підстав (договір, заповіт тощо) казати про це неможна. Утім навіть якщо було укладено цивільний правочин з передання права власності чи об'єкту права інтелектуальної власності не завжди можна казати про правомірність таких відносин, адже у цивільному праві чинним є не будь-який правочин, а лише той, що відповідає вимогам закону та належним чином укладено.

У сфері кіберзлочинності слід виділити три найбільш характерні групи порушень, що не відповідають цивільному законодавству та можуть стати підставою для кримінального провадження.

Першу групу складають порушення права інтелектуальної власності. Адже при всіх видах кіберзлочинів особи зазвичай використовують програмне забезпечення з порушенням закону (неліцензійні програми), без одержання дозволу від осіб, що мають право інтелектуальної власності на ці об'єкти.

Другу групу складають порушення права на інформацію. Останнім часом набувають розповсюдження злами баз даних, інших інформаційних ресурсів, що належать приватним особам чи державним установам. Потім ці бази даних можуть використовуватися для різного роду злочинних дій: шантажу, боротьби з конкурентами шляхом передання конференційних відомостей про порушення закону конкурентами до правоохоронних органів. До інших порушень цієї групи відноситься використання інформаційних баз даних для

подальших злочинних дій. Відомим став нещодавній випадок спроби продажу будівлі на Хрещатику (що була зупинена правоохоронними органами) за підробленими правовстановлювальними документами про право власності. При чому у підроблених документах фігурував справжній власник будівлі і було посилання на дійсний договір, за яким він придбав цю будівлю. Для цього треба було мати відомості з електронного Державного реєстру прав власності на нерухоме майно і дістати їх було можливим шляхом зламу (незаконного проникнення) до цієї електронної бази даних про власників нерухомості. До цієї ж групи правопорушень слід віднести так звані «хакерські» атаки на сайти державних установ, що блокують доступ до цих електронних ресурсів. Це чималою мірою блокує діяльність окремих сфер діяльності державних установ чи осіб, що правомірно звертаються до вказаних ресурсів. Так, для внесення даних у Державний реєстр прав власності на нерухоме майно нотаріус при посвідченні правочину з відчуження нерухомості має внести дані про нового власника до цього електронного ресурсу. У іншому випадку нотаріальна дія не зможе бути вчинена належним чином. Тому доступ до цих електронних баз даних є вкрай важливим, а блокування електронних ресурсів зазвичай є протиправним.

До третьої групи слід віднести порушення права власності шляхом заволодіння через електронні системи. Адже окрема група злочинів у сфері кіберзлочинності спрямована на незаконне заволодіння грошима з банківських рахунків. Для цього підробляються платіжні картки шляхом випуску їхнього дублікату з аналогічним магнітним кодом стрічки, що зчитується банкоматом. Така картка сприймається зчитуючим пристроєм банкомату як оригінальна і у момент зняття коштів за допомогою дублікату карти особою, що не є власником рахунку відбувається порушення права власності на кошти, що дозволяє казати про незаконне заволодіння ними (крадіжку).

Таким чином с лід виділити такі аспекти. Цивільне право регулює інститути права власності, права інтелектуальної власності та інші, грубе порушення правового регулювання яких підпадає під сферу публічного права (злочини проти права власності, порушення права інтелектуальної власності). У сфері кіберзлочинності слід виділити три найбільш характерні групи порушень, що не відповідають цивільному законодавству та можуть стати підставою для кримінального

провадження: порушення права інтелектуальної власності (використання не ліцензованих програм); порушення права на інформацію; порушення права власності шляхом заволодіння через електронні системи.

Одержано 12.11.2013

УДК 65.012.8+004

Андрій Вікторович ВІНАКОВ,
начальник відділу нагляду за додержанням законів органами внутрішніх справ при провадженні оперативно-розшукової діяльності прокуратури Харківської області

ДЕЯКІ ПИТАННЯ УДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ВІДПОВІДНОГО ПРОКУРОРСЬКОГО НАГЛЯДУ

На сьогоднішній день в Україні спостерігається зростання кількості оперативно-технічних заходів та негласних слідчих (розшукових) дій з використанням інформаційно-телекомунікаційних систем. Це, очевидно, викликано суттєвим збільшенням використання комп'ютерних систем правопорушниками.

Злочинці все частіше застосовують системний підхід при плануванні своїх дій, розробляють оптимальні варіанти проведення і забезпечення кримінальних «операцій», створюють системи конспірації і прихованого зв'язку, вживають додаткові заходи з протидії правоохоронним органам, використовують сучасні технології і спеціальну техніку, зокрема всілякі комп'ютерні пристрої і нові інформаційно-обчислювальні технології [1, с. 16–17]. Як відмічають В. Філіповський та Д. Погоржельський підозрювані особи найбільш часто використовують у своїй діяльності передплачені мобільні телефони, Інтернет у якості джерела інформації, мережні технології комунікацій (gadu-gadu або Skype), електронний банкінг, емейл, чати, форуми. Незначна кількість підозрюваних використовує шифрування інформації та онлайн-казино [2, с. 145].

Оскільки застосування комп'ютерної техніки злочинцями з кожним роком лише зростатиме, то і кількість відповідних інтрузивних заходів щодо них невпинно збільшуватиметься, а відтак потребує відповідного кількісного посилення і прокурорський нагляд за такою діяльністю, особливо у контексті

використання оперативними працівниками та слідчими під час її провадження інформаційно-телекомунікаційних систем.

З приводу такої негласної слідчої (розшукової) дії, передбаченої ст. 264 Кримінального процесуального кодексу, як зняття інформації з електронних інформаційних систем хотілося б зауважити, що у п. 1.14.1 Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затвердженої Наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5/ зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту, було віднесено до негласних слідчих (розшукових) дій.

Це, на нашу думку, є неприпустимим, оскільки суперечить логіці закону. Адже, виходить, що якщо, наприклад, слідчий доручить здійснити розшук підозрюваного оперативному працівнику, а той вирішить скористатися для цього комп'ютерними соціальними мережами, то відповідно він вже буде здійснювати описану негласну слідчу (розшукову) дію, здобуваючи відомості з електронних інформаційних систем або її частини (серверу соціальної мережі), доступ до яких не обмежується її власником, володільцем або утримувачем (відкритих для загального доступу). Звідси випливає, що під час здійснення вказаних дій має бути дотримана процедура, встановлена для негласних слідчих (розшукових) дій Кримінальним процесуальним кодексом України.

Такі ж саме ускладнення можуть виникати й щодо здійснення аналогічного оперативно-розшукового заходу. Тому потрібно негайно внести зміни до згаданої інструкції, скасувавши пункт 1.14.1.

Як відомо ст. 8 Закону України «Про оперативно-розшукову діяльність» містить бланкетну норму, яка відсилає до Кримінального процесуального кодексу в частині проведення окремих оперативно-розшукових заходів.

Так, якщо за результатами зняття інформації з електронних інформаційних систем будуть отримані відомості, які не

є потрібними для проведення оперативно-розшукової діяльності, то прокурор, як правило, приймає рішення про їх знищення.

Водночас згідно з п. 4 ст. 255 Кримінального процесуального кодексу України таке знищення здійснюється під контролем прокурора. Стосовно проведення відповідних оперативно-розшукових заходів вказана норма може бути розтлумачена як дозвіл прокуророві в окремих випадках на виконання контрольної функції, хоча у ч. 2 ст. 9 Закону України «Про оперативно-розшукову діяльність» надано вичерпний перелік відповідних контролюючих суб'єктів, серед яких відсутня прокуратура. Тому формулювання п. 4 ст. 255 Кримінального процесуального кодексу України, на нашу думку, є не зовсім коректним та потребує удосконалення. Вказану норму можна викласти так:

«знищення відомостей, речей та документів здійснюється під **наглядом** прокурора».

Враховуючи, що нагляд прокуратури в описаній сфері є досить новим напрямом, важливо зосередити зусилля юристів-науковців щодо вивчення цієї проблематики не лише в Україні, але й об'єднати науковий потенціал теоретиків і практиків, перш за все, з європейськими та американськими колегами, які вивчають нагляд прокуратури за здійсненням високотехнологічних спеціальних заходів у кримінальному процесі.

Список використаних джерел:

1. Тлиш А. Д. Проблемы методики расследования преступлений в сфере экономической деятельности, совершаемых с использованием компьютерных технологий и пластиковых карт : дис. … канд. юрид. наук : спец. 12.00.09 «Уголовный процесс, криминалистика и судебная экспертиза; оперативно-розыскная деятельность» / Тлиш Арсен Даурович. – Краснодар, 2002. – 254 с.

2. Filipkowski W. Technological aspects of the fight against organized crime in the opinion of public prosecutors [Електронний ресурс] / W. Filipkowski, J. Pogorzelski // Current Problems of the Penal Law and Criminology. – Wolters Kluwer Polska – LEX. – P. 135–152. – Режим доступу: http://www.researchgate.net/publication/229139918_Technological_aspects_of_the_fight_against_organized_crime_in_the_opinion_of_public_prosecutors.

Одержано 13.11.2013

УДК 004.77

Виктор Викторович ТЕНЯЕВ,
кандидат физико-математических наук, доцент,
заместитель начальника кафедры математики
и информационных технологий управления
Академии Федеральной службы исполнения наказаний России,
Николай Петрович ЛАДАРЕВ,
курсант
Академии Федеральной службы исполнения наказаний России

ПРЕДПОСЫЛКИ МИРОВОЙ КИБЕРВОЙНЫ

XXI век – это век великих компьютерных открытий, век создания новейших технологий и техники. Мир, вокруг нас, развивается так быстро, что мы не всегда успеваем быть в курсе всех новшеств, произошедших в нем. Но такое быстрое развитие имеет как положительные, так и отрицательные стороны. Сегодня компьютеры обеспечивают жизнедеятельность практически во всех важных сферах деятельности, начиная от контроля давления в нефтепроводе, а заканчивая контролем над работой больниц, экстренных служб и армии. Данные системы функционируют с использованием программного обеспечения и соответственно уязвимы для вредоносных программ – вирусов, которые могут привести к феноменальным последствиям с нанесением экономического и физического ущерба сопоставимого с воздействием обычных вооружений. Хочу обсудить понятие кибервойны, ее основные цели, с помощью чего ведется война такого рода, о примерах данных войн и об их опасности.

Кибервойна (англ. Cyber-warfare) – компьютерное противостояние в пространстве Интернета. Направлена, прежде всего, на дестабилизацию компьютерных систем и доступа к интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран, которые полагаются на интернет в повседневной жизни.

Специалисты выделяют следующие виды атак в интернете:

– вандализм;
– пропаганда;
– сбор информации;
– отказ сервиса;
– вмешательства в работу оборудования;
– атаки на пункты инфраструктуры [1].

Так для чего же ведется кибервойна? Ответ на этот вопрос не заставил себя долго ждать. Любые организации, государственные структуры, и другие образования зависят от сети интернет, поэтому любое развитое государство рассматривает сеть интернет как оружие, с помощью которого можно нанести значительный ущерб экономике и создать разлад в повседневной жизни другого государства.

Кроме того, разведывательные организации многих стран занимаются шпионажем в интернете: собирают информацию, взламывают компьютерные системы других государств, занимаются диверсионной деятельностью и экономическим шпионажем.

Рассмотрим кибервойну на конкретном примере: несколько лет назад в сетях ближневосточного региона появился вирус **Stuxnet** – предположительно, совместная разработка США и Израиля. Основной целью **Stuxnet** были промышленные объекты на иранских заводах и атомных станциях. Червь отличался особой живучестью и мог поразить любое устройство через обычную флешку – в результате его работы понесли ущерб тысячи центрифуг на заводе по обогащению урана в Натанзе. Каждое заражённое устройство с доступом к интернету оказывалось под контролем создателей вируса и передавало внутреннюю информацию. Таким образом, иранская атомная промышленность чуть не оказалась под управлением разработчиков **Stuxnet**.

В 2012 году сотрудниками из «Лаборатории Касперского» был идентифицирован новый вирус **Flame**, который изымал и удалял информацию с компьютеров Министерства нефти и газа Ирана. Для расследования подробностей атаки в «Лабораторию» обратился Международный союз электросвязи ООН. Если на расшифровку **Stuxnet** ушло полгода, то код **Flame**, по словам Александра Гостьева, главного специалиста «Лаборатории Касперского» в области защиты данных, был в 20 раз сложнее. Предполагаемый срок его расшифровки – около 10 лет. Из-за своего большого объёма (20 Мб) **Flame** закачивался по частям, чтобы записывать происходящее вокруг компьютера на микрофон, сканировать окрестности с помощью Bluetooth, каждые 15 секунд отсылать хакерам скриншоты с экрана и мониторить локальные сети на предмет сбора паролей и логинов. Это был действительно очень агрессивный вирус, чьи возможности просто поражали воображение [2].

Таким образом, открытых военных конфликтов между развитыми государствами, я думаю, ожидать не стоит. Война, в обычном представлении, нанесет огромный вред окружающей среде и принесет колоссальные человеческие жертвы, а на такое не пойдет ни одно развитое государство. Я считаю, что нужно как можно больше средств направлять на защиту компьютерных сетей, задействованных в управлении страной. Если «враги» смогут создать вирус, который будет способен контролировать важнейшие промышленные объекты, то наша обычная армия окажется бессильна и война будет проиграна, даже не начавшись. Не загарами тот день, когда сценарии боевых действий будут разворачиваться на мониторах воюющих стран, поэтому мы должны быть готовы к любой войне.

Список использованных источников:

1. Кибервойна [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Кибервойна.

2. Платов В. США и кибервойны. Часть 1 / Владимир Платов // Новое Восточное Обозрение : интернет-журнал [Электронный ресурс]. – Режим доступа: http://ru.journal-neo.org/2013/10/15/russsha-i-kibervojny-chast-1.

Одержано 12.11.2013

УДК 316.774

Анна Сергіївна ПОЛІТОВА,
кандидат юридичних наук,
начальник відділу міжнародних зв'язків
Донецького юридичного інституту МВС України

КІБЕРЗЛОЧИНИ: ПРОБЛЕМИ ВИЗНАЧЕННЯ

На сучасному етапі суспільні відносини не можуть існувати та нормально функціонувати без інформаційного обміну в інформаційно-телекомунікаційних системах. Процес інформатизації сучасного суспільства привів до того, що інформація перетворилася на своєрідний стратегічний ресурс, який володіє цінністю, тобто має якість товару. В свою чергу, впровадження сучасних інформаційних технологій в економіці, управлінні, кредитно-банківській діяльності, стрімкий розвиток інформаційно-телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет та спрощення доступу до неї широкого кола користувачів

через персональні комп'ютери – обумовило зростання злочинних проявів у зазначеній сфері.

Серед дослідників досі не існує єдиної точки зору щодо визначення «кіберзлочинності» чи «комп'ютерного злочину» або злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

Так, на погляд одних вчених, до комп'ютерної злочинності відносяться всі протизаконні дії, за яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом [1, с. 14], або всі протизаконні діяння, предметом і засобом здійснення яких є процедури й методи, а також процес комп'ютерного опрацювання даних [2, с. 72]. Пропонується і таке визначення комп'ютерних злочинів: «усі протизаконні дії, при яких електронне опрацювання інформації було засобом їх вчинення або їх об'єктом» [3, с. 65]. Іноді до комп'ютерних злочинів зараховують «злочини, пов'язані з втручанням у роботу комп'ютерів, і злочини, що використовують комп'ютери як необхідні технічні засоби» [4, с. 11]. А. Н. Караханьян під комп'ютерними злочинами розуміє протизаконні дії, об'єктом або знаряддям вчинення яких є ЕОМ [5, с. 243]. В. О. Голубєв уважає, що основна класифікуючи ознака належності злочинів до розряду комп'ютерних – це «використання засобів комп'ютерної техніки» [6, с. 39–40]. В. Лісовий визначає цю ознаку інакше – «електронна обробка інформації» – незалежно від того, на якій стадії злочину вона застосовувалася [7, с. 87]. Пропонується і таке визначення комп'ютерної злочинності, як порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [8, с. 387].

Щодо поняття «кіберзлочинності», то під нею розуміють злочинність в традиційному сенсі цього слова, але яка має місце в мережі Інтернет [9, с. 165]. Н. В. Савчук вважає, що кіберзлочинність – 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 [10, с. 338]. Поняття «кіберправопорушення» С. В. Мельник визначає як суспільно небезпечне винне діяння, яке здійснюється з використанням технологій перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді

комп'ютерних даних, і тягне за собою юридичну відповідальність. Відповідно, до кіберзлочинів слід віднести найбільш небезпечні кіберправопорушення за які встановлюється кримінальна відповідальність [9, с. 165]. А. М. Супруненко та М. С. Гожий під кіберзлочинністю вважають комплексне поняття, яке охоплює комп'ютерну злочинність та інші зазіхання при яких комп'ютер (ноутбук, планшет, смартфон та інші електронно-обчислювальні пристрої) виступає знаряддям або способом вчинення злочину проти громадської безпеки, моралі, авторських прав тощо [11, с. 56].

Деякі автори вважають, що сфера вчинення інтернет-злочинів – так званий віртуальний простір, який можна визначити як модельований за допомогою комп'ютера інформаційний простір, де містяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді і що перебувають у процесі руху по локальних і глобальних комп'ютерних мережах, або ж відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі [12].

Отже, проведений нами аналіз лише деяких понять «кіберзлочин», «комп'ютерний злочини», «Інтернет-злочин», дозволяє зробити наступний висновок: у міжнародних актах і нормативно-правових актах України необхідно закріпити загальновизнане поняття «кіберзлочинності», що дозволить більш точно визначити його межі, а також дозволить правильно кваліфікувати дії винних осіб.

Список використаних джерел:

1. Калюжный Р. А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. … д-ра юрид. наук : спец. 12.00.02 «Государственное право и управление; административное право; финансовое право» / Калюжный Ростислав Андреевич. – К., 1992. – 47 с.

2. Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д. Азаров // Право України. – 2000. – № 12. – С. 69–73.

3. Комп'ютерна злочинність : [навч. посіб.] / Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. [та ін.]. – К. : Атіка, 2002. – 240 с.

4. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юрид. лит., 1991. – 157 с.

5. Правовая информатика и кибернетика : учебник / [Атанесян Г. А., Гаврилов О. А., Дёри П. и др.] ; под ред. Н. С. Полевого. – М. : Юрид. лит., 1993. – 528 с.

6. Голубєв В. О. Правові проблеми захисту інформаційних технологій / В. О. Голубєв // Вісник Запорізького юридичного інституту. – 1997. – № 2. – С. 35–40.

7. Лісовий В. «Комп'ютерні» злочини: питання кваліфікації / В. Лісовий // Право України. – 2002. – № 2. – С. 86–88.

8. Дашян М. С. Право информационных магистралей / М. С. Дашян. – М. : Волтерс Клувер, 2007. – 288 с.

9. Юрасов А. В. Основы электронной коммерции : [учебник] / А. В. Юрасов. – М. : Горячая линия – Телком, 2008. – 480 с.

10. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби [Електронний ресурс] / Н. В. Савчук // Теоретичні та прикладні питання економіки. – Вип. 19. – 2009. – С. 338–342. – Режим доступу: http://archive.nbuv.gov.ua/portal/Soc_Gum/Tppe/2009_19/Zb19_48.pdf.

11. Супруненко А. М. Кіберзлочинність як особливий вид протиправної поведінки / А. М. Супруненко, М. С. Гожий // Боротьба з Інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (м. Донецьк, 12–13 черв. 2013 р.). – Донецьк : ДЮІ МВС України, 2013. – С. 55–57.

12. Кіпа О. О. Правопорушення в мережі Інтернет / О. О. Купа // Часопис Київського університету права. – 2010. – № 4. – С. 346–349.

Одержано 18.11.2013

УДК [341.48:004](4)

Сергій Павлович ЛАПТА,
кандидат юридичних наук, доцент, заступник начальника кафедри криміналістики, судової медицини та психіатрії Харківського національного університету внутрішніх справ

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ У ЄВРОСОЮЗІ

Науково-технічний прогрес та створення глобальних кібертехнологій стали також причиною виникнення кіберзлочинності, яка постійно набирає обертів. За даними Інтерполу, у Європі збитки від дій кіберзлочинців щорічно складають більш ніж 300 млрд. євро і кожного дня жертвами кіберзлочинів стає біля мільйону європейських громадян. Інтернет-злочинці викрадають номери та пін-коди банківських карток, зламують бази даних на серверах, персональних комп'ютерах та смартфонах, заволодівають профілями користувачів у соціальних мережах. При цьому, цілий ряд інтернет-видань

вважає, що ці проблеми – тільки початок того, що в майбутньому може чекати на суспільство.

З метою боротьби зі злочинними проявами у мережі Інтернет 23 листопада 2001 року у Будапешті Радою Європи була прийнята Конвенція про кіберзлочинність[1]. З того часу конференції з проблем інтернет-безпеки у Будапешті стали регулярними і с кожним разом все більше країн не тільки Європи, а й усього світу приймають у них участь.

Для координації зусиль у боротьбі з кіберзлочинами Комісією Євросоюзу була розроблена узгоджена політика співпраці між державами-членами ЄС та відповідними установами, що знайшло своє відображення у зверненні Єврокомісії до Європарламенту «Стратегії кібербезпеки Євросоюзу: відкритий, безпечний і надійний кіберпростір», де пропонується розширити співпрацю як на рівні правоохоронних органів окремих країн, так і глобальну міжнародну співпрацю [2].

Наступним кроком стало прийняття «Директиви про атаки проти інформаційних систем». Директива базується на правилах, що діяли з 2005 року (Council Framework Decision 2005/222/JHA). Зберігаючи ряд діючих положень, вона вводить нові види злочинів, такі як використання інструментів для великомасштабних атак, нові обставини, що обтяжують відповідальність та більш суворі санкції, які є необхідними для більш ефективної боротьби проти масштабних атак на інформаційні системи. Крім цього, Директива покращує міжнародне співробітництво між судовими органами та поліцією держав-членів та зобов'язує збирати статистичну інформацію про кібератаки і централізовано направляти її у компетентні органи. Протягом двох років з моменту опублікування Директиви у Офіційному віснику ЄС, держави-члени мають впровадити її положення у національні законодавства.

Слід зазначити, що поряд із позитивними моментами Директиви, інтернет-спільнота вбачає і деякі негативні, зокрема, щодо введення кримінальної відповідальності за виробництво, використання та продаж інструментів для атаки на інформаційні системи. До одних з найбільш важливих досліджень відносяться дослідження з пошуку вразливостей комп'ютерних систем, На думку членів правозахисної організації Electronic Frontier Foundation (EFF) програми, за використання яких згідно з Директивою настає кримінальна відповідальність,

можуть використовуватися не тільки для атак, а й для тестування систем на предмет вразливостей для посилення безпеки. Таким чином, під загрозу кримінальної відповідальності підпадають програмісти, які розробляють інструментарій для тестування вразливості інформаційних систем до кібератак. На думку членів EFF Європарламент повинен прописати у Директиві мету використання такого інструментарію, а не просто факт його «володіння, використання виробництва чи розповсюдження» [3].

У січні 2013 року за пропозицією Єврокомісії був створений і розпочав роботу Європейський центр з боротьби з кіберзлочинністю. Серед пріоритетів даної організації, яка здійснює свою діяльність під егідою Європолу зазначається розслідування випадків шахрайства через електронні мережі, зокрема, у сфері інтернет-банкінгу, накопичування інформації про кіберзлочини у Євросоюзі, узагальнення інформації щодо боротьби з кіберзлочинами та розповсюдження позитивного досвіду серед держав – членів ЄС, забезпечення підтримки досліджень, що проводяться у державах-членах ЄС із забезпечення кібербезпеки та узгодження заходів, направлених на боротьбу з кіберзлочинністю між судовими та правоохоронними органами держав – членів ЄС. Серед перших вагомих здобутків центру – викриття одної з найбільших шахрайських комп'ютерних мереж та арешт 11 членів злочинної організації. Дана мережа приносила своїм засновникам близько мільйона євро щорічно, використовуючи комп'ютери, що знаходилися у 33 країнах світу, у тому числі 22 країнах Європи. Гроші «відмивалися» злочинцями також з використанням інформаційних систем – різноманітних ігрових порталів, електронних платежів, шлюзів та віртуальних грошей [4].

Список використаних джерел:

1. Convention on Cybercrime : Budapest, 23.11.2001 [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

2. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace : Joint communication to the European parliament, the Council, the European economic and social committee and the Committee of the regions : JOIN(2013) 1 final : Brussels, 7.2.2013 [Електронний ресурс]. – Режим доступу: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

3. EFF требует защитить права программистов [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/420736.php. – 28.02.2012.

4. Европейский центр по борьбе с киберпреступностью демонстрирует свои первые результаты // Europa. Новости с европейским акцентом [Електронний ресурс]. – Режим доступу: http://euroua.com/europe/eu/1762.

Одержано 19.11.2013

УДК 343.1

Андрій Анатолійович ВАСИЛЬЄВ,
кандидат юридичних наук,
заступник начальника кафедри кримінального права та кримінології факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ,
Дмитро Валентинович ПАШНЄВ,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права та кримінології факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

ЄДИНИЙ ЦЕНТРАЛЬНИЙ ОРГАН УКРАЇНИ З МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ЩОДО ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV зі змінами, внесеними Законом України «Про внесення змін до Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 21.09.2010 № 2532-VI, фактично визначає три органи, які мають повноваження відносно здійснення міжнародного співробітництва у протидії кіберзлочинності: Міністерство юстиції України (щодо запитів судів) та Генеральна Прокуратура України (щодо доручень органів досудового слідства) є органами, відповідальними за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам, а Міністерство внутрішніх справ України є органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі.

Національний контактний пункт (НКП), на базі якого створено та функціонує вказана цілодобова контактна мережа, знаходиться в складі оперативного підрозділу – Управління боротьби з кіберзлочинами (УБК). У випадках, якщо цією мережею надходить запит від оперативного підрозділу іноземної держави, то УБК має право безпосередньо його виконати. Проте, відповідно до чинного законодавства, виконання запитів від органів досудового розслідування не входять до його компетенції.

Згідно положень нового КПК України та Закону України «Про оперативно-розшукову діяльність», проведення оперативним підрозділом процесуальних дій, без вчинення яких фактично неможливе здійснення МВС України вказаних вище функцій, можливе лише за дорученням органів досудового розслідування, або прокурора. Крім того, запит про міжнародну допомогу від органів досудового слідства повинен проходити процедуру документального оформлення в Генеральній Прокуратурі України, навіть якщо надійшов через цілодобову контактну мережу.

Таким чином, МВС України, у складі якого знаходиться УБК – підрозділ, основним завданням якого є протидія кіберзлочинності, – фактично позбавлений права виконувати ці обов'язки в сфері міжнародної правової допомоги без залучення до цього процесу Генеральної Прокуратури України.

Відповідно до п. 2b ст. 35 Конвенції про кіберзлочинність «якщо орган Сторони, визначений нею для здійснення контактів, не є частиною уповноваженого органу або органів такої Сторони, які відповідають за міжнародну взаємну допомогу або екстрадицію, то орган, визначений для здійснення контактів, забезпечує свою здатність проводити термінову координацію з таким уповноваженим органом або органами». Але забезпечення такої термінової координації між Генеральною Прокуратурою України та мережею, яка працює цілодобово, у реаліях сьогодення уявляється нездійсненним.

Фактично відбувається значне ускладнення процедури виконання запиту про міжнародну правову допомогу, що у ситуації розслідування кіберзлочину має критичний характер, адже затягування із виконанням запиту робить його результат фактично нульовим, зважаючи на швидкість руху комп'ютерної інформації, нестійкість та недовговічність електронних доказів та інші фактори.

За загальним правилом, Центральний орган України, через який здійснюється міжнародне співробітництво в ході кримінального провадження, визначається ст. 545 КПК України. Відповідно до ч. 3 цієї статті, якщо чинним міжнародним договором України передбачено інший порядок зносин, на визначений законодавчим актом орган поширюються повноваження Центрального органу України.

Очевидно, що зміст Конвенції про кіберзлочинність свідчить про особливий порядок зносин між державами стосовно надання міжнародної правової допомоги при розслідуванні кіберзлочинів. Отже, на наш погляд, доцільним є об'єднання всіх функцій (крім запитів про екстрадицію або тимчасовий арешт, які слід залишити Міністерству юстиції України) щодо міжнародного співробітництва стосовно кіберзлочинів в рамках повноважень одного органу, який і буде в цій сфері центральним органом України в значенні статті 545 КПК України.

Таким органом найбільш доцільно визначити МВС України, в складі якого функціонує Управління боротьби з кіберзлочинністю – для виконання запитів оперативних підрозділів, і слідчі підрозділи – для виконання запитів органів досудового слідства інших держав.

Одержано 11.11.2013

УДК 343.915

Вадим Миколайович БАБАКІН,
кандидат юридичних наук, доцент, докторант
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ МОЛОДІЖНІЙ ЗЛОЧИННОСТІ ЩОДО РОЗПОВСЮДЖЕННЯ У МЕРЕЖІ ІНТЕРНЕТ ІНФОРМАЦІЇ КСЕНОФОБНОГО ТА ПОРНОГРАФІЧНОГО ХАРАКТЕРУ

Одним з негативних соціальних і економічних наслідків науково-технічного прогресу варто визнати криміналізацію сфери використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. На сьогодні у світі поширено міграційні процеси, що впливає на змішення національних верств населення, що особливо простежується у країнах Європи. Це відповідним чином впливає й на переміщення людей різних релігійних

поглядів, проблем їх сумісного спілкування, дотримання різних традицій, релігійних обрядів в одному регіоні. Особливо нестійкими є погляди молоді до протилежних національних і релігійних концесій та поглядів, їх реагування на особливості та специфіку відправлення релігійних та інших обрядів тощо.

На нашу думку, на даний момент однією із найбільш нагальних проблем для країн світу і України є саме поширення в мережі Інтернет різних видів інформації расистського, ксенофобного, та іншого характеру, яка підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб, що ґрунтується на расовій, національній, релігійної або етнічної приналежності (в законодавстві України відповідальність за такі дії передбачена в ч. 2 та ч. 3 ст. 109, ст. 258-2, 295, 300, 436, ч. 2 ст. 442, КК України, а також дитячої порнографії та матеріалів порнографічного характеру (в законодавстві України відповідальність за такі дії передбачена в ст. 300 КК України. Піднята проблема полягає в тому, що будь-який користувач мережі Інтернет, з яких найбільша частина це особи молодого віку, має змогу отримати доступ до електронного ресурсу, на якому розміщена зазначена вище інформація, навіть якщо він навіть не знає назви даного Інтернет сайту. Достатньо лише ввести пошуковий запит «дивитись порнографію», чи «дивитись порно», чи «відео про вбивство» до пошукової системи, зокрема до такої як пошукової системи «Google», і користувач отримає відповідь на свій запит у вигляді посилань на інтернет-ресурси, на яких і розміщена інформація, щодо якої у користувача виник інтерес. Навіть якщо батьки на домашніх комп'ютерах своїх дітей поставлять спеціальні програмні фільтри для того, щоб діти не мали змоги отримати режим доступу до заборонених батьками інтернет-ресурсів, ніщо не заважатиме дітям отримати режим доступу до цих інтернет-ресурсів з інших комп'ютерів. І це є великою проблемою для будь якої країни, адже за таких умов в мережі Інтернет можливо розміщувати аудіо, відео, текстові та графічні матеріали будь-якого змісту, і кожен пересічний громадянин матиме змогу ознайомитись із інформацією, що містить в собі, наприклад, заклики до повалення конституційного ладу в країні, чи відеофільм дитячої порнографії.

Якщо інтернет-сайти розміщені на комп'ютерах, що фізично перебувають на території України, та на яких розміщена

інформація, розміщення та розповсюдження якої підпадає під склад певного виду злочину Кримінального кодексу України, то це ще невелика проблема для правоохоронних органів. Але часто буває так, що такі Інтернет сайти розміщені на комп'ютерах, які фізично перебувають, наприклад, на Філіппінських островах, і тоді припинити режим доступу до таких сайтів становить проблему для українських правоохоронців, ускладнює протидію таких кримінальних правопорушень.

Фізично, будь-які Інтернет ресурси розміщені на певних комп'ютерах, що розміщені по всьому світу. Для того, щоб будь-який користувач міг отримати доступ до певного ресурсу, данні про те, на якому саме комп'ютері розміщений той чи інший інтернет-сайт заносяться до спеціальних цифрових таблиць DNS-серверів, які фізично розміщені на території США. Проміжною ланкою між користувачем і DNS-сервером є інтернет-провайдер, тобто юридична особа, яка платно чи безоплатно забезпечує зв'язок між користувачем, DNS-сервером, та інтернет-сайтом, режим доступу до якого хоче отримати користувач. На території України існує безліч інтернет-провайдерів, але їхня діяльність ґрунтується лише на законах та підзаконних актах України. А оскільки будь-який Інтернет провайдер може налаштувати програмні фільтри так, щоб користувачі підключені до нього не мали доступу до певного Інтернет сайту чи ресурсу, ми пропонуємо:

1) створити відповідний підрозділ в системі Міністерства внутрішніх справ України, на який би покладалось завдання по пошуку та виявленню інтернет-ресурсів, де розміщена інформація расистського, ксенофобного, та іншого характеру, яка підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб, що ґрунтується на расовій, національній, релігійної або етнічної приналежності, а також різних видів дитячої порнографії та матеріалів порнографічного характеру;

2) на законодавчому рівні створити Єдиний державний реєстр заборонених Інтернет ресурсів, до якого вносити інтернет-ресурси виявлені зазначеним вище підрозділом;

3) законодавчо закріпити зобов'язання інтернет-провайдерів вносити інтернет-ресурси, що потрапили до зазначеного вище Єдиного державного реєстру заборонених Інтернет ресурсів до своїх програмних фільтрів, з метою блокування режиму доступу до них користувачами мережі Інтернет;

4) зважаючи на те, що кожен день в мережі Інтернет з'являється багато нових інтернет-ресурсів, а вже існуючі можуть змінювати характер та склад інформації, яка розміщується на них, то доцільно регулярно проводити обновлення Єдиного державного реєстру заборонених інтернет-ресурсів, тобто включати до нього нові інтернет-ресурси, та виключати ті, які зі своїх сторінок видалили інформацію забороненого характеру.

Можна зробити висновок, що для реалізації зазначених пропозицій щодо протидії розповсюдженню забороненої законодавством інформації в мережі Інтернет і впровадження вищезазначеного, необхідно створити відповідну законодавчу базу. Втім підняті питання не є остаточними і підлягають додатковому дослідженню або науковому вивченню.

Список використаних джерел:

1. Настільна книга слідчого / [М. І. Панов, В. Ю. Шепітько, В.О.Коновалова та ін.] – 3-тє вид., переробл. і доповн. – К. : Ін Юре, 2011. – 736 с. : 49 іл.

2. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/254к/96-вр.

3. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К. : Юрінком Інтер, 2012. – 608 с.

4. Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 : ратиф. Верховною Радою України із застереженнями і заявами Законом № 2824-IV від 07.09.2005 // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.

5. Таненбаум Э. Архитектура компьютера. – 5-е изд. (+CD). – СПб. : Питер, 2007. – 844 с. : ил.

6. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія / Д. М. Цехан ; за наук. ред. О. О. Подобного. – О. : Юрид. л-ра, 2011. – 216 с.

Одержано 11.11.2013

УДК 347.511

Юлія Володимирівна ЖЕЖЕРУН,
викладач кафедри банківської справи Черкаського інституту банківської справи Університету банківської справи Національного банку України (м. Київ)

ВІТЧИЗНЯНИЙ ДОСВІД БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В БАНКІВСЬКІЙ СФЕРІ

За останні роки в Україні постійно зростає кількість інтернет-користувачів банківськими послугами, що зумовлено вільним доступом до мережі Інтернет, невпинним розвитком якісно нових галузей економіки та банківських послуг, поширенням соціальних мереж, Інтернет магазинів, розширенням переліку товарів та послуг, за які можна розрахуватись через мережу Інтернет. За даними міжнародних організацій в Україні налічується близько 15 млн інтернет-користувачів. Разом з тим, з кожним роком суттєво зростає кількість злочинів у банківській сфері з використанням мережі Інтернет. У вітчизняній юридичній літературі для визначення даної категорії злочинів найчастіше вживається термін «кіберзлочинність у банківській сфері».

Термін «кіберзлочинність» нерідко вживається як синонім терміну «комп'ютерна злочинність». На думку американських дослідників Сюзанн Бреннер і Марка Гудмана [0], термін «кіберзлочинність» охоплює як традиційні злочини, скоєні за допомогою комп'ютера (крадіжка, шахрайство, вимагання), так і злочини, в яких об'єктом є комп'ютерні системи, програми та дані.

Порівняльний аналіз досліджень зарубіжного досвіду боротьби з кіберзлочинністю свідчить, що вона має тенденцію до зростання. Однією з умов її зростання є ускладнення технічних систем глобального зв'язку і спрощення доступу до використання комп'ютерних технологій широкого кола користувачів через персональні комп'ютери. Дослідження проблем боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні та технологічні засоби забезпечення інформаційної безпеки (технічного захисту інформації) в умовах інформатизації, у тому числі профілактики кіберзлочинів, не має значного успіху. Особливо це відчувається з часу приєднання до міжнародних систем телекомунікації нових країн та підвищення інтелектуального рівня користувачів комп'ютерної техніки [3]. Якщо ще декілька років тому більшість кіберзлочинів

припадала на махінації з пластиковими картками, то на сьогодні найбільш поширеними є злочини у сфері онлайн-платежів. А саме, збільшується кількість хакерських атак рахунків підприємств через зараження вірусами комп'ютерів та втручання в роботу клієнт-банків з метою подальшої крадіжки коштів. За даними Управління по боротьбі з кіберзлочинністю, в 2012 році було зафіксовано 139 таких випадків, за 1 квартал 2013 року – 127. За оцінками Інтерполу прибутки від скоєння кіберзлочинів у банківській сфері посідають третє місце у світі після доходів від незаконного обігу наркотичних засобів та нелегального постачання зброї.

Як зазначає Є. Зозуля ефективна боротьба проти транснаціональної комп'ютерної злочинності та кібертероризму вимагає тісного, швидкого, ефективного й функціонального міжнародного співробітництва усіх державних структур (і щонайперше правоохоронних органів) у розслідуванні такого роду злочинів [4]. До нормативно-правових актів, що регулюють суспільні відносини у сфері інформаційної безпеки в Україні слід віднести: закони України «Про інформацію» № 2657-XII від 02.10.1992, «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994, «Про державну таємницю» № 3855-XII від 21.01.1994, «Про основи національної безпеки України» № 964-IV від 19.06.2003; укази Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» № 891 від 24.09.2001, «Про Положення про технічний захист інформації в Україні» № 1229 від 27.09.1999, «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» № 891/2000 від 14.07.2000 та ін. Як свідчить практика боротьби з кіберзлочинністю зазначені нормативні-правові акти потребують систематизації, шляхом прийняття Кодексу про інформацію, який сприятиме правовому забезпеченню боротьби з кіберзлочинами.

Верховною радою України створено спеціальні організаційні структури з питань організаційно-правового забезпечення боротьби з кіберзлочинністю, а саме: Урядову комісію з питань інформаційно-аналітичного забезпечення органів виконавчої влади, Міжвідомчий комітет з проблем захисту прав на об'єкти інтелектуальної власності, Міжвідомчу робочу групу з розроблення та узгодження Концепції легалізації програмних продуктів та боротьби з їх нелегальним використанням.

Як зазначає С. Каланча, проблема превентивних можливостей глобальних інформаційних мереж, у тому числі Інтернет, та використання їх для боротьби зі злочинами, причому не тільки зі специфічними комп'ютерними, а й іншими видами злочинів, особливо транснаціональними і організованими, сьогодні майже не освоєна кримінологією [2].

Таким чином, на сьогодні проблеми протидії кіберзлочинності набувають все більшої актуальності, оскільки з кожним роком зростають збитки вітчизняних банків та їх клієнтів від даного виду злочинів. При цьому особливої уваги заслуговують високотехнологічні злочини з використанням новітньої техніки та програмного забезпечення. Тому подальших досліджень потребують можливості попередження кіберзлочинності в банківській сфері.

Список використаних джерел:

1. Brenner S. W. The emerging consensus on criminal conduct in cyberspace [Електронний ресурс] / Suzan W. Brenner, Mark D. Goodman // UCLA Journal of Law and Technology. – 2002. – № 3. – Режим доступу: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php.

2. Каланча С. Г. Кіберзлочинність: шляхи попередження та протидії / С. Г. Каланча // Наше право. – 2012. – № 3, ч. 2. – С. 213–217.

3. Кіберзлочинність [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Кіберзлочинність.

4. Зозуля Є. Діяльність МВС України щодо протидії транснаціональній злочинності у сфері високих технологій / Є. Зозуля // Наукові записки. Серія: Історія. – 2011. – Вип. 1. – С. 205–211.

Одержано 20.11.2013

УДК 347.440.44

Олексій Леонідович ЗАЙЦЕВ,
кандидат юридичних наук, доцент,
начальник кафедри охорони інтелектуальної власності,
цивільно-правових дисциплін факультету підготовки фахівців
для підрозділів боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ЕТАПИ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ, ЯКІ МОЖУТЬ БУТИ ОБ'ЄКТОМ КІБЕРЗЛОЧИНУ

Основна мета тез (завдання) – це визначення основних суперечностей у законодавстві, що регулює державні, що може привести до скоєння кіберзлочину у цій сфері. Для

спрощення аналізу матеріалу тез та природи відносин, що виникають у державних закупівлях, визначимо основні етапи.

Етап перший (організаційний). Державні закупівлі розпочинаються з затвердження Річного плану закупівель на засіданні комітету з конкурсних торгів. Форма річного плану закупівель передбачена наказом Міністерства економічного розвитку і торгівлі від 26 липня 2010 року № 922 в редакції наказу від 27 грудня 2011 р. № 428 [1]. З цивілістичної точки зору річний план важливий тому що в ньому зазначається істотна умова майбутнього договору, а саме – предмет закупівлі. Річний план та зміни до нього надсилаються центральному органу виконавчої влади, що реалізує державну політику у сфері казначейського обслуговування бюджетних коштів, річний план, кошторис (тимчасовий кошторис), фінансовий план (план асигнувань, план використання бюджетних (державних) коштів), зміни до них надсилаються уповноваженому органу протягом п'яти робочих днів з дня їх затвердження. Відповідно до річного плану затверджується документація конкурсних торгів. До неї висуваються суворі формальні вимоги відповідно до наказу Міністерства економічного розвитку і торгівлі від 26 липня 2010 р. № 919 [2]. Річний план закупівель та зміни до нього оприлюднюються замовником шляхом розміщення на власному веб-сайті або за його відсутності на веб-сайті головного розпорядника бюджетних коштів протягом п'яти робочих днів з дня їх затвердження. Недосконалість процедури на цьому етапі полягає в тому, що атака на веб-сайт замовника з метою знищення річного плану в якості наслідку може мати відміну вже проведених торгів.

Етап другий (оприлюднення інформації про закупівлю). Протягом усієї процедури закупівлі від її початку і до подання документів на оплату замовник здійснює періодичні дії для публічного інформування спільноти про хід процедури із закупівлі. Для оприлюднення на веб-порталі уповноваженого органу [3] замовник надає таку інформацію про закупівлю:

– оголошення про проведення процедури закупівлі;

– обґрунтування застосування процедури закупівлі в одного учасника;

– документацію конкурсних торгів або кваліфікаційну документацію;

– протокол розкриття пропозицій конкурсних торгів, цінових пропозицій, кваліфікаційних пропозицій;

– інформацію про відхилення пропозицій конкурсних торгів, цінових пропозицій, кваліфікаційних пропозицій та підстави такого відхилення у вигляді протоколу;

– повідомлення про акцепт пропозиції конкурсних торгів або цінової пропозиції (пропозиції за результатами застосування процедури закупівлі в одного учасника);

– оголошення про результати процедури закупівлі;

– повідомлення про відміну торгів чи визнання їх такими, що не відбулися, повідомлення про відміну процедури закупівлі в одного учасника (у разі наявності);

– звіт про результати проведення процедури закупівлі.

Оголошення про проведення процедури закупівлі та про результати процедури закупівлі обов'язково додатково розміщуються в міжнародному інформаційному виданні з питань державних закупівель уповноваженого органу та на вебпорталі уповноваженого органу англійською мовою, якщо очікувана вартість закупівлі перевищує суму, еквівалентну: для товарів – 200 тис. євро; для послуг – 300 тис. євро; для робіт – 500 тис. євро.

За загальним правилом, публікації здійснюються безкоштовно у «Віснику державних закупівель» та за плату в «Announcer of the public purchasing» у письмовій та електронній формі. Порушення правил публікації нездійснення публікації перерахованої інформації тягне відповідальність за ст. 164-14 Кодексу України про адміністративні правопорушення [4]. Основним недоліком законодавства, яке регулює цей етап можна назвати: скорочені строки для безкоштовних публікації, неприпустимість помилок та складність їх виправлення [5], відсутність цивільно-правових наслідків недотримання процедури публікації замовником, відсутність прямого доступу до публікації центрального органу виконавчої влади, що реалізує державну політику у сфері казначейського обслуговування бюджетних коштів.

Етап третій (безпосередньо закупівля). Закупівля може здійснюватися шляхом застосування однієї з таких процедур: відкриті торги; двоступеневі торги; запит цінових пропозицій; попередня кваліфікація учасників; закупівля в одного учасника; електронний реверсивний аукціон. Найбільш незахищений вид закупівель з боку кібератак – це електронний реверсивний аукціон.

Як висновок можемо зазначити таке: по-перше, законодавство з державних закупівель потребує уніфікації та удосконалення особливо з кримінальним; по-третє, автор розуміє, що вищенаведені матеріали потребують ретельного аналізу та буде вдячний за раціональну критику з озвучених питань. Адреса автора – zal2207zal@ukr.net. Заздалегідь дякую.

Список використаних джерел:

1. Про затвердження форм документів у сфері державних закупівель : наказ М-ва екон. розвитку і торгівлі від 27.12.2011 № 428 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0624-10. – Редакція від 17.02.2012.

2. Про затвердження стандартної документації конкурсних торгів : наказ М-ва екон. розвитку і торгівлі від 26.07.2010 N 919 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0653-10.

3. Державні закупівлі [Електронний ресурс]. – Режим доступу: https://tender.me.gov.ua/EDZFrontOffice/.

4. Кодекс України про адміністративні правопорушення : від 07.12.1984 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/80731-10.

5. Інструкція подання, прийому та розміщення інформації про державні закупівлі в інформаційному бюлетені «Вісник державних закупівель» та на веб-порталі Уповноваженого органу «Державні закупівлі» : затв. наказом від 12.02.2013 № 25 [Електронний ресурс]. – Режим доступу: http://files.vdz.net.ua:8080/doc/instruction_VDZ.pdf. – Із змінами та допов., внес. наказами від 15.03.2013 № 46, від 21.08.2013 № 126.

Одержано 13.11.2013

УДК 343.96+343.326+343.341

Олексій Олександрович ДЕРЕВЯГІН,
кандидат юридичних наук,
доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту
підготовки фахівців для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ

НАЦІОНАЛЬНИЙ АСПЕКТ КІБЕРЗЛОЧИННОСТІ

Кількість кіберзагроз та кіберзлочинів в Україні та світі постійно зростає, але законодавство не встигає за цими процесами. Зі свого боку, правоохоронні органи хоч і намагаються мінімізувати, але невирішених проблем ще дуже багато -

знаходження балансу між анонімністю і необхідністю розкривати кіберзлочини, готовність провайдерів йти назустріч правоохоронцям, низька грамотність самих інтернет-користувачів. Різні аспекти зазначеної проблематики активно обговорюються на галузевих заходах, наприклад: на регіональній конференції ENOG 6 (Євро - азіатська група мережевих операторів)/RIPE NCC, Четвертому українському форумі з управління Інтернетом IGF – UA 2013, відомчих науково-практичних конференціях системи МВС України і деяких інших.

Україна знаходиться серед лідерів кіберзлочинів. За даними «Лабораторії Касперського», в I кварталі 2013 року наша країна займала «почесне» 5-те місце серед країн на вебресурсах яких, розміщені шкідливі програми. На той момент в Україні кількість зафіксованих інтернет-загроз перевищило 47 млн зразків, а зараженню через веб-ресурси в першому кварталі 2013 року піддалися 49 % українських користувачів [1]. З такими показниками Україна посіла 8-ме місце в списку країн, жителі яких піддаються найбільшому ризику зараження в Інтернеті.

По 2012 року Україна посіла 17-те місце в списку країн з найвищим відсотком комп'ютерних атак, а 47 % інтернет-користувачів в Україні стикаються з кібератаками [2]. Якщо порівнювати з даними 2011 року, то ситуація погіршилася. Роком раніше небезпеки піддатися атакам в Інтернеті в середньому піддавалися 45,^{n} %.

Також в 2012 році Україна зайняла дев'яте місце в світі за кількістю комп'ютерів, заражених популярними сімействами DDoS-ботів. На території України було зафіксовано 2,49 % комп'ютерів, заражених деякими популярними сімействами DDoS-ботів [2].

В цілому, у світі жертвами кіберзлочинців щодня стають один мільйон людей. Далі ситуація буде тільки погіршуватися, і Європейський центр по боротьбі з кіберзлочинністю при Європолі вже опублікував похмурий футурологічний прогноз з описом можливих сценаріїв розвитку кіберзлочинності в Європі до 2020 року [3].

Втім, в Україні до такого сценарію також готуються. Так, МВС розробило законопроект «Про кібернетичну безпеку України», в якому вперше вводяться поняття «кібербезпека» і «кіберпростір». А також розширюється список злочинів, які є

загрозою національній безпеці. До них пропонується віднести несанкціоноване втручання в роботу державних інформаційних ресурсів, пропаганду в Інтернеті культу насильства, жорстокості, порнографії та сепаратизму. При цьому Україна має «цифрову залежність» від зарубіжних виробників операційних систем, ПО, пошукових інтернет-ресурсів і т. д.

Заслуговують на не аби яку увагу й новини про електронний шпіонаж, які займають перші шпальти друкованих засобів масової інформації. Щорічно компанії втрачають мільярди доларів на втратах інтелектуальної власності та розкраданні комерційних таємниць із подальшим перепродажем конкурентам з метою вимагання та незаконного отримання прибутку. Корпоративні мережі по всьому світу є прекрасною мішенню для злочинців, здатних дістатися до інформації, минаючи всі системи захисту.

Електронний шпіонаж, інтернет-шпіонаж, кібершпіонаж – новітні види збору інформації, в основі яких лежать інформаційно-комунікаційні технології, що забезпечують процесам спостереження та стеження всюдисущість і повсюдність. Ступінь насиченості суспільства електронними пристроями та їх ефективність такі, що під контролем опиняються навіть стаціонарні предмети та предмети, які пересуваються у просторі, більшість подій, що відбуваються. Вони дозволяють точно фіксувати об'єкти та процеси, в реальному режимі часу передавати про них дані, класифікувати, обробляти інформацію та надавати її в потрібний час і в будь-яке місце для прийняття рішень, накопичувати, аналізувати та синтезувати величезні масиви даних, виділяти все цінне, що в них міститься, і зберігати стільки часу, скільки необхідно. За масштабами цей вид шпіонажу вже набагато перевершив особистісний канал отримання інформації, що домінував до недавнього часу [4, с. 64].

Варто зауважити, що в боротьбі з кіберзлочинністю МВС не завжди оперативно отримує запитувану інформацію від інтернет-провайдерів. Крім того, не повністю врегульовано питання термінів зберігання певної інформації провайдерами та яка відповідальність передбачена за її незбереження.

Разом з тим експерти від інтернет-ринку говорять про низьку якість інформаційних запитів з боку правоохоронних органів (особливо в регіонах), що заважає надавати якісні та своєчасні відповіді.

Необхідно розрізняти технічну анонімність від її правового поняття. Якщо визнавати кіберпростір соціально-значимою сферою, то не можна не погоджуватися з необхідністю контролю за ним. Необхідні правила та умови, які зроблять неможливою повну технічну анонімність, а акцент у розвитку потрібно зробити на юридичній анонімності (це робить законодавство у сфері персональних даних).

Складнощі розслідування кіберзлочинів полягають у тому, що багато з них виглядають незначними, хоча для їх доказів потрібно зібрати стільки доказів, як при значному правопорушенні. Крім того, для таких злочинів дозволяється застосовувати більш «простий», але менш ефективний арсенал засобів і методів правоохоронної діяльності. Більше того, у зв'язку з тим, що кіберзлочинність глобальна, то розслідування таких справ можливо тільки при виявленні всієї схеми і безлічі потерпілих, що збільшує час реагування. Також практикується відмова від вчинення злочинів у країні свого проживання.

В цілому, протягом 2012 року зареєстровано 2011 злочинів з використанням високих технологій, а за перше півріччя 2013 зареєстровано 1878 заяв та повідомлень про злочини даної категорії. Їх розкриваність знаходиться на рівні 50 % [5].

Таким чином, можна зробити висновок про те, національний рівень кіберзлочинності невпинно зростає, що для зниження рівня його розвитку потрібна розробка суттєвих заходів, починаючи з прийняття адекватного законодавства та закінчуючи рішенням суто технологічних питань. Головне ж завдання полягає в тому, щоб на міжнародному рівні, наприклад, в рамках ООН, розробити комплексну програму, що включатиме в себе всі можливі форми та методи боротьби з електронним шпіонажем – юридичні, програмні, технологічні, організаційні, економічні, політичні і т. д. Ці дії матимуть успіх лише в тому випадку, якщо будуть спиратися на систему постійного моніторингу кіберпростору на загальнопланетарному та національному рівнях.

Список використаних джерел:

1. Киберугрозы первого квартала 2013 года: шпионы атакуют : пресс-релиз / Itexpert [Електронний ресурс]. – Режим доступу: http://itexpert.in.ua/rubrikator/item/26195-kiberugrozy-pervogo-kvartala-2013-goda-shpiony-atakuyut-press-reliz.html.

2. Новиков С. В 2012 году 46,8 % украинских пользователей подвергались атакам при работе в Сети / С. Новиков ; Itexpert [Електронний ресурс]. – Режим доступу: http://itexpert.in.ua/

rubrikator/item/21709-v-2012-godu-468-ukrainskich-polzovateley-podvergalis-atakam-pri-rabote-v-seti-s-novikov.html.

3. Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers / Европейский центр по борьбе с киберпреступностью при Европоле [Електронний ресурс]. – Режим доступу: https://www.europol.europa.eu/content/project-2020-scenarios-future-cybercrime.

4. Еляков А. Электронный шпионаж / А. Еляков // Международная экономика и международные отношения. – 2009. – № 8. – С. 62–68.

5. Стан та структура злочинності в Україні (станом на 20 листопада 2012 року) / МВС України [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/813157.

Одержано 15.11.2013

УДК 343.85:004

Александр Анатольевич КИРИЧЕНКО,
доктор юридических наук, профессор, заведующий кафедрой гражданского и уголовного права и процесса Черноморского государственного университета,
Татьяна Александровна КОРОСТАШОВА,
соискатель кафедры гражданского и уголовного права и процесса Черноморского государственного университета

ЗНАЧЕНИЕ НОВОЙ ДОКТРИНЫ АНТИДЕЛИКТНЫХ ОРГАНОВ В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПЛЕНИЯМ

Противодействие киберпреступлениям и иным киберправонарушениям должны осуществлять государственные органы, которые, в свою очередь, имеют семантически необоснованное наименование «правоохранительными» и недостаточно четкую систему, что не может не сказаться на эффективности, рациональности и качестве проведения такого противодействия.

Существующее наименование такого рода государственных органов именно правоохранительными как форма обуславливает соответствующее несовершенное ее содержание – деятельность этих органов, направленную якобы лишь на предупреждение киберпреступлений и других правонарушений, а не на проведение всех стадий противодействия такого рода правонарушениям. К примеру, Ю. Д. Ткач выделяет такие стадии преодоления макроправонарушений:

1. Выявление латентных макроправонарушений.
2. Прекращение длящихся макроправонарушений.
3. Раскрытие макроправонарушений.
4. Досудебное расследование макроправонарушений.
5. Досудебное разрешение или судебное рассмотрение (первая инстанция) и пересмотр антикриминального дела.
6. Исполнение досудебного или судебного решения.
7. Проведение работы с лицом, освобожденным из мест лишения свободы, до истечения или погашения срока судимости.
8. Осуществление иных мероприятий по предупреждению макроправонарушений.

Как видим, охрана права от нарушения, т. е. охрана прав, свобод, интересов и обязанностей каждого физического или юридического лица либо государства в целом от посягательств киберправонарушителей, по сути является лишь предупреждением такого рода правонарушений, что представляет собой только одну из восьми фактически существующий стадий преодоления правонарушений вообще и киберправонарушений, в частности. Именно поэтому, чтобы привести в соответствие форму и содержание, т. е. наименование государственных органов, которые должны противодействовать правонарушениям, и их деятельность, которая призвана охватывать все без исключения стадии противодействия правонарушениям вообще и киберправонарушениям в частности, а не только их предупреждение, предложено правоохранительные органы переименовать антиделиктными, деятельность – в антиделиктную, а правоохранителей – в антиделиктологов.

Антиделиктных органов имеется или должно быть несколько десятков, новейшее наименование которых по схеме «антиделиктный орган – деятельность – сотрудник» может быть представлена в контексте унификации и локальности изложения таким образом:

1. Суд, судебная, судья.
2. Прокуратура, прокурорская, прокурор.
3. Адвокатура, адвокатская, адвокат.
4. Чекистатура (вместо службы безопасности), чекистатурная, чекист.
5. Парачекистатура (вместо милиции), парачекистатурная, парачекист.

6. Следотура, следственная, следователь.

7. Экспертнотура, экспертная, эксперт.

8. Налоготура, налоговая, налоговик.

9. Таможеннотура, таможенная, таможенник.

10. Погранотура, пограничная, пограничник.

11. Эмчаэстатура (МЧС), эмчаэсная, эмчаэсник.

12. Пожарнотура, пожарная, пожарник.

13. Ордистатура (объединение всех существующих оперативно-розыскных подразделений, за исключением СБУ).

14. Исполнитатура (исполнительные процедуры по всем видам судопроизводства, в т. ч. и антикриминального), госисполнительная, госисполнитель.

15. Госохраннотура (охрана госслужащих), госохранная, госохранник.

16. Объектноохраннотура (вместо госслужбы охраны), объектноохранная, объектноохранник.

17. Патрульнотура, патрульная, патрульный.

18. Конвойнотура, конвойная, конвоир.

19. Ревизийнотура (вместо КРУ), ревизионная, ревизор.

20. Потребделиктатура (защита прав потребителей), потребантиделиктная, потребантиделиктолог.

21. Трудоделиктатура, трудоантиделиктная, трудоантиделиктолог.

22. Ценоделиктатура, ценоантиделиктная, ценоантиделиктолог.

23. Земледеликтатура, землеантиделиктная, землеантиделиктолог.

24. Лесоделиктатура, лесоантиделиктная, лесоантиделиктолог.

25. Вододеликтатура, водоантиделиктная, водоантиделиктолог.

26. Недроделиктатура, недроантиделиктная, недроантиделиктолог и т. д.

Из указанной системы наиболее тесно связаны или должны быть связаны с противодействием киберпреступлениям и другим киберправонарушениям (с учетом их нового наименования) такие антиделиктные органы, как ордистатура, прокуратура, суд, следотура, экспертнотура, адвокатура, чекистатута, парачекистатута, погранотура, таможеннотура, налоготура, исполнитатура и др., предлагаемое наименование и система которых позволяет надеяться на соответствующий

вклад в повышение эффективности, рациональности и качества противодействия такого рода правонарушениям.

Список использованных источников:

1. Свыше ста пятидесяти лучших доктрин и концепций научной школы профессора Аланкира (приглашение к дискуссии) : науч. гипердокл. [Электронный ресурс] / А. А. Кириченко, В. Д. Басай, Е. В. Кириленко, С. А. Кириченко, Т. А. Коросташова, Ю. А. Ланцедова, Ю. Д. Ткач, А. С. Тунтула, В. С. Шаповалова / 57 700 слов – К. : ЕМНЛЮ «Consensus omnium», 2013. – 188 с. – Режим доступа: http://consensusomnium.com/ru/reports_ru/#.

Одержано 14.11.2013

УДК 343.985

Владлена Олександрівна ПРИХОДЬКО,
викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

ЩОДО ПРОБЛЕМ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАСТОСУВАННЯ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Людство, поставивши собі на службу комп'ютери, телекомунікаційні та глобальні комп'ютерні мережі не передбачило, які можливості для зловживань створюють ці технології. Сьогодні жертвами злочинців у віртуальному просторі можуть стати не тільки окремі люди, але й цілі держави [1, с. 15]. На сьогодні суттєвою проблемою в організації належної протидії кіберзлочинності залишається певне відставання нормативно-правового регулювання державою інформаційно-телекомунікаційної діяльності від розвитку суспільних відносин в цій сфері, що обумовлює невідповідність чинного законодавства вимогам часу.

Зокрема, активний розвиток технологій, засобів забезпечення анонімності та власної конспірації в мережі Інтернет значно ускладнює, а в деяких випадках ще й унеможливлює контроль та документування протиправних дій, а разом з тим і пошук злочинців.

На теперішній час загальносвітовою тенденцією є поширення доступу користувачів до мережі Інтернет та збільшення обсягів обміну даними з використанням технології Wi-Fi. Особливістю зазначеного стандарту бездротової передачі даних є використання спільного радіочастотного спектру та

виділення корисного сигналу за допомогою розділення його у просторі. Серед переваг, які надає вказана технологія, є швидкість розгортання та введення в експлуатацію обладнання, швидкість передачі даних, можливість розташування абонентських станцій на значній відстані від базової, організація корпоративних (відомчих) мереж тощо.

Водночас, експерти в галузі інформаційних технологій вказують на недосконаліть засобів захисту даних, які передаються за допомогою зазначеної технології. Більшість із стандартів шифрування, які на сьогодні застосовуються в Wi-Fi, є вкрай вразливими щодо посягань зловмисників або осіб, які просто намагаються отримати безкоштовний доступ до мережі Інтернет. При цьому для здійснення несанкціонованого втручання в роботу Wi-Fi мережі їм не потрібні складні програмні інструменти – все необхідне програмне забезпечення можливо отримати на ресурсах «хакерської» спрямованості в Інтернеті. Зламавши Wi-Fi мережу зловмисник, який володіє спеціальними знаннями, отримує не лише доступ до інформації та ключових даних, що зберігаються на її комп'ютерах, а й можливість прихованого розповсюдження власної, у тому числі шкідливої інформації чи програмного забезпечення, включення відповідних машин до так званих BOT-NET мереж, з подальшим використанням у «хакерських» цілях.

Аналіз «хакерських» форумів також свідчить про існування певного кола осіб, які готові надати платні послуги із «зламу» Wi-Fi мереж. Ці особи підтверджують свої можливості наявністю окремих внутрішніх документів (контрактів, звітності, листування тощо) різноманітних вітчизняних та іноземних фірм та організацій.

Іншим негативним аспектом використання технології Wi-Fi у вітчизняних реаліях є надання можливостей зловмисникам по забезпеченню власної анонімності. Функціонування відкритих точок доступу Wi-Fi в готелях, клубах, закладах харчування, торгівельно-розважальних та спортивних центрах (на даний час лише в Харківському регіоні нараховується понад сотні таких місць) створює передумови до приховування слідів протиправної діяльності через складність ідентифікації кінцевого користувача доступу до мережі Інтернет. Такі точки вже активно використовуються «хакерами» та екстремістські-налаштованими особами, що не виключає можливості їх використання для здійснення терористичної діяльності.

Разом із цим, на відміну від багатьох інших країн, у вітчизняному законодавстві відсутні будь-які нормативні засади, які регламентують порядок та стандарти надання послуг бездротового доступу до Інтернету. З огляду на розглянуту проблематику, запобігання певним кіберзлочинам може бути забезпечено комплексним використанням в точках вільного Wi-Fi доступу до мережі Інтернет захищених протоколів обміну даними, накопиченням на серверах надавачів цієї послуги інтернет-статистики відвідувань (лог-файлів), застосуванням відкритого відеоспостереження, залишенням при отриманні паролів Wi-Fi доступу паспортних даних тощо.

Прогнозується, що вказані заходи викличуть неоднозначну реакцію або навіть не сприйняття з боку окремих прихильників подальшої демократизації суспільства, як такі, що начебто суперечать правам людини. Проте, суворе дотримання надавачами таких послуг вимог чинного законодавства щодо захисту персональних даних здатне знівелювати відповідні протиріччя.

На завершення можна сказати, що в умовах створення розвинутими країнами у складі Збройних Сил спеціальних підрозділів для ведення так званих «кібервійн», використання для їх оснащення найсучасніших науково-прикладних досліджень, у тому числі спеціально створеного шкідливого програмного забезпечення значної руйнівної сили, активізації діяльності міжнародних екстремістських та «хакерських» організацій та використання ними національних сегментів Інтернету для розміщення матеріалів певної спрямованості, а також поширення своєї ідеології або залучення нових членів, – державі необхідно терміново вжити низку заходів, спрямованих на упорядкування функціонування українського сегменту мережі Інтернет та його суб'єктів, зокрема на деанонімізацію користувачів, діяльність яких містить ознаки приготування чи скоєння злочинів або суперечить засадам державної політики в інформаційній сфері.

Список використаних джерел:

1. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – К. : Скіф, 2012. – 728 с.

Одержано 07.11.2013

УДК 343.98

Татьяна Федоровна БЕССОННАЯ,
преподаватель кафедры криминалистики,
судебной медицины и психиатрии
факультета подготовки специалистов для подразделений следствия
Харьковского национального университета внутренних дел

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОГО И КАДРОВОГО ОБЕСПЕЧЕНИЯ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В УКРАИНЕ

Широкое внедрение современных информационных технологий (IT) создает новые, уникальные возможности для более активного и эффективного развития экономики, политики, государства, общества, социального сознания и гражданина. Однако совершенствование технологий приводит не только к укреплению индустриального общества, но и к появлению новых, ранее неизвестных источников опасности для него. Экономика и обороноспособность ведущих государств мира все в большей степени зависят от нормального функционирования глобальных компьютерных сетей. Нарушение их работоспособности может повлечь серьезные последствия, а национальные и международные правовые институты и организационные структуры практически не готовы к адекватному противодействию новым угрозам.

Одним из серьезных шагов, направленных на урегулирование этой проблемы, явилось принятие Советом Европы 23 ноября 2001 г. Конвенции по борьбе с киберпреступностью. Этот документ стал первым международным соглашением по юридическим и процедурным аспектам расследования и криминального преследования киберпреступлений.

Полноценный Закон о борьбе с киберпреступностью необходим и Украине. Кабинет министров Украины 6 марта 2013 г. одобрил предложенный Министерством внутренних дел законопроект «О внесении изменений в Закон Украины «Об основах национальной безопасности Украины» относительно кибернетической безопасности Украины». Этот законопроект направлен на формирование принципов государственной политики в сфере обеспечения кибернетической безопасности Украины путем определения основных реальных и потенциальных угроз национальной безопасности кибернетического характера, основных направлений государственной

политики и основных функций субъектов обеспечения национальной безопасности в этой сфере.

Принятие законопроекта заложит правовую основу для дальнейшей нормотворческой деятельности на законодательном и подзаконном уровне, направленной на создание и совершенствование национальной системы кибернетической безопасности, противодействия кибернетической преступности.

Компьютерная преступность стала одной из международных проблем, которая обусловлена созданием международных информационных систем, таких, например, как сеть Интернет, которая объединяет вычислительные центры и системы многих стран и обеспечивает обмен данными между разнообразными источниками и пользователями. Киберпреступники с легкостью преодолевают географические и политические границы, а их жертвами могут стать пользователи в любой части света. Правоохранительные же органы имеют ограниченную юрисдикцию – они не могут самостоятельно проводить расследования на территории других государств. Поэтому сотрудничество с коллегами на международном уровне совершенно необходимо

Стремительная компьютеризация общества и появление новых, ранее неизвестных преступлений в сфере информационных технологий выявили, что правоохранительные органы не готовы в полной мере к противодействию с этим новым антисоциальным явлением. Поэтому квалифицированная кадровая обеспеченность сферы информационной безопасности является одним из основных факторов, влияющих на результативность борьбы с киберпреступностью. Помимо этого необходимо совершенствование процессов и методики обучения, повышения квалификации специалистов, занятых в сфере обеспечения информационной безопасности и борьбы с киберпреступностью, в частности в органах внутренних дел Украины.

Для перехода на более высокий уровень работы правоохранительных органов в борьбе с киберпреступностью требуются новые системные знания, но тут возникает несколько проблем: недостаток в профильных учебных заведениях системы МВД Украины факультетов подготовки специалистов по борьбе с киберпреступностью; отсутствие единой системы переподготовки по данным направлениям; отсутствие программ

по привлечению на службу государству специалистов по IT-технологиям; несовершенство законодательной базы.

Таким образом, в ближайшем будущем необходимо создать структуру образования, а также принять ряд законов в данной сфере. В первую очередь, закрепив в нормативно-правовых актах используемые в области кибербезопасности понятия, определить «правила игры» для провайдеров упорядочив их работу и определив им обязанности в поддержке госорганов в данной сфере. Совершенствовать подготовку и переподготовку личного состава на базе профильных государственных высших учебных заведений, подготавливающих узкоспециализированных специалистов в области высоких технологий. Также необходимо сочетание специализированного законодательства, эффективного надзора со стороны правоохранительных органов и общественной осведомленности.

Одержано 05.11.2013

УДК 351.746.1(476)

Володимир Валентинович ЧУМАК,
кандидат юридичних наук,
старший викладач кафедри адміністративної діяльності ОВС факультету з підготовки фахівців для підрозділів міліції громадської безпеки та кримінальної міліції у справах дітей Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В РЕСПУБЛІЦІ БІЛОРУСЬ

Законодавство Республіки Білорусь, що стосується забезпечення інформаційної безпеки, почало формуватися з моменту здобуття країною незалежності, і в даний час, динамічно розвиваючись, має вертикальну (за видами юридичних актів) і горизонтальну (по галузях законодавства) структуру.

Перший високотехнологічний злочин в Білорусі був зафіксований 20 листопада 1998 року. Так, впровадивши в програмне забезпечення комп'ютера шкідливу програму «BackOrifice», зловмисник здійснив несанкціонований доступ до мережевих реквізитів користувачів Інтернету з числа клієнтів найбільшого в Білорусії столичного сервіс-провайдера [1, с. 100–101]. За період з 1998 по 2000 рр. було порушено лише 3 кримінальні справи, пов'язаних з використанням

комп'ютерних технологій. З моменту набрання чинності у 2001 р. КК Білорусі число зареєстрованих злочинів даної категорії почало стрімко зростати.

Багато дослідників, в тому числі і закордонні, відзначають прогресивний характер КК Білорусі, який досить точно сприйняв концепцію комп'ютерної злочинності, майбутні її тенденції, і в цьому відношенні навіть випередив Конвенцію Ради Європи про кіберзлочинність 2001 р. У Кримінальному Кодексі Білорусі 1999 р. включена глава № 31 «Злочини проти інформаційної безпеки», що містить 7 складів злочинів.

8 листопада 2011 р. був прийнятий Указ Президента Республіки Білорусь № 515 «Про деякі питання розвитку інформаційного суспільства в Республіці Білорусь», який передбачає створення Ради з розвитку інформаційного суспільства при Президентові Республіки Білорусь, а також затверджує Положення про Раду з розвитку інформаційного суспільства при Президентові Республіки Білорусь, склад зазначеної Ради та Положення про незалежного регулятора у сфері інформаційно-комунікаційних технологій, складу Ради незалежного регулятора у сфері інформаційно-комунікаційних технологій [2].

У зв'язку з розвиненням комп'ютеризації у республіці з'явилася необхідність вдосконалення процесу документообігу та відповідної нормативної основи. У зв'язку з цим 28 грудня 2009 р. був прийнятий Закон Республіки Білорусь «Про електронний документ і електронний цифровий підпис» [3].

У листопаді 2010 року Указом Президента Республіки Білорусь була прийнята нова Концепція національної безпеки, в якій вперше було дано визначення інформаційної безпеки, визначено основні національні інтереси в інформаційній сфері, а також названі внутрішні і зовнішні джерела загроз інформаційної безпеки. Пріоритетним напрямком на шляху нейтралізації цих загроз відповідно до документа є вдосконалення нормативної правової бази забезпечення інформаційної безпеки і завершення формування комплексної державної системи забезпечення інформаційної безпеки. При цьому важливе значення відводиться нарощуванню діяльності правоохоронних органів щодо запобігання, виявлення та припинення злочинів проти інформаційної безпеки, а також надійному забезпеченню безпеки інформації, що охороняється відповідно до законодавства.

27 травня 2009 р. набула чинності Постанова Ради Міністрів Республіки Білорусь № 675 [4], якою було затверджено

Положення про порядок захисту інформації, Положення про порядок атестації систем захисту, Положення про порядок проведення експертизи засобів захисту інформації. Ці положення розроблені відповідно до Закону Республіки Білорусь від 10 листопада 2008 р. «Про інформацію, інформатизації і захисту інформації» та визначають порядок захисту інформації в державних інформаційних системах, а також інформаційних системах, що містять інформацію, поширення і (або) надання якої обмежено, порядок атестації та державної експертизи систем і засобів захисту такої інформації.

Повсюдне поширення в Білорусії мережі Інтернет призвело не тільки до того, що кіберпростір став одним з основних джерел отримання інформації, але й до того, що Інтернет став «майданчиком» скоєння різних правопорушень і, особливо, в комерційній сфері. Все це вимагало від держави вжиття рішучих заходів щодо створення нормативної основи регулювання національного сегменту мережі Інтернет.

З цією метою 1 лютого 2010 р. був виданий Указ Президента Республіки Білорусь № 60 «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет» [5]. Документ спрямований на захист інтересів громадян, суспільства і держави в інформаційній сфері, підвищення якості та здешевлення інтернет-послуг, забезпечення подальшого розвитку національного сегменту мережі Інтернет. Пізніше на виконання цього указу в квітні 2010 р. були прийняті дві постанови Ради Міністрів Республіки Білорусь – № 644 та № 649 [6; 7]. Ці нормативні акти регламентують порядок реєстрації та здійснення юридичними та фізичними особами діяльності з реалізації товарів, виконання робіт, надання послуг на території Республіки Білорусь з використанням інформаційних мереж, систем і ресурсів, що мають підключення до мережі Інтернет.

Саме сукупність даних нормативних правових актів становить правову основу регулювання відносин, що складаються в процесі обігу інформації та забезпечення інформаційної безпеки.

Таким чином, можемо зробити висновок, що норми кримінального закону Республіки Білорусь про злочини проти інформаційної безпеки є частиною національного інформаційного законодавства як комплексної галузі права і захищають найбільш важливі суспільні відносини у даній сфері.

Прийняття КК Білорусії з одного боку опосередковано викликало зростання числа комп'ютерних злочинів, так як у нього були включені склади, що раніше не мали місця в національному кримінальному законодавстві; а з іншого боку правоохоронці отримали «інструментарій» боротьби з комп'ютерними злочинами у вигляді норм кримінального закону, що передбачають кримінальну відповідальність за вчинення подібних діянь.

Список використаних джерел:

1. Масленченко С. В. Белорусский сегмент преступности в сфере высоких технологий / С. В. Масленченко // Милиции Беларуси 90 лет: история и современность : материалы науч.-практ. конф., Минск, 27 февр. 2007 г. / М-во внутр. дел Республики Беларусь, Акад. МВД Республики Беларусь ; редкол.: К. И. Барвинок (отв. ред.) и [др.]. – Минск, 2007. – С. 100–104.

2. О некоторых вопросах развития информационного общества в Республике Беларусь : указ Президента Республики Беларусь от 8 нояб. 2011 г. № 515 [Електронний ресурс]. – Режим доступу: http://pravo.by/main.aspx?guid=3871&p2=1/13064.

3. Об электронном документе и электронной цифровой подписи : закон Республики Беларусь від 28 дек. 2009 г. № 113-З [Електронний ресурс]. – Режим доступу: http://pravo.by/main.aspx?guid=3871&p0=H10900113&p2=%7BNRPA%7D.

4. О некоторых вопросах защиты информации : постановление Совета Министров Республики Беларусь от 27 мая 2009 г. № 675 [Електронний ресурс]. – Режим доступу: http://www.levonevski.net/pravo/norm2013/num18/d18700.html.

5. О мерах по совершенствованию использования национального сегмента сети Интернет : указ Президента Республики Беларусь от 1 февр. 2010 г. № 60 [Електронний ресурс]. – Режим доступу: http://pravo.by/main.aspx?guid=3871&p0=P31000060&p2=%7BNRPA%7D.

6. О некоторых вопросах совершенствования использования национального сегмента глобальной компьютерной сети Интернет : постановление Совета Министров Республики Беларусь от 29 апр. 2010 г. № 644 [Електронний ресурс]. – Режим доступу: http://pravo.by/main.aspx?guid=3871&p0=C21000644&p2=%7BNRPA%7D.

7. О регистрации интернет-магазинов в Торговом реестре Республики Беларусь, механизме контроля за их функционированием и внесении дополнений и изменений в некоторые постановления Совета Министров Республики Беларусь : постановление Совета Министров Республики Беларусь от 29 апр. 2010 г. № 649 [Електронний ресурс]. – Режим доступу: http://www.pravo.by/main.aspx?guid=3871&p0=C21000649&p2=%7BNRPA%7D.

Одержано 18.11.2013

УДК 342.9

Антоніна Володимирівна РУМЯНЦЕВА-КОЗОВНИК,
ад'юнкт
Харківського національного університету внутрішніх справ

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ОРГАНІВ ВНУТРІШНІХ СПРАВ ЩОДО ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ ДИТЯЧОЇ ПОРНОГРАФІЇ В МЕРЕЖІ ІНТЕРНЕТ

З появою та розвитком всесвітньої мережі Інтернет з'явився і новий вид злочинності – кіберзлочинність (комп'ютерна злочинність), яка з кожним роком набирає свої оберти і несе за собою серйозні, а часом незворотні наслідки.

Комп'ютерна злочинність – це сукупність комп'ютерних злочинів, у яких комп'ютерна інформація становить предмет злочинних посягань. Ці діяння є замахом на безпеку сфери комп'ютерної інформації, постаючи одним із найбільш небезпечних і шкідливих явищ сучасного світу.

Останнім часом в суспільстві все більше занепокоєння викликає поширення злочинів у сфері суспільної моралі. Особливо широкого розповсюдження набула дитяча порнографія в мережі Інтернет, як продукція виготовлена внаслідок експлуатації чи насильства над дітьми. Чверть від усіх кіберзлочинів займають саме ці злочини.

Порнографія є особливо тяжкою формою сексуальної експлуатації дітей. Вона приймає останніми роками усе більш широкі масштаби розповсюдження і є грубим порушенням невід'ємного права дитини на гармонійне виховання і розвиток.

До проблем подолання дитячої порнографії неодноразово зверталися такі науковці, як, О. Бут, В. Іващенко, М. Коллінз, І. Лисенко, К. Левченко, Н. Плахотнюк, О. Рябчинська, О. Швед та інші, які висловлювали різні пропозиції з протидії дитячій порнографії, але єдиної думки щодо способів подолання дитячої порнографії в мережі Інтернет до цього часу не вироблено.

Значним кроком уперед у цій боротьбі стало прийняття Генеральною Асамблеєю ООН Факультативного протоколу до Конвенції про права дитини, який стосується торгівлі дітьми, дитячої проституції та дитячої порнографії. Стаття 2 цього протоколу визначає дитячу порнографію як «будь-яке зображення

будь-якими засобами дитини, яка здійснює реальні або змодельовані відверто сексуальні дії, або будь-яке зображення статевих органів дитини, головним чином, в сексуальних цілях» [1]. Протокол ратифіковано Законом України № 716-IV від 3 квітня 2003 р. і, як кожна держава-учасниця Протоколу, Україна зобов'язується забезпечити визнання таких діянь кримінальним злочином, незалежно від місця його вчинення (національний чи транснаціональний рівень).

Хвиля дитячої порнографії, яка накрила багато країн, створює ряд досить складних, але невідкладних проблем як стосовно боротьби з цим негативним та небезпечним явищем, так і з його попередженням, бо з урахуванням розвитку і вдосконалення інформаційних та комунікативних каналів проблему цю досить важко вирішити тільки в рамках однієї держави, вона потребує зважених та скоординованих зусиль світового співтовариства [2, с. 197].

Провідне місце у системі запобігання поширенню дитячої порнографії в мережі Інтернет, попередження та протидії злочинам, пов'язаним із сексуальною експлуатацією дітей займають органи внутрішніх справ.

З метою цілеспрямованої протидії злочинам, пов'язаним з вчиненням кіберзлочинів у структурі карного розшуку центрального апарату та ГУМВС, УМВС були створені управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України.

Одним із основних напрямків діяльності підрозділу боротьби з кіберзлочинністю є протидія обігу дитячої порнографії та сексуальному розбещенню дітей, учинюваним із використанням телекомунікаційних мереж. Доречно зазначити, що на цьому напрямку діяльності зусилля оперативного складу зосереджені не лише на виявленні осіб, причетних до вчинення злочину, але й на ідентифікації жертв сексуальної експлуатації [4].

Міжнародне співробітництво та взаємодія з міжнародними правоохоронними органами є одним із пріоритетів в діяльності підрозділу боротьби з кіберзлочинністю. Часто на базі Управління проходять міжнародні тренінги для співробітників підрозділу, які проводять експерти ОБСЄ щодо розслідування комп'ютерних злочинів.

У березні 2013 року за підтримки посольства Великобританії в Україні на базі Національної академії внутрішніх

справ був проведений тренінг з питань боротьби з дитячою порнографією в мережі Інтернет.

Також співробітники підрозділу проходили стажування у відділах по боротьбі з організованою злочинністю у Великобританії.

За підтримки посольства США в Україні працівники підрозділу навчалися в Академії ФБР у міжнародному центрі з протидії кіберзлочинності.

В цьому році співробітники кримінальної поліції Німеччини проходили стажування на базі Управління боротьби з кіберзлочинністю МВС України.

Таким чином, головними завданнями міжнародного співробітництва є обмін досвідом щодо розслідування кіберзлочинів, підвищення кваліфікації та використання досвіду міжнародних експертів щодо протидії та боротьби з розповсюдженням дитячої порнографії в мережі Інтернет.

Міністерством внутрішніх справ України на сьогодні налагоджено співробітництво з Міжнародною організацією кримінальної поліції – Інтерполом, Європолом, Регіональним центром Південно-Східної ініціативи співробітництва з транснаціональною злочинністю, міжнародними організаціями та правоохоронними органами інших держав.

Доречним буде зазначити, що відділ боротьби з кіберзлочинністю МВС України є надзвичайно молодим. Відтак, наразі проблема номер один, – проблема формування кадрів. Це пов'язано з тим, що фахівці, які працюватимуть у цій сфері, повинні бути як оперативниками, так і фахівцями з комп'ютерної техніки. Вочевидь, що підготовка кваліфікованих кадрів для зазначеного підрозділу – одне з нагальних завдань вищих навчальних закладів МВС України.

Зазначимо, що ця проблема є досить ефективно вирішуваною. Позитивний досвід підготовки фахівців для підрозділів боротьби з правопорушеннями у сфері високих комп'ютерних технологій накопичується у Харківському національному університеті внутрішніх справ, у якому підготовка спеціалістів зазначеного профілю проводиться на факультеті підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми.

Безумовно, специфіка протидії таким протиправним посяганням у сучасних умовах вимагає особливого підходу до

комплектування підрозділу боротьби з кіберзлочинністю. Зокрема, такі працівники, на додаток до знань у сфері високих інформаційних технологій, навичок отримання інформації та збору доказів у електронній формі, повинні достатнім чином володіти іноземними мовами.

Аналіз викладеного матеріалу дає підстави дійти висновків, що, враховуючи те, що кіберзлочинність невпинно вдосконалює способи вчинення протиправних посягань та має тенденцію до зростання організованості, нагальним завданням є систематичне підвищення кваліфікації оперативних працівників шляхом ознайомлення з передовим зарубіжним досвідом та нововведеннями щодо методології розкриття й розслідування таких злочинів.

Отже, зазначені проблеми потребують розроблення відповідної стратегії щодо боротьби з кіберзлочинністю усіма правоохоронними органами України, зважаючи на те, що боротьба з цим найсучаснішим видом злочинності повинна стати однією з найважливіших їх функцій.

Список використаних джерел:

1. Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії : ратиф. законом України від 03.04.2003 № 716-IV [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/995_b09.

2. Рябчинська О. Законодавче забезпечення захисту прав дітей від сексуальної експлуатації: тенденції розвитку та вдосконалення / О. Рябчинська // Вісник Запорізького юридичного інституту. – 2001. – № 3. – С. 192–199.

3. Зозуля Є. Діяльність МВС України щодо протидії транснаціональній злочинності у сфері високих технологій / Є. Зозуля // Наукові записки. Серія: Історія. – 2011. – Вип. 1. – С. 205–211.

4. У Міністерстві внутрішніх справ України створено відділ боротьби з кіберзлочинністю [Електронний ресурс]. – Режим доступу: http://www.mvs.gov.ua/mvs/control/main/uk/publish/article/243867.

Одержано 12.11.2013

УДК 343.63

Олександр Сергійович СУББОТЕНКО,
головний спеціаліст відділу державної реєстрації речових прав на нерухоме майно реєстраційної служби Вишгородського районного управління юстиції Київської області

ДО ПИТАННЯ ПРО ЗАХИСТ ЧЕСТІ, ГІДНОСТІ ТА ДІЛОВОЇ РЕПУТАЦІЇ У МЕРЕЖІ ІНТЕРНЕТ

Інформаційно-телекомунікаційні системи настільки глибокого проникли в усі сфери суспільного життя, що на сьогодні важко уявити можливість спілкування без їх застосування. Так, напевно, ні для кого не є таємницею те, що на сьогоднішній день Інтернет став надбанням усього людства, оскільки уже мало хто уявляє собі життя без нього. Дійсно, ця всесвітня мережа суттєво впливає на різноманітні сторони життя людства, проте варто зазначити, що у неї існує і безліч негативних властивостей. Так, спочатку Інтернет утворювався як мережа для вільного поширення й одержання корисних для суспільства даних, з урахуванням норм права та морально-етичних принципів, що забезпечують соціальну справедливість та рух у напрямі до свободи. Простота, швидкість і географічний розмах поширення відомостей у цій мережі переконує безліч людей у перевагах цього засобу комунікації. Однак, рівень оволодіння новими інформаційними технологіями далеко не завжди відповідає рівню їх етики, моралі та коректності. Нажаль, на сьогоднішній день Інтернет перетворився на повсякденний засіб передачі будь-якої інформації, не завжди достовірної, що досить часто призводить до порушення норм, якими охороняється честь, гідність та ділова репутація.

Окремі питання захисту честі, гідності та ділової репутації розглядалися такими вченими як В. А. Бортник, В. О. Глушков, І. М. Даньшин, С. Ф. Денисов, О. М. Джужа, М. Й. Коржанський, А. А. Музика, Й. С. Ной, В. І. Осадчий, М. А. Придворов, В. В. Сташис, В. І. Шакун та інші.

Проте комплексного дослідження проблеми відповідальності за посягання на честь та гідність особи, у тому числі з використанням інформаційно-телекомунікаційних мереж, до цього часу в Україні не проводилось.

Треба зазначити, що з однієї сторони, можливість вільного висловлювання в мережі Інтернет користувачам забезпечена

Конституцією України, а саме ст. 34 гарантовано право на свободу думки і слова, вільне вираження своїх поглядів і переконань. Цією нормою встановлюється, що кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або у інший спосіб – на свій вибір. Відповідно до ст. 68 Основного Закону України кожен зобов'язаний неухильно додержуватися Конституції та законів України, не посягати на права і свободи, честь і гідність інших людей. Таким чином, праву на свободу думки і слова, на вільне вираження своїх поглядів і переконань, що гарантоване Конституцією України у ст. 34, відповідає обов'язок не поширювати про особу недостовірну інформацію та таку, що ганьбить її гідність, честь чи ділову репутацію.

Відповідно до чинного законодавства України, у випадку розміщення в мережі Інтернет інформації, що порушує честь, гідність та ділову репутацію особа, права якої порушено, може або ж безпосередньо звернутися до особи, яка здійснила дане порушення, з вимогою про спростування такої інформації, або ж звернутися до суду. Крім того, позови про захист гідності, честі чи ділової репутації мають право пред'явити фізична особа у разі поширення про неї недостовірної інформації, яка порушує її особисті немайнові права, а також інші зацікавлені особи (зокрема члени її сім'ї, родичі), якщо така інформація прямо чи опосередковано порушує їх особисті немайнові права.

Якщо недостовірна інформація, що порочить гідність, честь чи ділову репутацію, розміщена в мережі Інтернет на інформаційному ресурсі, зареєстрованому в установленому законом порядку як засіб масової інформації, то при розгляді відповідних позовів судам слід керуватися нормами, що регулюють діяльність засобів масової інформації. Крім того, відповідно до п. 12 Постанови Пленуму Верховного Суду України «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» належним відповідачем у разі поширення оспорюваної інформації в мережі Інтернет є автор відповідного інформаційного матеріалу та власник веб-сайту, особи яких позивач повинен установити та зазначити в позовній заяві. Якщо автор поширеної інформації невідомий або його особу та/чи місце проживання (місцезнаходження) неможливо встановити, а також коли інформація є анонімною і

доступ до сайту – вільним, належним відповідачем є власник веб-сайту, на якому розміщено зазначений інформаційний матеріал, оскільки саме він створив технологічну можливість та умови для поширення недостовірної інформації. Про це також йдеться і у п. 13 Інформаційного листа Вищого Господарського Суду України «Про деякі питання практики застосування господарськими судами законодавства про інформацію».

Проте, у більшості випадків захист честі, гідності та ділової репутації цивільно-правовими засобами є не достатнім. Варто також зазначити, що на сьогоднішній день почастішала практика звернення до Європейського суду з прав людини, оскільки серед українських судів існує досить велика проблема визначення пріоритетів при здійсненні правосуддя під час розгляду справ щодо свободи поширення інформації, можливості її обмеження, спростування недостовірної інформації та захисту честі й гідності людини. Така проблема пов'язана передусім із недосконалістю нашого законодавства. Оскільки, на жаль, сьогоднішній стан законодавства дозволяє іноді неоднаково тлумачити правові норми, які регулюють захист особистих немайнових благ – честі, гідності та ділової репутації. Окрім того, згідно із сучасними стандартами захисту прав особи, виникає необхідність забезпечення в Україні справедливої рівноваги при здійсненні конституційних прав на захист гідності і честі, з одного боку, та свободи слова – з іншого.

Вищевказане, враховуючи існуючі проблеми щодо захисту честі, гідності та ділової репутації чинним законодавством України, дозволяє запропонувати таку систему заходів, спрямованих на захист честі, гідності та ділової репутації від протиправних посягань на ці немайнові особисті (приватні) права особи: шкода заподіяна діловій репутації особи повинна відшкодовуватися у цивільно-правовому порядку наявним інструментарієм цивільного законодавства; посягання, пов'язані із заподіянням шкоди шляхом образи, внаслідок підвищеної суспільної небезпечності, слід визнати кримінальним проступком, а наклеп – злочином та передбачити за них кримінальну відповідальність.

Одержано 15.11.2013

УДК 343.346.8/7(477)

Тихін Віталійович ШЕВЧЕНКО,
слухач магістратури
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ВИЗНАЧЕННЯ ПРЕДМЕТА ЗЛОЧИНУ, ЩО ПЕРЕДБАЧЕНИЙ СТ. 361-2 КК УКРАЇНИ

В умовах швидкого розвитку комп'ютерних технологій, що є невід'ємною складовою сучасного світу, захист інформації від протиправних посягань є одним із важливих питань сьогодення, а розвиток і удосконалення законодавства у сфері боротьби з кіберзлочинністю є одним із важливих і перспективних напрямків його розвитку.

Розвиток методів обробки інформації за допомогою комп'ютерів призвів до застосування цих машин в усіх галузях національної економіки та інших сферах суспільного життя. Значна кількість таких машин об'єднана комп'ютерними мережами, деякі з них набули інтернаціонального характеру. За цих умов виникли і набули суспільної небезпеки різні діяння, що заподіюють шкоду нормальній роботі комп'ютерів та комп'ютерних мереж, у тому числі несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

Вивченням даного питання займаються такі вітчизняні вчені, як Д. С. Азаров, К. І. Бєляков, В. А. Ліпкан, В. Ю. Баскаков, М. С. Вертузаєв, В. М. Заяць, В. Є. Постульга, М. В. Рудик, О. С. Самойлова, Ю. В. Янчук та інші.

Метою нашого дослідження є чітке визначення змісту предмета злочину, передбаченого ст. 361-2 КК України, та відмежування його від інших, тотожних або схожих предметів.

Предметом даного злочину виступає інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації [1, с. 907]. Встановлення даного предмета в процесі кваліфікації злочину є обов'язковою. Тому усвідомлення змісту даної інформації дає можливість нам здійснити правильну кваліфікацію

діяння, що пов'язане з незаконним збутом або розповсюдженням такої інформації.

Згідно до закону України «Про інформацію», *інформація* – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Відповідно ст. 21 даного закону, інформацією з обмеженим доступом є *конфіденційна, таємна та службова інформація* [2].

Відповідно до ст. 7 закону України «Про доступ до публічної інформації» *конфіденційна інформація* – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація про стан довкілля, про якість харчових продуктів і предметів побуту, про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян, а також іншою інформацією, що становить суспільний інтерес(суспільно необхідною інформацією) [3].

У ст. 8 закону України «Про доступ до публічної інформації» зазначається, що *таємна інформація* – інформація, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю [3].

У свою чергу, *службова інформація*, згідно до ст. 9 закону України «Про доступ до публічної інформації» це – інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень, зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [3].

У даній роботі ми дослідили питання предмету злочину, передбаченого ст. 361-2 КК України та встановили що відноситься до інформації з обмеженим доступом, її ознаки та

характеристику, що чітко відмежовує її від інших видів інформації.

Як висновок необхідно зазначити, що на сьогоднішній день спостерігається збільшення кількості комп'ютерних злочинів, зокрема несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, і розробка та застосування надійних механізмів їх протидії, а також удосконалення законодавства є важливою складовою успішності протидії кіберзлочинності.

Список використаних джерел:

1. Кримінальний кодекс України. Науково-практичний коментар / [Ю. В. Баулін, В. І. Борисов, С. Б. Гавриш та ін.] ; за заг. ред. В. В. Сташиса, В. Я. Тація. – Вид. 3-тє переробл. та доповн. – Х. : Одісей, 2006. – 1184 с.

2. Про інформацію : закон України від 02.10.1992 № 2657-XII [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2657-12. – Редакція від 10.08.2012.

3. Про доступ до публічної інформації : закон України від 13.01.2011 № 2939-VI [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2939-17. – Редакція від 09.06.2013.

Одержано 11.11.2013

УДК [343.3/.7:004](477)

Сергій Михайлович ЗАЇКА,
курсант
Харківського національного університету внутрішніх справ;
науковий керівник – кандидат юридичних наук, старший викладач кафедри адміністративної діяльності ОВС факультету з підготовки фахівців для підрозділів міліції громадської безпеки та кримінальної міліції у справах дітей Харківського національного університету внутрішніх справ Чумак Володимир Валентинович

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: НАСЛІДКИ ТА ШЛЯХИ ПРОТИДІЇ

На сьогодні комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері

комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки [1]. Слід зауважити, що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України вперше передбачив самостійний розділ про ці злочини - розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»; положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві [2].

Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства, так чи інакше, пов'язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією.

Останнім часом в Україні значно зросла кількість Інтернет – користувачів, адже підключення до глобальної мережі стало доступним та зручним. Сьогодні персональний комп'ютер, КПК, мобільний телефон з підключенням до Інтернету сприймається як належне та необхідне. Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого. Інтернет – це чудовий засіб для зв'язку та спілкування. Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються злочини – кіберзлочини.

Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем – це далеко не повний перелік подібних злочинів [1].

Стержневою основою кіберзлочинів є передбачені кримінальним законом суспільно небезпечні діяння і закріпленні в окремому Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України [2].

В Україні кіберзлочинність регулюють такі нормативно-правові акти: Конвенція про Кіберзлочинність, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Кримінальний Кодекс України [4; 5].

Основною причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість, – вона неймовірно прибуткова. Величезні суми грошей з'являються в кишенях злочинців у результаті окремих великих афер, не говорячи вже про невеликі суми, які йдуть просто 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, які 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].

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

Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.

Список використаних джерел:

1. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ / В. Прохоренко // Економічна правда. – 26 лют. 2013 р.
2. Кримінальний кодекс України : закон України від 05.04.2001 № 2341-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14.
3. Міжнародна Конвенція «Про кіберзлочинність» : від 23.11.2001 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.
4. Про ратифікацію Конвенції про кіберзлочинність : закон України від 07.09.2005 № 2824-IV [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2824-15.

Одержано 19.11.2013

УДК 343.9:[343.3/.7:004](477)

Ігор Геннадійович КАТАШЕВ,
курсант
Харківського національного університету внутрішніх справ;
науковий керівник – кандидат юридичних наук, старший викладач кафедри адміністративної діяльності ОВС факультету з підготовки фахівців для підрозділів міліції громадської безпеки та кримінальної міліції у справах дітей Харківського національного університету внутрішніх справ Чумак Володимир Валентинович

ПРАВОВІ АСПЕКТИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У БОРОТЬБІ З КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ

Науково-технічний прогрес суттєво впливає на характер злочинності, створюючи передумови для вчинення нових злочинів. З поступовим розвитком комп'ютерних мережевих технологій, підключенням до глобальних комп'ютерних мереж користувачів із все зростаючої кількості країн виникають сприятливі умови для використання їх із злочинною метою. Відповідно, проблема боротьби зі злочинами у сфері комп'ютерної інформації із внутрішньодержавної перейшла у міжнародну.

Світова практика боротьби з правопорушеннями, пов'язаними із застосуванням комп'ютерної техніки, доводить необхідність міждержавної співпраці у боротьбі з останніми [1, с. 4].

Діяльність світового співтовариства з формування і розвитку правових основ регулювання відносин, що виникають щодо комп'ютерної інформації, має багатоаспектний характер.

Одним з її елементів є створення правових інститутів, що забезпечують міжнародне співробітництво у попередженні і припиненні найбільш тяжких протиправних діянь, до яких відносять і злочини у сфері комп'ютерної інформації.

Сьогодні міжнародне співробітництво у боротьбі зі злочинністю певною мірою являє собою узгоджену діяльність різних держав, що регулюється нормами міжнародного і національного права, з захисту інтересів особи, суспільства, держави і світового співтовариства, а також з прийняття суб'єктами цієї діяльності обумовлених національним кримінальним законодавством заходів, спрямованих на забезпечення національного кримінального процесу і здійснення правосуддя їх судами у справах про злочини, які посягають на внутрідержавний порядок [2, с. 7].

Основними елементами міждержавної співпраці у сфері боротьби з комп'ютерною злочинністю виділяють питання юрисдикції, розслідування комп'ютерних правопорушень, питання уніфікації кримінального законодавства [1].

Видів злочинів, що вчиняються з використанням комп'ютерів, дуже багато. У зв'язку з цим у науці кримінального права і кримінальному законодавстві різних держав поки що не вироблено єдиного поняття таких злочинів. Кожен автор по-своєму дає визначення цього виду злочинів [2, с. 6].

Найбільш значною у сфері розробки кримінально-правових і процесуальних аспектів боротьби із вказаною категорією злочинів є діяльність Організації Об'єднаних Націй, Організації економічного співробітництва і розвитку, Європейського Союзу, Ради Європи, Співдружності Незалежних Держав. Необхідно зазначити, що неабияку роль у боротьбі зі злочинами, пов'язаними з комп'ютерами, відіграють Інтерпол, країни «Великої Вісімки» («G-8») [1; 2] та деякі інші [3, с. 43].

Визначними міжнародно-правовими документами у питанні правового регулювання міжнародних відносин у даній сфері є Конвенція ООН проти транснаціональної організованої злочинності (ст. 20), Віденська декларація про злочинність і правосуддя: відповіді на виклики XXI століття (ООН), Конвенція Європейського Союзу про взаємну правову допомогу з кримінальних справ 2000 р. (глава 3); Європейська Конвенція про кіберзлочинність, Договір про співробітництво держав-учасниць СНД у боротьбі зі злочинами у сфері

комп'ютерної інформації (підписаний учасниками у 2001 році); та ряд інших документів, зокрема рекомендацій Ради Європи, що застосовуються разом із прийнятими конвенціями. Застосуванню підлягають і положення інших правових документів, наприклад, Конвенції про правову допомогу і правові відносини по цивільних, сімейних і кримінальних справах (держав-учасниць СНД), Європейської конвенції про взаємну допомогу у кримінальних справах та ін. [4, с. 24; 5, с. 1049].

Таким чином, процес інформатизації, комп'ютеризації суспільства постійно і динамічно рухається вперед, зокрема і в нашій державі. Тому вбачається за потрібне враховувати міжнародні напрацювання і рекомендації у сфері боротьби з даною категорією злочинів при розробці і втіленні в життя відповідних норм права та здійсненні практичної діяльності правоохоронними органами держави.

Список використаних джерел:

1. Сеитов Т. Б. Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью : автореф. дис. … канд. юрид. наук : 12.00.10 / Сеитов Т. Б. – Алматы, 2002. – 25 с.

2. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. – М. : Юрлитинформ, 2002. – 496 с.

3. Правові основи захисту комп'ютерної інформації від протиправних посягань : матеріали міжвуз. наук.-практ.конф., 22 груд. 2000 р. / Донец. ін-т внутр. справ ; за ред. Ю. Л. Титаренко. – Донецьк, 2001. – 320 с.

4. Тертишник В. М. Науково-практичний коментар до Кримінально-процесуального кодексу України / В. М. Тертишник. – К. : АСК, 2002. – 1056 с.

5. Україна в міжнародно-правових відносинах. – Кн. 1 : Боротьба зі злочинністю та взаємна правова допомога : зб. док. (укр. та рос. мовами). – К. : Юрінком, 1996. – 1184 с.

Одержано 19.11.2013

УДК 343.451

Андрій Анатолійович ПРИХОДЬКО,
заступник начальника курсу навчально-наукового інституту підготовки фахівців для підрозділів кримінальної міліції Харківського національного університету внутрішніх справ,
Владислав Вячеславович ПАНКЕЄВ,
курсант
Харківського національного університету внутрішніх справ

ФІШИНГ ЯК НАЙПОШИРЕНІШИЙ ВИД ШАХРАЙСТВА В ІНТЕРНЕТІ: ВИДИ ТА СУТНІСТЬ

Застосування сучасних інформаційних технологій несе в собі, крім позитивних аспектів, потенційну можливість використання сучасних комп'ютерних технологій з корисливою метою. Інтенсивна автоматизація систем в економіці, управлінні та особливо в кредитно-банківській діяльності обумовило виникнення нового класу злочинів - злочинів в області комп'ютерної інформації або «комп'ютерних» злочинів. Проблема шахрайства в Інтернеті дуже актуальна у наш час. І найпоширенішим видом шахрайства в Інтернеті є фішинг.

Фішинг – це вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів Інтернету персональних даних клієнтів інтернет-аукціонів, сервісів з переводу або обміну валюти, інтернет-магазинів. Шахраї використовують різні способи, які змушують користувачів самим розставатися з конфіденційними даними. Фішинг-зловмисник відправляє своїй жертві нібито офіційні листи, спонукаючи користувача добровільно відправити йому конфіденційну інформацію. Найцікавішими для фішерів є імена користувача і паролі. За допомогою цих даних злочинці можуть видавати себе за володаря інформації і робити від його імені різні дії. Має бути досконало зрозуміло, що банк або страхова агенція ні за яких обставин не просить своїх клієнтів повідомити по електронній пошті, по СМС або по телефону номери кредитних карт, PIN, TAN або інші дані для організації доступу до різних систем.

Вперше фішинг з'явився у 1996 р., коли передплатники служби America Online почали одержувати підроблені повідомлення, в яких просили повідомити їхній пароль для входу в систему, нібито «для модифікації інформації». Тоді шахраї просто користувалися Інтернетом, оплачуючи його за допомогою чужих рахунків.

Можна виділити три види фішингу, такі як: поштовий, онлайновий та комбінований. Перший з них полягає у відправленні жертві листа по електронній пошті в якому присутня вимога вислати у відповідь будь-які дані, які цікавлять шахрая. В якості прикладу можна привести самий примітивний спосіб одержання даних для виходу в Інтернет. Зловмисник просто представляється співробітником провайдера користувача Інтернету й, розповідаючи історію про «базу даних, яка вийшла з ладу», просить останнього вислати його логін та пароль. Причому для більшої переконливості шахрай може використати поштову скриньку з назвою сервера, що схожий на назву сервера провайдера. Під онлайновим фішингом маються на увазі афери, коли зловмисники копіюють які-небудь сайти, найчастіше інтернет-магазини. При цьому вони використовують схожий дизайн та доменні імена. Комбінований вид майже відразу ж одержав величезне поширення. Суть полягає в наступному: шахрай створює підроблений сайт якої-небудь організації, а потім заманює на нього користувачів за допомогою листів-принад. Головна небезпека комбінованого фішинга полягає в його високій правдоподібності.

З далекого 1996 року фішинг еволюціонував і так звані «фішери» стали більш винахідливими. Тепер посилання на фальшиві сервери зловмисники ховають усередину коду листа, показуючи користувачеві посилання у вигляді дійсної адреси, тобто використовуються віруси-хробаки і шпигунські програм для непомітного перенаправлення користувачів на фальшиві сайти. Крім того, самі фішингові атаки стали більш ефективними. Відбулося це завдяки персоніфікації: тепер для того, щоб виманити у жертви секретні дані про кредитну карту, шахраї використовують реальну інформацію про власника рахунку. Для більшої переконливості в електронному повідомленні використовуються логотипи банку, імена й прізвища реальних керівників організації. Потім все відбувається за давно налагодженою схемою: жертві пропонується зайти на ідентичний банківському сайт й «підтвердити» інформацію про рахунок. Необхідність таких дій шахраї пояснюють виходом з ладу програмного забезпечення банку або атакою хакерів.

Одержано 21.11.2013

УДК 65.012.8+004

Роман Григорьевич СОБОЛЬ,
курсант
Харьковского национального университета внутренних дел,
Максим Викторович ПОЛЯКОВ,
курсант
Харьковского национального университета внутренних дел

РАЗВИТИЕ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ ВЕДУЩИХ СТРАН

На сегодняшний день информационные технологии проникли практически во все сферы жизни человека, многие уже не представляют свою жизнь без интернета. Поиск информации упростился. С одной стороны, это определенно положительный фактор, а с другой – может быть чревато негативными последствиями, поскольку зачастую возникают возможности для манипуляций. Поэтому уже давно и во всем мире актуальны вопросы защиты личной информации и обеспечения кибербезопасности.

Эффективный контроль преступности в киберпространстве требует интенсивного международного сотрудничества, так как эта проблема не ограничивается рамками одной страны. Именно поэтому требуется разработка и внедрение новых механизмов международного сотрудничества аналогичных существующим: проект ООН по разработке законодательства в области киберпреступности для стран Африки (проект ESCWA), совместный проект Европейского союза и Международного Союза Электросвязи для государств Тихоокеанского региона (проект ICB4PAC), Конвенция Совета Европы о киберпреступности, решения Совета Европейского Союза, Модельный Закон стран Карибского Бассейна о киберпреступности (проект HIPCAR) и многие другие.

Уже давно в мире предпринимаются определенные шаги в направлении противодействия киберпреступности.

В начале 2013 г. в Совете федерации России состоялось обсуждение проекта национальной стратегии кибербезопасности и предложено создание «экспертно-консультационного органа при президенте РФ по вопросам кибербезопасности», а также расширить «оперативные возможности» правоохранителей. Все это позволит создать «фронт борьбы с киберпреступниками» [1].

Украине так же необходим полноценный Закон о борьбе с киберпреступностью, в тоже время на заседании, состоявшемся 6 марта 2013 года, Кабинет Министров Украины одобрил законопроект «О внесении изменений в Закон Украины «Об основах национальной безопасности Украины» относительно кибернетической безопасности Украины. Указанный законопроект направлен на формирование основ государственной политики в сфере обеспечения кибернетической безопасности Украины путем определения основных реальных и потенциальных угроз национальной безопасности кибернетического характера, основных направлений государственной политики и основных функций субъектов обеспечения национальной безопасности в этой сфере. В законопроекте, в частности, оговаривается введение таких основополагающих понятий, как «кибернетическая безопасность (кибербезопасность)» и «кибернетическое пространство (киберпространство)» [2].

В рамках заключительной конференции проекта CyberCrime@EAP Украина продемонстрировала значительный прогресс в защите прав граждан в противодействии киберпреступности. «У нас достаточно высокие показатели раскрываемости преступлений в банковской сфере (80 % возврата украденных средств)», - отметил представитель МВД Украины.

Александр Зегер, представитель Секретариата Совета Европы, в свою очередь отметил высокий профессионализм украинских коллег, и подчеркнул: «Созданные украинскими правоохранителями механизмы по противодействию киберпреступности могут послужить примером и для других стран, а главное, что и другие страны могут использовать этот опыт в своей работе» [3].

На данном этапе Украина активно занимается вопросом сотрудничества с другими странами в вопросе борьбы с киберпреступностью. Только в течении этого года (2013) состоялись встречи с представителями таких стран как США, ФРГ, Чешской Республики, Республики Австрии, Литвы, а так же другими странами-участниками ЕС.

Вопрос противодействия преступности в киберпространстве и создание эффективной системы кибербезопасности страны является одним из приоритетных направлений деятельности правоохранительных органов ведущих стран мира.

Подобный опыт уже имеет целый ряд государств. Так, в США это направление по приоритетности уступает только борьбе с терроризмом и шпионажем.

Для комплексного противодействия киберпреступности не достаточно и невозможно предпринимать меры только в рамках одного государства, необходим целый комплекс взаимодействий с другими странами.

Таким образом, международное сотрудничество является ключевым моментом в борьбе с киберпреступностью. Это единственный путь обеспечить безопасность пользователей и государства от электронных посягательств. В то же время, неэффективность международного сотрудничества – в частности, в вопросах взаимной правовой помощи – по-прежнему считается одним из основных препятствий к принятию эффективных мер по борьбе с киберпреступностью.

Список использованных источников:

1. Борьбу с киберпреступлениями предлагают вывести на новый уровень [Электронный ресурс]. – Режим доступа: http://www.kommersant.ru/doc-y/2136150.

2. Правительство одобрило законопроект о кибернетической безопасности Украины [Электронный ресурс]. – Режим доступа: http://www.kmu.gov.ua/control/publish/article?art_id=246124654.

3. Максим Литвинов: «Объединив усилия, мы достигнем высоких результатов в борьбе с киберпреступностью» [Электронный ресурс]. – Режим доступа: http://mvs.gov.ua/mvs/control/main/ru/publish/article/915199.

Одержано 19.11.2013

УДК 343.98

Ігор Володимирович КОБЗЕВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційної та економічної безпеки
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ,
Костянтин Едуардович ПЕТРОВ,
доктор технічних наук, професор,
професор кафедри інформаційних технологій та захисту інформації
факультету права та масових комунікацій
Харківського національного університету внутрішніх справ

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Комп'ютерні і телекомунікаційні технології охоплюють практично усі сфери життя суспільства. Воно поставило ці технології собі на службу, що породило новий вид злочинності – комп'ютерну злочинність.

Можна виділити такі основні тенденції розвитку комп'ютерної злочинності в Україні: найвищі темпи росту; корислива мотивація більшості вчинених комп'ютерних злочинів; ускладнення способів скоєння комп'ютерних злочинів і поява нових видів протиправної діяльності у сфері інформаційних технологій; зростання професіоналізму комп'ютерних злочинців; омолодження комп'ютерної злочинності та збільшення долі осіб, що раніше не притягувалися до кримінальної відповідальності; зростання матеріальних збитків від комп'ютерних злочинів в загальній частці збитків від інших видів злочинів; перенесення центру тяжіння на скоєння комп'ютерних злочинів з використанням комп'ютерних мереж; переростання комп'ютерної злочинності в розряд транснаціональної злочинності; високий рівень латентності комп'ютерних злочинів. Боротьба з кіберзлочинністю повинна стати пріоритетним напрямком усіх правоохоронних органів і силових відомств.

Оскільки Інтернет взагалі нікому конкретно не належить, ніким конкретно не регулюється, то немає і адміністративної інстанції, що відповідає за Інтернет. Положення ускладнюється ще й тим, що інформація може зберігатися на Web-сайтах в інших країнах або на інших континентах, де законодавство не

готове встановлювати відповідальність за зберігання і поширення непристойного або забороненого контенту. Проблема повинна вирішуватися на міжнародному рівні, можливо у рамках таких організацій, як ООН і ЮНЕСКО.

Результати аналізу характеристики комп'ютерної злочинності дозволяють прогнозувати подальше ускладнення боротьби з нею з огляду на те, що способи скоєння комп'ютерних злочинів з кожним роком набувають все більш витонченого характеру. До вирішення цієї проблеми необхідно підходити комплексно.

Фахівці виділяють наступні елементи організації діяльності правоохоронних органів в глобальних інформаційних мережах: вивчення і оцінка обстановки в мережах; здійснення оптимальної розстановки сил і засобів, забезпечення взаємодії; управління, планування і контроль; координація дій суб'єктів правоохоронних органів.

Важливим елементом системи заходів боротьби з комп'ютерною злочинністю є заходи превентивного характеру, або заходи попередження. Більшість іноземних фахівців вказують на те, що попередити комп'ютерний злочин набагато легше і простіше, ніж розкрити і розслідувати його. Зазвичай виділяють три основні групи заходів попередження комп'ютерних злочинів, до яких можна віднести правові, організаційно-технічні та криміналістичні.

Стратегія міжнародної співпраці у сфері протидії комп'ютерної злочинності і пріоритетні напрями її реалізації полягають в укладанні міждержавних угод, організації міждержавної оперативно-розшукової діяльності, прийнятті міждержавного регламенту і вдосконаленні інтеграційних процесів у рамках міждержавних організацій, обґрунтуванні необхідності розробки і прийнятті відповідної комплексної міждержавної програми.

Сукупність потреб, задоволення яких забезпечує існування і можливість прогресивного розвитку кожного громадянина, суспільства і держави – це частина національних інтересів, без реалізації яких неможливо забезпечити стабільний стан держави і суспільства, а також нормальний розвиток країни як незалежного суб'єкта міжнародних відносин.

Усі інтереси в інформаційній сфері підрозділяються на інтереси особи, держави та суспільства. Проблема кіберзлочинності нині зачіпає, як цілі держави, так і окремих осіб.

Виходячи з вищевикладеного, можна зробити висновок, що протидія кіберзлочинності – це важлива частина захисту національних інтересів.

Кіберзлочинність вже стала великою проблемою для всього світу. Правоохоронні органи намагаються боротися з нею, законодавці ухвалюють нові закони, поліцейські агентства формують спеціальні підрозділи по боротьбі з кіберзлочинністю. Щоб успішно боротися з кіберзлочинністю, повинні залучатися IT-фахівці і ті активні члени суспільства, яких зачіпає злочинна діяльність, що знайшла сприятливе середовище – віртуальний простір.

Необхідно створити уніфіковану класифікацію і формальну модель кіберзлочинів, які полегшать протидію і розслідування злочинів такого роду. Організація забезпечення інформаційної безпеки повинна носити комплексний характер і ґрунтуватися на глибокому аналізі можливих негативних наслідків. При цьому важливо не упустити будь-які істотні аспекти. Аналіз негативних наслідків передбачає обов'язкову ідентифікацію можливих джерел загроз, чинників, що сприяють їх прояву і, як наслідок, визначення актуальних загроз інформаційній безпеки.

Для ефективної протидії цьому виду злочинів зусиль тільки на національному рівні явно недостатньо. Потрібна розробка, стандартизація і уніфікація законодавства і програмних засобів, що дозволить визначати місцезнаходження і встановлювати особи злочинців, які протиправно використовують комп'ютерні мережі і глобальні телекомунікаційні системи. Все це і намагаються робити країни, що підписали Європейську конвенцію по боротьбі з кіберзлочинністю.

Одержано 06.11.2013

УДК 343.98

Віталій Анатолійович СВІТЛИЧНИЙ,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів
боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ,
Юрій Миколайович ОНИЩЕНКО,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів
боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

СТАН ТА ОСОБЛИВОСТІ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Під терміном «кіберзлочинність» прийнято мати на увазі будь-який злочин, здійснений за допомогою віртуального простору і комп'ютерів. У реальному світі кібератаки паралізують діяльність серйозних фірм, електронних ЗМІ, громадяни втрачають гроші завдяки різним шахрайським схемам. Проте точний об'єм втрат визначити неможливо, адже багато фірм піклуючись про свою репутацію, не називають суми своїх збитків, а деякі з них навіть не підозрюють, що на них здійснювалися напади з боку кіберзлочинців. Тому недивно, що безпекою кіберпростору стурбовані уряди більшості країн світу.

У МВС України створено Управління по боротьбі з кіберзлочинністю. Основним завданням якого є організаційне і практичне забезпечення реалізації державної політики по попередженню і протидії злочинам і правопорушенням, що здійснюються з використанням інформаційних технологій і телекомунікаційних мереж, а також протидії легалізації доходів, отриманих від таких злочинів і правопорушень [1].

Боротьба з кіберзлочинністю неможлива без глибокого розуміння правових основ щодо використання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі Internet і обумовленими цими характеристиками правовими і соціальними проблемами, з якими стикаються законодавці і правоохоронні органи усіх країн, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і ріст кіберзлочинності.

Нажаль, в Україні на сьогодні відсутнє ефективне законодавство у сфері боротьби з кіберзагрозами і кіберзлочинами. Як відомо, історія законопроекту № 2483 «Проект Закону

про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» триває близько двох років і в результаті законопроект не ухвалений.

Країні ще належить зіткнутися з проблемою кіберзлочинності повною мірою, але експерти вже зараз розуміють, що потрібний комплексний підхід, а саме: законодавчі заходи, комп'ютерна грамотність користувачів мережі і активне використання систем інформаційної безпеки великими операторами інтернет-транзакций, такими як банки і оператори стільникового зв'язку. За даними Національного центру підтримки електронного урядування в I кварталі 2013 року наша країна займала «почесне» 5-те місце серед країн, на вебресурсах яких, розміщені шкідливі програми. Кількість зафіксованих інтернет-загроз перевищила 47 млн випадків, а зараженню через веб-ресурси в першому кварталі 2013 року піддалися 49 % українських користувачів. З такими показниками Україна зайняла 8-ме місце в списку країн, мешканці яких піддаються найбільшому ризику зараження в Інтернеті [2].

Кіберзлочинці мають великі знання в областях інформаційних технологій і електроніки, і тому протидіяти їм непросто. Як правило, такі протизаконні дії не обмежуються рамками одного міста або однієї країни. І хоча Кримінальний кодекс України передбачає обмеження свободи на строк до 3 років або позбавлення волі на строк до 12 років для тих, хто промишляє інформаційним шахрайством, проте кіберзлочинців це не зупиняє, недосконалість законодавства, величезні гроші при відносно невисокому ризику бути спійманим, – усе це призводить до абсолютної або майже абсолютної безкарності.

Звичайно, є реальні рішення суду, є відшкодування фінансового збитку, але чи варто довіряти офіційній статистиці? Адже багато хто, комерційні і державні структури, вважає за краще не поширювати інформацію про те, що сталося, особливо це стосується випадків просочування даних, оскільки не бажають, щоб конкуренти використали ситуацію у своїх цілях або іншого негативного розголосу.

Найбільшої шкоди кіберзлочини завдають як фінансовому стану, так і діловій репутації, причому шкода репутації перевищує грошові втрати [3]. Сьогодні економічна і політична

репутація є одними з найбільш важливих активів для комерційних і державних структур, і саме на них ґрунтується довіра клієнтів до банків і громадян до уряду країни. Втрати від крадіжки, комп'ютерного злому одноразові, а тінь, кинута на репутацію, може вплинути на розвиток подій в майбутньому.

Список використаних джерел:

1. Управління по боротьбі з кіберзлочинністю [Електронний ресурс]. – Режим доступу: http://cybercrimecenter.info/ru/.

2. Кіберзлочинність по-українськи [Електронний ресурс]. – Режим доступу: http://internetua.com/kiberprestupnost-po-ukrainski/.

3. Репутаційна шкода від кіберзлочинів удвічі перевищує фінансові втрати банків [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/news/top/index.shtml?2013/11/08/548924.

Одержано 07.11.2013

УДК [343.98:004](477)

Ольга Сергіївна ЛУНЬОВА,
ад'юнкт
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ В УКРАЇНІ

На сьогоднішній день кримінальні правопорушення з використанням комп'ютерних і цифрових технологій – це одні з найактуальніших та динамічних суспільно небезпечних посягань. Розвиток науки й технологій у сфері комп'ютеризації та інформатизації зумовили швидке їх поширення та відповідний ріст суспільної небезпеки.

На початку 90-х років в українській науковій літературі з'явилося поняття «кіберпростір» - це новий, різноманітний за своєю топологією, вид семіотичного простору, в якому операції зі знаками здійснюються за допомогою сучасних комп'ютерних технологій, що полегшують та істотно прискорюють розумову діяльність людей.

Виникнення певних умов для розвитку нових суспільних відносин приводить до появи осіб, які намагаються отримати незаконну вигоду за рахунок відсутності їх належної правової регламентації. Так само сталося і з появою кіберпростору. Через кроткий проміжок часу українському суспільству стало добре відомо і поняття «кіберзлочинність» – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням

інформаційних технологій і глобальних мереж. З'явилася проблема: до органів внутрішніх справ зверталися особи із заявами про порушення їх прав, але такі дії зловмисників не були віднесені до злочинів чинним на той час Кримінальним кодексом. Все це в сукупності призвело до негайної потреби прийняття відповідних нормативних актів, що регулюватимуть виниклі суспільні відносини.

Національне законодавство в сфері захисту, застосування та використання комп'ютерних технологій розвивалось поступово, в декілька етапів.

В 1994 році було прийнято Закон України «Про захист інформації в автоматизованих системах», який в 2005 році було викладено в новій редакції «Про захист інформації в інформаційно-телекомунікаційних системах». Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Стаття 2 закону визначає, що об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Закон України «Про основи національної безпеки» від 19.06.2003 у ст. 7 визначив, що на сучасному етапі одними з основних реальних та потенційних загроз національній безпеці України, стабільності в суспільстві, в інформаційній сфері є комп'ютерна злочинність та комп'ютерний тероризм; а у ст. 8 закріплено, що одним з основних напрямів державної політики з питань національної безпеки України в інформаційній сфері є вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну.

Прийнятий у 2001 році Кримінальний кодекс України у розділі XVI вперше передбачив кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, фактично легалізувавши кримінальну відповідальність за протиправні діяння в зазначеній сфері.

Особливою рисою кіберзлочинності є її глобальність та міжнародна розповсюдженість, адже найчастіше зловмисники

використовуюсь глобальні телекомунікаційні мережі, наприклад Інтернет. Тому протидія кіберзлочинам в окремо взятій державі малоефективна і вимагає укладання міжнародних угод та договорів.

Україна ратифікувала низку міжнародних угод, зокрема «Угоду про співробітництво у формуванні інформаційних ресурсів і систем, реалізації міждержавних програм держав - учасниць Співдружності Незалежних Держав у галузі інформатизації», укладену в Москві 24.12.1999, «Угоду про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі зі злочинами у сфері комп'ютерної інформації», укладену в Мінську у 2001 році, згідно якій: «злочин в сфері комп'ютерної інформації – кримінально каране діяння, предметом посягання якого є комп'ютерна інформація; комп'ютерна інформація – інформація, що знаходиться в пам'яті комп'ютера, на магнітних чи інших носіях в формі, доступній сприйняттю ЕОМ, або що передається по каналам зв'язку». Одним з фундаментальних міжнародних договорів, що регулює відносини в сфері кіберпростору стала «Конвенція про кіберзлочинність» від 23.11.2001, яку Україна ратифікувала у 2005 році.

Конвенція поділяє злочини за об'єктом посягання на такі: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, 2) правопорушення, пов'язані з комп'ютерами, 3) правопорушення, пов'язані зі змістом, 4) правопорушення, пов'язані з порушенням авторських та суміжних прав. Частина друга Конвенції присвячена «Процедурному праву», яка регламентує сферу процедурних положень, умови і запобіжні заходи, термінове збереження комп'ютерних даних, які зберігаються, термінове збереження і часткове розкриття даних про рух інформації, порядок представлення, обшук і арешт комп'ютерних даних, які зберігаються, збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації, юрисдикцію.

В 2011 році в Україні був створений Департамент по боротьбі з кіберзлочинністю МВС України, який діє на підставі Наказу Міністра МВС України від 31.05.2012 № 494 «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю

ГУМВС, УМВС». Основним завданням Управління боротьби з кіберзлочинністю МВС України є організаційне та практичне забезпечення реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, що вчиняються з використанням інформаційних технологій та телекомунікаційних мереж (у сфері інформаційно-телекомунікаційних технологій, у сфері електронних платежів і господарської діяльності, зокрема, порушення прав інтелектуальної власності та заняття гральним бізнесом, злочини проти інформаційної безпеки, у тому числі незаконні дії зі спеціальними технічними засобами негласного отримання інформації), а також протидії легалізації доходів, отриманих від таких злочинів і правопорушень.

Подальший розвиток національного законодавства та прийняття нового Кримінального процесуального кодексу 2012 року передбачили низку новел. Так положення ст. 99 Кримінального процесуального кодексу України 2012 року, закріплюють, що до документів можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні). А ст. 84 КПК закріплено, що процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. Тож електронні носії інформації - це джерела доказів. Таким чином, з'явилась можливість доказування наявності того чи іншого протиправного діяння, пов'язаного з рухом інформації в електронному вигляді в реальному масштабі часу.

На теперішній час законодавство України в сфері протидії та розслідування кіберзлочинів знаходиться в процесі становлення та потребує подальшої розробки. Процес нормативного регулювання цієї сфери суспільних відносин ускладнюється динамікою змін самих відносин. Адже щоб ефективно захищати суспільство від кіберзлочинності треба постійно слідкувати за діяльністю обізнаних в цій сфері спеціалістів, виявляти нові тенденції та засоби вчинення злочинних дій та приймати відповідно до цього нормативні акти.

Проблема профілактики і протидії кіберзлочинності в Україні – це комплексна проблема яка потребує подальшого розвитку не тільки законотворчої діяльності, а й таких наук як криміналістика та кримінологія, кримінальний процес,

виховання та навчання кваліфікованих в цій галузі спеціалістів. Жодна держава світу на сьогодні не в змозі ефективно протистояти кіберзлочинності самостійно. Тому основним завданням, що стоїть перед Україною, є активізація міжнародної співпраці в цій сфері.

Одержано 22.11.2013

УДК 34(477)

Руслан Володимирович ОЛІЙНИК,
здобувач Харківського національного університету внутрішніх справ, прокурор Черкаського району Черкаської області

ПРІОРИТЕТНІ НАПРЯМКИ ДІЯЛЬНОСТІ ПРОКУРАТУРИ УКРАЇНИ ЩОДО ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Сьогодні у цілому світі, у тому числі й в Україні, набуває особливої актуальності проблема організації ефективної боротьби з кіберзлочинністю, яка стала одним з основних викликів сучасному суспільству. Так, в Україні за останнє десятиліття можна спостерігати стійку тенденцію до збільшення кількості кіберзлочинів. Спектр кіберзлочинів різноманітний – від створення комп'ютерних вірусів, вчинення крадіжок, різних видів шахрайства, комп'ютерних підробок до порушення авторських прав і розповсюдження дитячої порнографії. Зареєстровано випадки і так званого кібертероризму, коли комп'ютер використовувався як зброя для блокування важливих систем життєзабезпечення і створення загрози для цілих груп населення.

Найбільшу небезпеку становить несанкціонований доступ до інформаційних ресурсів. Вагомі заходи усіх державних інституцій та правоохоронних органів свідчать про те, що ця проблема надзвичайно важлива для суспільства, яке має активно протидіяти подібним негативним явищам.

Комплекс завдань захисту інформаційної безпеки органів прокуратури України є частиною загальних заходів щодо попередження та протидії кіберзлочинності. На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці прокуратури можна назвати:

– несанкціонований доступ до інформаційних ресурсів прокуратури, зокрема: розкриття інформаційних ресурсів; порушення цілісності інформаційних ресурсів; збій у роботі обладнання тощо;

– негативні інформаційні впливи з використанням засобів масової інформації, а також мережі Інтернет, спрямовані на підрив авторитету органів прокуратури;

– розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави.

Важливу загрозу становить несанкціонований доступ до інформаційних ресурсів. Зокрема, загроза розкриття інформаційних ресурсів прокуратури полягає в тому, що інформація стає відомою необмеженій кількості осіб. Це можуть бути як відкриті ресурси, так і ресурси з обмеженим доступом. Дані ресурси мають передаватися один одному і зберігаються в єдиній інформаційній системі.

Загроза порушення цілісності інформаційних ресурсів прокуратури полягає в умисному впливі (модифікації, видаленні, знищенні) даних, які зберігаються в інформаційній системі органів прокуратури, а також передаються від даної інформаційної системи до інших. Систему органів прокуратури становлять: Генеральна прокуратура України, прокуратури Автономної Республіки Крим, областей, міст Київ і Севастополь (на правах обласних), Дніпровська екологічна прокуратура (на правах обласної), регіональні військові прокуратури, міські, районні, міжрайонні, районні в містах, і якщо на рівні Генеральної прокуратури та прокуратур обласного значення така єдність є організованою, то зв'язки районних, міжрайонних, районних в містах залишаються не налагодженими на відповідному рівні.

Загроза збою в роботі самого обладнання може виникнути при блокуванні доступу до одного або декількох ресурсів інформаційної системи. Насправді блокування може бути постійним, коли ресурс, що запитується, не може бути отриманим або виникають затримки в його отриманні, що є достатнім для того, щоб він став некорисним.

Найбільш частими і небезпечними є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, що обслуговують інформаційні системи. Іноді такі помилки є загрозами (неправильно введені дані, помилки в програмі, котрі викликають колапс системи), іноді вони створюють ситуації, якими можуть скористатися зловмисники.

Наступними за розміром шкоди можна назвати фальсифікації (пошкодження обладнання; вбудовування логічної

бомби, яка з часом руйнує програми і дані; введення неправильних даних; знищення даних; зміну даних; модифікацію даних; надання доступу до даних із обмеженим доступом тощо). У більшості випадків суб'єктами вчинення даних дій є штатні працівники структурних підрозділів органів прокуратури, які добре обізнані з роботою інформаційної системи, а також заходів безпеки. Це можуть бути співробітники, які незадоволені або не поділяють цінностей правоохоронної діяльності.

Невдоволені своїм становищем співробітники створюють реальну загрозу інформаційній безпеці прокуратури. Необхідно слідкувати за тим, щоб при звільненні співробітника його права доступу до інформаційних ресурсів були повністю обмежені, а після його звільнення змінені всі паролі доступу до внутрішньої мережі. Більш того, слід обмежити його спілкування з особами, що мають доступ до важливої інформації.

Серйозною загрозою можуть бути програмні віруси. Водночас дотримання правил користування комп'ютерною технікою, а також наявність у штаті співробітників органів прокуратури відповідного фахівця з даних питань значно полегшить вирішення зазначених завдань.

У той же час загрози інформаційній безпеці, з одного боку, є організаційним компонентом системи органів прокуратури, а з іншого – індикатором ефективності її функціонування, адже реалізація загроз і переростання їх у небезпеки свідчить про неефективність функціонування даної системи і навпаки. На сьогодні розглядати будь-які загрози в інформаційній сфері необхідно з урахуванням того контексту, в якому вони виникають і знаходять свій прояв. У той же час на державному рівні з метою забезпечення інформаційної безпеки прокуратури необхідно частіше залучати засоби масової інформації до забезпечення неухильного додержання конституційних прав і свобод людини і громадянина, захисту конституційного устрою, вдосконалення системи політичної влади з метою зміцнення демократії, духовних та моральних засад суспільства; підвищення ефективності функціонування правоохоронних органів.

Одержано 25.11.2013

РОЗДІЛ 2
КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ ПРОБЛЕМИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

УДК 343.12

Євген Дмитрович ЛУК'ЯНЧИКОВ,
доктор юридичних наук, професор,
професор кафедри кримінально-правових дисциплін
Національної академії внутрішніх справ,
Борис Євгенович ЛУК'ЯНЧИКОВ,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики та судової медицини
Національної академії внутрішніх справ

УЧАСТЬ СПЕЦІАЛІСТА В РОЗСЛІДУВАННІ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Організація і проведення слідчих (розшукових) дій під час розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж має певні особливості, що вимагає від слідчого як особистого володіння спеціальними знаннями та навичками, так і використання допомоги осіб, що на високому рівні володіють такими знаннями. Необхідність використання спеціальних знань в галузі комп'ютерів та інформаційних мереж може виникати під час провадження більшості слідчих (розшукових) дій в процесі розслідування таких злочинів.

Чинний КПК України (ст. 71) передбачає дві форми використання допомоги спеціаліста у досудовому провадженні: а) надання консультацій з питань, що потребують відповідних спеціальних знань; б) надання безпосередньої технічної допомоги під час досудового розслідування.

Особливого значення використання спеціальних знань набуває під час проведення таких слідчих (розшукових) дій як слідчий огляд та обшук, оскільки вони пов'язані безпосередньо з виявленням, дослідженням та вилученням комп'ютерного обладнання і його програмного забезпечення.

Незважаючи на певний рівень володіння потрібними знаннями у цій галузі, під час підготовки до проведення зазначених слідчих дій слідчому необхідно вирішити питання щодо залучення до цього певного кола спеціалістів. Залучення осіб, що володіють спеціальними знаннями до проведення

слідчих дій обумовлюється необхідністю використання сучасних досягнень у сфері комп'ютерних систем та інформаційних технологій.

Використання допомоги зазначених осіб дозволить своєчасно визначати індивідуальний почерк роботи програміста й ідентифікаційних характеристик розроблених ним програм, перелік електронних адрес і сайтів Інтернет, якими оперував користувач. Спеціаліст допоможе дослідити матеріальні носії з метою пошуку відповідної інформації та провести ідентифікацію комп'ютерних систем за слідами на різних матеріальних носіях інформації.

Досліджуючи дане питання І. В. Європіна слушно звертає увагу на труднощі, що виникають у доборі спеціалістів, яким можна доручити таку важливу справу [1, с. 10–11]. Аналіз наукової літератури та матеріалів практики дозволяє виділити декілька варіантів залучення обізнаних осіб до участі в розслідуванні комп'ютерних злочинів. В першу чергу ними можуть бути співробітники експертних установ Міністерства юстиції або МВС України. Зазначені особи володіють знаннями, що необхідні для пошуку, фіксації, вилучення та дослідження комп'ютерних слідів злочину; мають документи, що підтверджують їх кваліфікацію; проходять періодичну професійну перепідготовку і підвищення кваліфікації; не мають особистого інтересу у конкретному провадженні.

Другу групу обізнаних осіб складають спеціалісти з ІТ-технологій інших підприємств, організацій, установ. Щодо таких осіб пропонується створювати постійний список, періодично його переглядати та оновлювати, за відповідними критеріями. Така організація цієї роботи сприятиме підвищенню професійного рівня зазначених осіб, забезпечить результативність їх допомоги слідчому. Періодичне їх залучення до участі у слідчих діях сприятиме формуванню у них цілеспрямованих пошукових навичок. Такий спеціаліст може виявити спеціальні засоби, встановлені власником в комп'ютері для знищення інформації при несанкціонованому доступі; встановити необхідний пароль для доступу до інформації, з'ясувати правила його використання і чи не призведе порушення цих правил до знищення файлів тощо [1, с. 11].

Другою формою використання спеціальних знань під час проведення слідчих (розшукових) дій є отримання консультацій фахівців з комп'ютерних технологій. Під консультацією

розуміють – довідкову діяльність, яка не потрібує проведення будь-яких досліджень для відповіді на запитання слідчого. Опитування експертів показує, що така форма використання спеціальних знань в процесі розслідуванні комп'ютерних злочинів є достатньо розповсюдженою [2, с. 96]. Нажаль чинний КПК не визначає форму, в якій можуть надаватися консультації на досудовому провадженні. Якщо слідувати за аналогією з формою консультації в процесі судового розгляду – вона може бути усною або письмовим роз'ясненням (ст. 360 КПК).

Для розслідування комп'ютерних злочинів можуть створюватися групи, до складу яких залучаються спеціалісти на постійній основі. У таких випадках можна обмежитися отриманням усних консультацій. У будь-який момент слідчий може звернутися до такого спеціаліста за консультацією або роз'ясненням. Коли слідчий звертається по допомогу епізодично, краще скористатися письмовими консультаціями. Маючи письмові роз'яснення спеціаліста, слідчий може звертатися до їх змісту у будь-який момент планування відповідної слідчої (розшукової) дії або тактичної операції, користуватися інформацією, що у них міститься.

На завершення слід зазначити, що використання допомоги спеціаліста сприяє підвищенню результативності розслідування комп'ютерних злочинів.

Список використаних джерел:

1. Європіна І. В. Криміналістичне забезпечення протидії комп'ютерній злочинності : автореф. дис. … канд. юрид. наук : 12.00.09 / Європіна Ірина Володимирівна. – К., 2011. – 18 с.

2. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09 / Пашнєв Дмитро Валентинович. – Х., 2007. – 335 с.

Одержано 14.11.2013

УДК 343.98

Руслан Леонтійович СТЕПАНЮК,
доктор юридичних наук, доцент,
начальник кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ СТАНУ МЕТОДИКО-КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Швидкий розвиток інформаційних технологій, активне впровадження засобів комп'ютерної техніки і програмних продуктів у життя сучасного суспільства, широке розповсюдження комп'ютерних систем і мереж закономірно призводить і до окремих негативних явищ, до яких слід віднести кіберзлочинність. Як відомо, за останні роки кількість користувачів мережі Інтернет збільшилось у сотні разів. У цій глобальній комп'ютерній мережі здійснюється все більше різноманітних операцій, зокрема підприємницька діяльність, спілкування між людьми, розміщення аудіовізуальної та іншої продукції тощо. Не дивовижно, що зручність використання комп'ютерних систем і мереж для задоволення повсякденних потреб людини робить їх привабливим засобом для протиправних посягань.

У сучасний період широкого розповсюдження набувають такі суспільно-небезпечні прояви у кіберпросторі, як шахрайства з використанням комп'ютерних систем і мереж, злочини, пов'язані з порушенням авторських і суміжних прав, розповсюдження порнографії, пропаганда насильства та жорстокості, тероризму, заклики до масових заворушень, прояви вандалізму тощо. Тому закономірно, що криміналістична наука не може залишатись осторонь і повинна забезпечувати органи досудового розслідування та суди ефективними прийомами, засобами і методами боротьби з кіберзлочинністю.

В цьому сенсі слід відзначити, що в останні десятиліття спостерігається активізація наукових розробок у галузі криміналістики, спрямованих на формування рекомендацій у даній сфері. Ученими підготовлено досить ґрунтовні праці з питань розслідування злочинів у сфері комп'ютерної інформації, окремих різновидів шахрайств у мережі Інтернет,

розповсюдження порнографії, розкрадань, вчинених за допомогою комп'ютерних систем і мереж у сфері банківської діяльності тощо. Приділялась певна увага і окремим аспектам тактики різних видів огляду та обшуку, пов'язаних із комп'ютерною технікою, використанню спеціальних знань у галузі комп'ютерної техніки під час досудового розслідування, проблемам призначення та проведення експертиз комп'ютерної техніки та програмних продуктів. Проте стан наукового криміналістичного забезпечення діяльності з розслідування кіберзлочинів вимагає удосконалення, як уявляється, у трьох основних напрямах:

а) удосконалення положень криміналістичної техніки щодо використання комп'ютерних технологій у криміналістичній діяльності;

б) розробка та розвиток положень криміналістичної тактики з питань проведення окремих слідчих дій як щодо комп'ютерної техніки та програмних продуктів, так і з використанням комп'ютерних технологій під час підготовки, безпосереднього проведення та фіксації результатів слідчих дій;

в) формування загальнотеоретичних засад методики розслідування кіберзлочинів і створення окремих міжвидових, видових і підвидових методик розслідування цієї категорії злочинів (методико-криміналістичне забезпечення).

Останній напрям наукової діяльності у сучасний період привертає все більшу увагу вітчизняних і зарубіжних дослідників. На монографічному рівні розглядались питання розслідування злочинів у сфері комп'ютерних технологій в цілому, а також деякі окремі криміналістичні методики (наприклад, розслідування шахрайств, пов'язаних із функціонуванням електронних розрахунків). Але системного підходу до формування методико-криміналістичних рекомендацій поки що не спостерігається, що викликано відсутністю чітко визначених класифікаційних критеріїв цієї діяльності.

Як відомо, в основі класифікації окремих методик розслідування знаходиться криміналістична класифікація злочинів, яка, в свою чергу, формується, перш за все, на кримінально-правовій основі. Проте щодо кіберзлочинів єдиний підхід до їх класифікації до цього часу не вироблений. У КК Україні є розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», який охоплює лише невелику

частину злочинних посягань. Інші діяння кваліфікуються як злочини проти власності, виборчих, трудових та інших особистих прав і свобод людини і громадянина, громадського порядку та моральності тощо.

У міжнародних нормативно-правових актах, національному законодавстві різних держав підходи теж відрізняються. При цьому на міждержавному рівні найбільш поширеним є поділ цих злочинів на комп'ютерні злочини (вузьке розуміння) та злочини, вчинені з використанням або за допомогою комп'ютерів, комп'ютерних мереж та інших засобів доступу до кіберпростору (широке розуміння). У конвенції Ради Європи до кіберзлочинів віднесено п'ять груп посягань: злочини безпосередньо проти комп'ютерних даних і систем; злочини, пов'язані з використанням комп'ютерних засобів для одержання економічної вигоди; розповсюдження дитячої порнографії; злочини, пов'язані з порушенням авторських і суміжних прав; поширення інформації расистського та іншого характеру, що підбурює до насильницьких дій, ненависті тощо.

Немає єдиної думки й у чисельних класифікаціях кіберзлочинів, запропонованих ученими.

На нашу думку, в таких умовах криміналістична класифікація зазначеної категорії злочинів може бути побудована на досить традиційному для криміналістики підході, тобто, перш за все, на криміналістичному критерії з використанням кримінально-правової ознаки. У даному випадку мова має йти про побудову окремих методик розслідування:

а) кількох видів злочинів, об'єднаних єдиним криміналістично значущим критерієм (міжвидові методики);

б) виду злочину, передбаченого КК України (видові методики);

в) конкретизованого у залежності від певної ознаки (вчинення злочину з використанням комп'ютерної техніки, систем або мереж) різновиду злочинів (підвидові методики).

Тому вважаємо, що подальше вдосконалення стану методико-криміналістичного забезпечення досудового розслідування кіберзлочинів має здійснюватись у напрямах формування та впровадження в практику низки окремих криміналістичних методик:

а) загальної міжвидової методики розслідування кіберзлочинів;

б) видових методик розслідування злочинів, передбачених статті 361–363-1 КК України;

в) підвидових методик розслідування найбільш поширених різновидів злочинів, характерних для кіберпростору (кіберкрадіжок, кібершахрайств, службових розкрадань у банківській сфері за допомогою комп'ютерної техніки, систем і мереж, кібервандалізму, порушення авторського права і суміжних прав у кіберпросторі тощо.

Одержано 12.11.2013

УДК 343.11

Геннадій Іванович ГЛОБЕНКО,
кандидат юридичних наук, доцент,
заступник начальника кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ,
Олексій Олексійович БОНДАРЕНКО,
кандидат юридичних наук, доцент,
професор кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ОКРЕМІ ПИТАННЯ ЩОДО МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Сучасний світ неможливо уявити без інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та інших засобів комунікацій. Комп'ютерна техніка активно впроваджується в різні галузі людської діяльності. Разом з цим за допомогою даних засобів зростає кількість крадіжок коштів з банківських рахунків, шахрайств з пластиковими платіжними картками, порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж тощо. Ще однією специфічною рисою даного виду злочинів є те, що у більшості випадків втручання в роботу електронно-обчислювальної системи відбувається з метою вчинення інших злочинів, які є більш тяжкими, наприклад, ознайомлення з інформацією містить державну таємницю, підробка грошей і цінних паперів, шпигунство.

Вищевказану категорію кримінальних правопорушень називають злочинами в сфері інформаційних технологій або частіше кіберзлочинами. Слід зазначити, що кіберзлочинність характеризується транснаціональністю, латентністю, динамічністю темпів зростання та масштабністю наслідків. Дане

явище набуває масштабів загрози міжнародній безпеці і стало одним з головних предметів державної та міжнародної діяльності. Так, існує думка, що дохід від кіберзлочинів значно перевищив дохід від інших злочинів, включаючи торгівлю наркотиками. За останніми даними, наведеними в липні 2013 року в спільному аналізі американського Центру стратегічних і міжнародних досліджень та компанії McAfee, щорічні втрати світової економіки від кіберзлочинів досягли вже 500 мільярдів доларів [1].

Тому не безпідставно правоохоронні органи більшості країн світу намагаються консолідувати спільні зусилля в напрямку ефективності боротьби з вищевказаною категорією злочинів. З цією метою 23 листопада 2001 року була прийнята Конвенція по боротьбі з кіберзлочинністю (далі-Конвенція). Цей документ став першою міжнародною угодою з юридичних і процедурних аспектів розслідування та кримінального переслідування кіберзлочинів. Конвенцією передбачені скоординовані дії на національному та міждержавному рівнях з припинення несанкціонованого втручання в роботу комп'ютерних систем, незаконного перехоплення даних і втручання в комп'ютерні системи. Всі кіберзлочини Конвенція ділить на чотири види: злом комп'ютерних систем, шахрайство, заборонений контент (расистські сайти та вебсторінки з дитячої порнографією) та порушення авторських прав. На сьогоднішній день ця Конвенція підписана та ратифікована більш ніж 20 країнами. Повільність процесу її ратифікації пояснюється необхідністю внесення в законодавства країн відповідних змін.

Важливу роль у боротьбі з кіберзлочинністю мають і інші міжнародні угоди в цій галузі, зокрема, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 року, Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського Союзу та міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект SCB4PAC), проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проект ESCWA) та ін.

Слід зауважити, що на даний час чинним законодавством України термін «кіберзлочинність» не визначено. Конвенція також не надає конкретного визначення, хоча і окреслює коло суспільно-небезпечних діянь, що повинні набути статусу кіберзлочинів на рівні національних законодавств. До них

належать: незаконний доступ до комп'ютерної системи, нелегальне перехоплення даних, втручання у дані, втручання у систему, зловживання пристроями, підробка та шахрайство пов'язані з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав. У свою чергу в юридичній літературі пропонується до даної категорії злочинів віднести злочини передбачені Розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України [2, с. 516].

Жодна держава не може захистити себе, вживаючи заходів лише на національному рівні. Необхідна розробка на міжнародному рівні та імплементація в національні законодавства держав процесуальних стандартів, що дозволятимуть ефективно розслідувати злочини в глобальних інформаційних мережах. Крім цього, необхідно налагодити співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні. Складність розкриття злочинів вчинених в досліджуваній сфері, у всякому разі на території країн пострадянського простору, перш за все пояснюється істотним відставанням технологій, що знаходяться на озброєнні правоохоронних органів, від технічного рівня злочинців.

На даний час в Україні сформований базис основних нормативних актів, що стосується досліджуваного питання. Також здійснюється підготовка фахівців для розслідування кіберзлочинів, зокрема, у Харківському національному університеті внутрішніх справ, які отримують глибокі знання як в галузі права, так і комп'ютерних технологій.

Таким чином, міжнародне співробітництво є суттєвим чинником у ліквідації правового вакууму, що існує між розвитком інформаційних технологій та реагуванням на них законодавства. Процес розроблення та впровадження окреслених заходів на міжнародному рівні є комплексною проблемою. Однак, це найбільш ефективний шлях щодо ефективного розслідування кіберзлочинів.

Список використаних джерел:

1. Номоконов В. А. Киберпреступность: проблемы борьбы и прогнозы [Електронний ресурс] / В. А. Номоконов, Т. Л. Тропина. – Режим доступу: http://cripo.com.ua.sect_id=1&aid=164985.

2. Бондаренко О. О. Пропозиції щодо надання органам розслідування повноважень, необхідних і достатніх для ефективної боротьби з кіберзлочинністю (з метою їх внесення до проекту

Кримінального процесуального кодексу України) / О. О. Бондаренко, Г. І. Глобенко, А. А. Васильєв // Актуальні питання діяльності слідчих підрозділів органів внутрішніх справ України : зб. наук. пр. ф-ту з підготовки слідчих ХНУВС за 2012 рік / за заг. ред. чл.-кор. НАПрН України, д-ра юрид. наук С. М. Гусарова; академіка НАПрН України, д-ра юрид. наук, проф. О. М. Бандурки. – Х. : НікаНова, 2013. – С. 516–519.

Одержано 19.11.2013

УДК 65.012.8+004

Marcus K. ROGERS,
Computer and Information Technology Department Purdue University,
James GOLDMAN,
Computer and Information Technology Department Purdue University,
Rick MISLAN,
Computer and Information Technology Department Purdue University,
Timothy WEDGE,
National White Collar Crime Center,
Steve DEBROTA,
U.S. Attorney's Office – Southern Indiana

COMPUTER FORENSICS FIELD TRIAGE PROCESS MODEL

With the proliferation of digital based evidence, the need for the timely identification, analysis and interpretation of digital evidence is becoming more crucial. In many investigations critical information is required while at the scene or within a short period of time – measured in hours as opposed to days. The traditional cyber forensics approach of seizing a system(s)/media, transporting it to the lab, making a forensic image(s), and then searching the entire system for potential evidence, is no longer appropriate in some circumstances. In cases such as child abductions, pedophiles, missing or exploited persons, time is of the essence. In these types of cases, investigators dealing with the suspect or crime scene need investigative leads quickly; in some cases it is the difference between life and death for the victim(s).

The Cyber Forensic Field Triage Process Model (CFFTPM) proposes an onsite or field approach for providing the identification, analysis and interpretation of digital evidence in a short time frame, without the requirement of having to take the system(s)/media back to the lab for an in-depth examination or acquiring a complete forensic image(s). The proposed model adheres to commonly held forensic principles, and does not negate

the ability that once the initial field triage is concluded, the system(s)/storage media be transported back to a lab environment for a more thorough examination and analysis. The CFFTPM has been successfully used in various real world cases, and its investigative importance and pragmatic approach has been amply demonstrated. Furthermore, the derived evidence from these cases has not been challenged in the court proceedings where it has been introduced.

The CFFTPM is a formalization of real world investigative approaches that have distilled into a formal process model. At the heart of the model is the notion that some investigations are extremely time sensitive; hours can literally mean the difference between life and death for a victim or the escape of the suspect. Most law enforcement cases today involve digital evidence of some kind. We are truly a digital nation and as such our lives (the good and the bad) are reflected in technology and the bits and bytes. Correspondingly, digital evidence is a primary source of critical information and investigative leads that are required within the first few hours of many investigations.

While the investigative approaches that were used to develop the model came primarily from child pornography cases, the model is general enough to be used across a wide spectrum of investigations.

The six primary phases of the CFFTPM (planning, triage, usage/user profiles, chronology/timeline, email & IM, and case specific evidence) are important in such diverse cases as financial fraud, identity theft, cyber stalking and murder. The various sub-phases or tasks under each primary phase need to be modified based on the specifics of each investigation. The tasks and considerations discussed under Conference on Digital Forensics, Security and Law, 2006 each of the phases act as examples of the decision making process that needs to take place – sensitivity of time vs. quality and importance of the evidence derived.

The CFFTPM is consistent with the various theoretical models that have been developed within the field of digital forensic science. By following the CFFTPM a computer forensic examiner has not precluded a more thorough traditional examination and analysis back in the lab. The procedures used on site are forensically sound, maintain the chain of custody, and comply with Federal and State rules for the admissibility of evidence.

One of the biggest advantages of the CFFTPM (very practical and pragmatic) is due to the fact the model was developed in

reverse of most other models in the area. The investigators in the field matured their instinctive approaches based on actual trial and error, cases, court decisions and the direction from prosecutors. The CFFTPM merely aggregated these approaches and articulated them into a more formal methodology; still maintaining the investigative essence and the key components that have been battle tested.

Just as it has been said that «one software tool does not a computer examiner make», only possessing one investigative process model is equally as limiting. Computer forensic examiners need a repertoire of tools and just as important, a repertoire of examination and investigative approaches. The CFFTPM is not the ultimate solution for every case; it should only be used where appropriate and only after carefully weighing the legal and technical considerations. In those instances where it has been employed it has been extremely effective!

Одержано 10.11.2013

УДК 343.98

Валерія Олегівна МАЛЯРОВА,
кандидат юридичних наук, доцент,
професор кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ЗЛОЧИНИ ПРОТИ МОРАЛЬНОСТІ У СФЕРІ СТАТЕВИХ СТОСУНКІВ ТА ВИСОКІ ТЕХНОЛОГІЇ: ЗВ'ЯЗОК І ВЗАЄМНИЙ ВПЛИВ

Новий Кримінальний процесуальний кодекс України наголошує, що завданнями кримінального провадження є захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура [1, с. 3].

Вдосконалення чинного законодавства, потребує і правозастосовної практики в найбільш актуальних, проблемних випадках. Одним з таких пріоритетних питань є протидія злочинам проти моральності у сфері статевих стосунків, а саме: торгівлі людьми; ввезенню, виготовленню, збуту і розповсюдженню порнографічних предметів; розбещенню неповнолітніх; створенню або утриманню місць розпусти; сутенерству або втягненню особи в заняття проституцією (ст. 149, 156, 301, 302 і 303 КК України).Нерідко способи вчинення цих категорій злочинів тісно пов'язані з використанням комп'ютерних технологій і всесвітньої мережі Інтернет.

Ці злочини викликають особливу стурбованість, ще і тому, що у сучасному суспільстві має місце певна тенденція до падіння морально-духовної культури, що обумовлено низкою факторів, таких як аномія, еклектичне змішування елементів різних культур, комерціалізація значної частини суспільних благ, проникнення елементів кримінальної субкультури до масової культури тощо.

Нажаль ці негативні тенденції характерні не тільки для України, але й для світового суспільства в цілому. З кожним роком молодшає дитяча порнографія. У мережі Інтернет дедалі частіше можна знайти дитячу порнографію, у тому числі зі сценами сексуального насильства над дітьми віком від трьох до п'яти років. Перегляд таких сайтів провокує агресивну, асоціальну поведінку у людей с несформованою або порушеною психікою. І безумовно, це призводить до серйозних фізичних і моральних збитків самим дітям, негативні наслідки чого для суспільства в цілому неможливо переоцінити. При цьому переважна більшість дитячої порнопродукції розповсюджується саме через Інтернет. Торговці живим товаром використовують комп'ютерну мережу для пошуку людей, які в силу тяжких життєвих обставин, згодні на вилучення в них органів. Крім того, для вчинення торгівлі людьми злочинці за допомогою комп'ютерних технологій виготовлюють документи, що посвідчують особи тих, хто потребує незаконного перетину кордонів. Іноді ці документи бувають такі якісні, що відрізнити їх від справжніх можливо тільки експерти-криміналісти.

Віртуальна мережа надає безмежні можливості для злочинців. Українське суспільство, як частина світового суспільства, все більш залежить від світової павутини. Це сприяє росту кіберзлочинності, яка с кожним роком стає більш прибутковою та трансформується в транснаціональну злочинність.

Сьогодні є підстави вести мову про феномен звикання до злочинності, маргіналізацію значної частини населення України. Окремою проблемою постає відсутність належного контролю з боку держави та громадськості за інформаційним простором. Саме тому в Інтернеті дедалі частіше знаходить своє поширення продукція, що пропагує культ насильства та жорстокості, расової нетерпимості, порнографія. Саме розбещення потреб та падіння моральності призвело до збільшення попиту на відповідну продукцію кримінального походження: порнографію (в тому числі дитячу), проституцію; до появи нових форм рабства, до подальшого поширення транснаціональної кіберзлочинності та організованої злочинності, яка отримує надприбутки від деградації духовної сфери життєдіяльності українського суспільства та, врешті-решт, втрати національної ідентичності й високоморальної самобутності.

Ціна злочинності проти моральності принципово не може бути виміряна у грошовому еквіваленті, адже завдає непоправних збитків генофонду нації: діти та молодь – найбільш вразливі до деформаційних процесів ціннісної системи координат, зазнають як психологічної, так і фізичної шкоди. Таким чином, криміналізація та дисфункціональність сфери моральності становить суттєву загрозу національній безпеці України. Необхідною умовою функціонування України як нової держави є входження її в міжнародне співтовариство. Але це тягне за собою і появу і певних соціально-економічних, політичних, юридичних та морально-етичних проблем та зобов'язань, серед яких певне значення мають зобов'язання у зв'язку з приєднанням України до міжнародних конвенцій та інших документів, прийнятих у зв'язку з необхідністю об'єднання зусиль держав у боротьбі зі злочинами, які вчинюються за допомогою комп'ютерних мереж.

Надійнішим засобом для попередження злочинів проти моральності у сфері статевих стосунків є виховання морально і духовно здорової молоді. Надійнішим засобом для попередження злочинності в галузі високих технологій є науково-технічний прогрес, що служить протидії кіберзлочинності.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України : прийн. Верховною Радою України Законом № 4651-V1 від 13.04.2012 р. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Кримінального процесуального кодексу України» № 4651-V1 від 13.04.2012 р. – Х. : Право, 2012. – 392 с.

Одержано 14.11.2013

УДК 343.985

Світлана Олександрівна КНИЖЕНКО,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

РОЗСЛІДУВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН

На сьогодні доходи комп'ютерних злочинців за оцінками кримінологів посідають третє місце після доходів наркоділків та постачальників зброї [1, с. 51]. Вдосконалення комп'ютерних технологій призвело до появи нових видів комп'ютерних злочинів, в тому числі й до несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – ст. 361 Кримінального Кодексу України.

За своїм способом неправомірний доступ до комп'ютерної інформації має певну специфіку й характеризується високим ступенем латентності та низьким рівнем розкриття. Одним із поширених способів неправомірного доступу до комп'ютерної інформації на сьогодні є глобальна телекомунікаційна мережа Інтернет.

Відсутність у оперативних працівників, слідчих, прокурорів та суддів практичних рекомендацій з розслідування досліджуваних злочинів призводить до порушення прав потерпілих осіб й сприяє збереженню високого рівня латентності протиправних дій у цій галузі та їхньої безкарності.

У криміналістичній літературі окремі аспекти розслідування комп'ютерних злочинів розглядалися в роботах Ю. В. Гавриліна, В. А. Голубєва, А. Ю. Головіна, В. Є. Козлова, В. В. Крилова**,** В. С. Цимбалюка та інших. Водночас алгоритму початкового етапу розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин з використанням мережі Інтернет не розроблено.

На початковому етапі розслідування вказаних злочинів слідчий допускає низку криміналістичних помилок, серед яких варто назвати: несвоєчасність огляду; неповнота та формальне відношення до нього; невикористання всіх можливостей з фіксації функціонування та впливу шкідливих програм.

Вважаємо, що ефективними шляхами до розв'язання вказаних проблем необхідний цілий комплекс заходів, до

яких слід віднести: спеціалізовану додаткову теоретичну підготовку оперативних працівників, слідчих, прокурорів та суддів у сфері високих технологій; введення спеціалізації слідчих за групами злочинів; використання спеціальних знань під час кримінального провадження; посилення прокурорського нагляду за законністю розслідування злочинів у сфері комп'ютерної інформації.

Алгоритм початкового етапу розслідування досліджуваних злочинів повинен включати:

1. Допит потерпілого та можливих свідків (очевидців) злочину. Так, слідчому необхідно у потерпілого встановити, що слугувало підставою для рішення про те, що був несанкціонований доступ, розмір матеріальної шкоди, з'ясовується з яким провайдером був укладений договір.

Варто погодитися з думкою Ю. В. Гавриліна про те, що у випадку неправомірного доступу до комп'ютерної мережі необхідно допитати інженерів-програмістів, що займаються розробкою програмного забезпечення, операторів, спеціалістів з технічного забезпечення, що займаються ремонтом засобів комп'ютерної техніки, системних програмістів, інженерів із засобів зв'язку та телекомунікаційному обладнанню, спеціалістів по забезпеченню безпеки комп'ютерних систем та інше [2, с. 23].

2. Проведення огляду місця події – місць виявлення слідів злочину з обов'язковим оглядом комп'ютерного засобу. В ході огляду місця події слідчому необхідно з'ясувати характеристики комп'ютера; програмного забезпечення, що на ньому встановлене; розташування окремих елементів комп'ютерної системи, їх призначення, визначити наявність та можливість їх з'єднання з іншими комп'ютерними системами. При цьому з'ясовується розташування під'єднувальних кабелів та можливість підключення чи відключення певних пристроїв від комп'ютерної системи без доступу у приміщення, а також безпосередньо в самому приміщенні. З тим, щоб у подальшому виключити можливість оскарження в суді правильність проведеного огляду та його результатів слідчий повинен підбирати понятих, які мають певні знання в галузі комп'ютерної техніки (основних операціях, назвах комп'ютерних програм тощо).

Слід наголосити, що при використанні програм, які призначені для виявлення впроваджених й функціонуючих шкідливих програм в комп'ютерній системі в жодному випадку не можна проводити видалення шкідливих програм з машинних

носіїв. Їх задача тільки протестувати зміст машинних носіїв інформації; виявити файли та папки, в яких знаходяться шкідливі програми чи програми, які припустимо є шкідливими.

Програмні засоби, які використовуються в ході проведення слідчих дій повинні відповідати наступним вимогам: програми повинні бути сертифіковані; вони повинні бути захищеними від внесення в них несанкціонованих змін; вони не повинні змінювати настройки та конфігурацію засобів комп'ютерної техніки; не повинні змінювати зміст та якості комп'ютерної інформації (нажаль такі вимоги часто ігноруються правоохоронними органами); повинні надавати інформацію у доступному для сприйняття вигляді особою, що їх використовує та бути зручними для використання [3, с. 78].

3. Проведення комп'ютерних експертиз (програм для ЕОМ, баз даних, окремих файлів, спеціальних технічних засобів тощо).

4. Отримання необхідних документів, що свідчать про протиправність події або відображають незаконність проведення операції у сфері комп'ютерної інформації (договору на отримання послуг Інтернет тощо); отримання у провайдера протоколу роботи в мережі даного абонента за певний період часу з зазначенням дати, часу, початку сесії, тривалості роботи, грошових коштів, списаних з рахунку клієнта; журналів реєстрації користувачів; актів відомчих комісій; журналів обліку збоїв у роботі комп'ютерної мережі окремих комп'ютерів чи технічних пристроїв з ладу; файлів адміністратора мережі, в яких фіксується вся робота мережі; актів за результатами антивірусних перевірок, інші.

5. Отримання ідентифікаційних даних про власника комп'ютерного засобу, що здійснив незаконний дистанційний доступ до комп'ютерної інформації.

6. Проведення оперативно-розшукових заходів щодо встановлення осіб, які причетні до злочину.

7. Вивчення довідкової літератури, відомчих нормативних актів, положень, інструкцій.

При розслідуванні досліджуваних злочинів слідчому необхідно залучати спеціаліста в галузі електронно-обчислювальної техніки та програмного забезпечення для збору необхідної інформації; уточнення характеру та ступеню шкідливого впливу на інформацію; визначення можливого місця та способу вчинення злочину; визначення порядку

фіксації специфічних слідів, що залишились на місці події; визначення напрямку пошуку, виявлення та фіксації й вилучення слідів навколо та на самих засобах комп'ютерної техніки; оцінки належності шкідливої програми до вже відомих, характеру її дії, нанесеної шкоди; виявлення можливих заходів безпеки, що використали злочинці з метою знищення доказів тощо.

Список використаних джерел:

1. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями : [монография] / Д. Айков, К. Сейгер, У. Фонсторх ; пер. с англ. – М. : Мир, 1999. – 345 с.

2. Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации : [учеб. пособие] / Ю. В. Гаврилин. – М. : ЮИ МВД РФ, Книжный мир, 2001. – 88 с.

3. Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений : [монография] / Л. Н. Соловьев. – М. : Собрание, 2004. – 224 с.

Одержано 12.11.2013

УДК 343.1(477)

Ірина Володимирівна ЛЄШУКОВА,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ПРОБЛЕМНІ ПИТАННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Для сучасного суспільства все більше набирає актуальності проблема під назвою «кіберзлочинність» так як значущість інноваційних процесів та інформатизація набирає обертів. Ця проблема, безумовно, потребує вирішення, шляхом негайного створення системи протидії даному різновиду злочинності на державному рівні. У ряді міждержавних нормативно-правових актів визнано, що кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремих держав, а загрожує людству та міжнародному порядку.

Розглядаючи протидію злочинам у сфері використання комп'ютерних технологій, з точки зору міжнародного співробітництва, слід зрозуміти причини їх підвищеної небезпеки для світового співтовариства, що обумовлено певними

особливостями, притаманними саме цьому різновиду злочинності, а саме:

– транскордонний характер – тобто, у злочинця є можливість несанкціоновано проникнути в будь-яку комп'ютерну систему, яка з'єднана зі світовою мережею Інтернет (не зважаючи на державні кордони та відстань до неї);

– високий рівень латентності, причинами якого є: складність виявлення злочинів правоохоронними органами; небажання потерпілих повідомляти про вчинений злочин; помилкове (або умисне) «списання» наслідків протиправних посягань за рахунок апаратно-програмних проблем комп'ютерних систем;

– відсутність усталених методик розкриття та розслідування вказаних злочинів, відпрацьованих механізмів міждержавної допомоги в розслідуванні, причинами чого є їх відносна новизна;

– значний рівень залежності сучасного суспільства від інформаційних технологій, які впроваджуються майже у всі сфери життєдіяльності людини та функціонування держави (банківська, енергетична, транспортна, оборонна та інші сфери), і можуть розглядатися як потенційні об'єкти злочинних атак.

Головним кроком України на шляху до міждержавної співпраці у зазначеній сфері є ратифікація 7 вересня 2005 р. Конвенції про кіберзлочинність від 23 листопада 2001 р. [1], яка передбачає надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньодержавному, так і міжнародному рівнях, укладення домовленостей щодо дієвого міжнародного співробітництва. Відповідно до зазначеної Конвенції сторони співробітничають шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, а також внутрішньодержавного законодавства з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, збиранням доказів у електронній формі. Так, згідно ст. 35 Конвенції про кіберзлочинність та доручення Президента України від 3 грудня 2010 р. № 02/78475-01 МВС України створило у структурі Департаменту боротьби з кіберзлочинністю і торгівлею

людьми МВС України контактний пункт з реагування на кіберзлочини (далі – національний контактний пункт). На сьогодні національний контактний пункт здійснює свою діяльність у структурі Управління боротьби з кіберзлочинністю МВС України цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення.

Більшість запитів, які надсилаються та надходять каналами національного контактного пункту, стосуються отримання інформації, яка знаходиться в операторів та провайдерів телекомунікацій про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання, так як ця інформація здебільшого має суто технічний характер та є первинною інформацією при проведенні перевірки за будь-яким фактом учинення адміністративного або кримінального правопорушення.

Після набрання чинності Кримінальним процесуальним кодексом України (19 листопада 2012 р.) виконання Україною своїх міжнародних зобов'язань у частині положень Конвенції про кіберзлочинність та функціонування національного контактного пункту стало вкрай проблематичним, оскільки п. 7 ст. 162 КПК України інформацію, яка знаходиться в операторів та провайдерів телекомунікацій про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання, віднесено до речей та документів, які містять охоронювану законом таємницю [2].

Таким чином, МВС України позбавлене можливості опрацьовувати запити компетентних органів іноземних держав щодо збирання доказів у справах про кіберзлочини і встановлення місцезнаходження підозрюваних у рамках Конвенції про кіберзлочинність. Разом з тим у розділі IX «Міжнародне співробітництво під час кримінального провадження» КПК України фактично відображений механізм міжнародного співробітництва в рамках Конвенції про правову допомогу і правові відносини в цивільних, сімейних і кримінальних справах від 22 січня 1993 р. [3], при цьому не зазначено

механізму отримання інформації від операторів та провайдерів телекомунікацій за запитами міжнародних правоохоронних органів у рамках Конвенції про кіберзлочинність. У подальшому це може призвести до відмови в наданні інформації компетентними органами іноземних держав через недотримання Україною принципу взаємності, закріпленого в ст. 25 Конвенції про кіберзлочинність [1].

Крім того, на теперішній час дискусійною темою є впровадження Єдиного реєстру досудових розслідувань (далі – ЄРДР) за новим КПК України [4]. Так, відповідно до ч. 2 ст. 214 КПК України факт внесення відомостей до ЄРДР прирівнюється до рішення про початок досудового розслідування, тому ЄРДР, з одного боку – «це створена за допомогою автоматизованої системи електронна база даних», порядок формування та ведення якої регулюється наказом, а з іншого боку – це «інструмент усього слідства України». На нашу думку, проблемою у функціонуванні ЄРДР перш за все може стати незаконне втручання в його роботу ззовні, тобто так звані «хакерські атаки», тому що ні для кого не секрет, що перша «хакерська атака» на Пентагон була скоєна ще у середині 1970-х років, і це було зроблено із хуліганських мотивів, а ЄРДР – це автоматизована комп'ютерна система, яка напряму пов'язана з функціонуванням великого державного апарату. У розділі 18 Кримінального кодексу України передбачено статтю 376-1 «Незаконне втручання в роботу автоматизованої системи документообігу суду» [5], але немає спеціалізованої статті, яка б передбачала настання кримінальної відповідальності за незаконне втручання в роботу автоматизованої системи документообігу слідчих підрозділів, тобто в роботу ЄРДР. Очевидно, що у випадку незаконне втручання в роботу такої автоматизованої системи, як ЄРДР – дії злочинця будуть кваліфікуватись за відповідною статтею розділу 16 Кримінального кодексу України, але ми вважаємо, що більш доречним було б доповнити КК України спеціалізованою ст. 376-2 «Незаконне втручання в роботу автоматизованої системи документообігу слідчих підрозділів».

Підсумовуючи викладене вище, хотілося б зазначити, що хоча в наш час Україна вже стала суб'єктом міжнародної співпраці по боротьбі зі злочинами у сфері використання комп'ютерних технологій (кіберзлочинами), недосконалість внутрішньодержавної законодавчої бази не дозволяє їй

повноцінно виконувати всі взяті на себе зобов'язання. Вирішення цієї проблеми можливе лише шляхом прийняття Верховною Радою України нормативно-правових актів щодо перехоплення, збереження та подальшого використання комп'ютерних даних під час виявлення, попередження, припинення та розслідування правопорушень. Разом з тим, не слід забувати про розробку механізму реалізації таких нормативних актів із закріпленням обов'язків співробітників установ, підприємств і організацій, що будуть безпосередньо виконувати подібні дії, а також - передбачення способів відшкодування або зменшення витрат на впровадження відповідних апаратно-програмних комплексів.

Список використаних джерел:

1. Конвенція про кіберзлочинність : від 23 листоп. 2001 р. // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

2. Кримінальний процесуальний кодекс України : закон України від 13 квіт. 2012 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17.

3. Конвенція про правову допомогу і правові відносини у цивільних, сімейних і кримінальних справах : від 22 січ. 1993 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/997_009.

4. Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ Ген. прокурора України від 17 серп. 2012 р. № 69 [Електронний ресурс]. – Режим доступу: http://www.gp.gov.ua/ua/pd.html?_m=publications&_t=rec&id=110522.

5. Кримінальний кодекс України : закон України від 5 квіт. 2001 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14.

Одержано 11.11.2013

УДК 343.985

Світлана Миколаївна ЛОЗОВА,
кандидат психологічних наук,
доцент кафедри криміналістки, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ПСИХІЧНИХ ДЕВІАЦІЙ КІБЕРЗЛОЧИНЦЯ

Кількість злочинів, які вчиняються в кіберпросторі, зростає пропорційно кількості користувачів комп'ютерних мереж,

і, по оцінці фахівців Інтерполу, темпи росту злочинності в глобальній мережі Інтернет є самими швидкими на планеті. Кіберзлочинність - це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера, інформації, у якому перебувають відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [1].

Поряд з багатьма перевагами Інтернет простір має багато небезпек. В першу чергу слід вказати на неконтрольований доступ до інформації, яка впливає на психіку особи (особливо це стосується неповнолітніх), матеріали антигуманного або порнографічного характеру, ймовірність спілкування з кіберзлочинцями, з особами, які мають серйозні психічні захворювання або збочені сексуальні нахили, а також пропаганда насильства, наркотиків і багато іншого.

Особистість в кіберпросторі, що наділена уявної свободою і анонімністю відчуває в собі так званий «режим Бога», тобто ілюзорну здатність керувати різними ситуаціями. Слід відмітити, що в залежності від особливостей психіки даної особи в кіберпросторі ми можемо спостерігати як девіантну поведінку, так і безпосередньо делінквентну (кіберзлочинність).

Першою рисою особистості кіберзлочинця є ескапізм – втеча від дійсності, прагнення піти від реальності, від загальноприйнятих норм суспільного життя у світ ілюзій, або псевдодіяльності. Комп'ютерний світ, особливо разом з Інтернетом, є прекрасним альтернативним світом, в якому можливо знайти цікаве заняття, захист від небажаних соціальних контактів, реалізувати креативний потенціал і навіть заробити гроші. З іншого боку, людина, яка чимось сильно захоплена в реальному світі, навряд чи зможе знайти достатню кількість часу і сил, щоб стати хорошим фахівців в специфічних областях ІТ.

Ескапізм є фактором для виникнення комп'ютерної або мережевої залежності [2]. Така залежність (у слабкій або сильній формі) є другою рисою особистості ймовірного злочинця. Комп'ютерна залежність (адикція) може початися зі звичайного

захоплення, яке адикцією не являється. Залежність у важкій формі ближче до психічної девіації (тобто відхилення), а в ще більш тяжкій формі деякі вважають таку адикцію хворобою, яка потребує лікування. Першими з нею зіткнулися лікарі-психотерапевти, а також компанії, що використовують у своїй діяльності Інтернет і несуть збитки, у випадку, якщо у співробітників з'являється патологічний потяг до перебування он-лайн. Cyber Disorder (CD)[3] увійде в DSM-V на рівних з іншими нехімічними адикціями. Комп'ютерна або мережева адикція характеризується нездатністю людини відволіктися від роботи в Мережі, дратівливістю при вимушених відволіканнях, готовністю знехтувати цінностями (матеріальними та соціальними) реального світу заради світу віртуального, зневагою своїм здоров'ям. Дослідження показують, що люди, які страждають мережевою залежністю в той же час відрізняються високим рівнем абстрактного мислення, індивідуалізмом, інтровертністю, емоційною чутливістю і деяким ступенем нонконформізму.

Наприклад, у затриманого британською поліцією дев'ятнадцяти річного Раяна Клірі (Ryan Cleary) із відомої хакерської групи LulzSec, яка об'явила про свій розпуск [4], було діагностовано синдром Аспергера, що дозволить йому уникнути кримінального покарання. Синдром Аспергера – одне з п'яти загальних порушень розвитку, що характеризується серйозними труднощами в соціальній взаємодії, а також обмеженим, стереотипним, повторюваним репертуаром інтересів і занять, відсутністю здібностей до невербальної комунікації, обмеженою емпатією по відношенню до однолітків і фізичною незручністю.

Також деякі інтернет-шахраї керуються не тільки отриманням прибутку. Більше того, їх злочинний дохід часто буває менше, ніж середня зарплата фахівця тієї ж кваліфікації. В даному випадку мотивом для вчинення шахрайства є антисоціальна психопатія (соціопатія) таких осіб та їх патологічна тяга до ведення подібних «ігор». Соціопатія визнана окремим видом психічного розладу і зареєстрована під назвою «antisocial personality disorder» в класифікаторі хвороб ВООЗ. Зазвичай такі типи діють імпульсивно і не схильні до планування, особливо довгострокового. За неофіційною класифікацією, LulzSec відносяться до так званих «сірих» хакерів (Greyhat) – тип кіберхуліганів, які зламують сайти або

піддають їх DDoS-атаці не заради власного збагачення, а для того, щоб або вказати власникам сайту на пролом в системі безпеки, або «помститися» за ту чи іншу дію, вчинену компанією, що володіє сайтом.

Список використаних джерел:

1. Кіберзлочинність в Україні / Социальная Научная Сеть [Електронний ресурс]. – Режим доступу: http://www.science-community.org/ru/node/16132.

2. Федотов Н. Н. Форензика – компьютерная криминалистика [Електронний ресурс]. – Режим доступу: http://osipov.ua/pr/13970-forenzika-kompyuternaya-kriminalistika-nn-fedotov.html.

3. Патологічна залежність або адикція / I-MEDIC : медичні статті [Електронний ресурс]. – Режим доступу: http://i-medic.com.ua/index.php?newsid=25293.

4. Шадрин И. Уход LulzSec не улучшит ситуацию с киберпреступностью – эксперты : Сюжет: Действия хакерской группы Lulz Security / Иван Шадрин ; РИА Новости [Електронний ресурс]. – Режим доступу: http://www.digit.ru/internet/20110628/382665214.html.

Одержано 12.11.2013

УДК 343.985

Тетяна Петрівна МАТЮШКОВА,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

ОКРЕМІ ВЕРСІЇ ПРИ РОЗСЛІДУВАННІ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Версія – це обґрунтоване припущення про наявність і обставини розслідуваної події, про дії конкретних осіб і наявність у цих діях складу певного злочину. Їхня пізнавальна функція полягає у систематизації доказового матеріалу, його аналізі та обґрунтованому висуненні припущення, що визначає найбільш ефективний шлях швидкого, повного та неупередженого розслідування.

За обсягом припущень версії поділяються на загальні та окремі. Загальні версії пояснюють зміст і сутність всієї злочинної події, окремі – зміст окремих фактів. Версії висуваються для встановлення обов'язкових та допоміжних обставин, які підлягають доказуванню у кримінальному

провадженні (час, місце, спосіб вчинення злочину, особа злочинця та інші елементи предмету доказування). Перелік видів окремих версій змінюється в залежності від категорії злочину і конкретної ситуації розслідування.

На початковому етапі розслідування залежно від виду комп'ютерного злочину можуть висуватись типові окремі версії про мотиви його вчинення, особу злочинця (злочинців), місце його (їх) знаходження, ступінь підготовки, використані засоби та знаряддя, ін.

Типовими окремими версіями про мотиви вчинення комп'ютерних злочинів можуть бути наступні:

1) хуліганські;

2) корисливі;

3) приховання іншого злочину (наприклад, розкрадання коштів);

4) під впливом погрози чи примушування, матеріальної чи службової залежності від злочинця;

5) внаслідок збігу тяжких особистих чи сімейних обставин;

6) політичні;

7) дослідницький інтерес;

8) помста;

9) усунення конкурента шляхом знищення його ділової, соціальної, політичної репутації;

10) заволодіння результатами наукових досліджень;

11) отримання конфіденційної інформації тощо.

Типовими окремими версіями про особу злочинця щодо ступеня зв'язку злочинця із постраждалим будуть такі:

1) злочин вчинено внутрішнім співробітником, користувачем, клієнтом, обслуговуючим персоналом тощо;

– злочинці, які вчинюють злочини з використанням програмних засобів. До них можна віднести операторів ЕОМ, бухгалтерів, касирів, продавців, операторів периферійних устаткувань, адміністраторів баз і банків даних, бібліотек програмних засобів, операторів-програмістів (системних та прикладних), інженерів-програмістів та ін.;

– злочинці, які вчинюють злочини з використанням апаратних засобів комп'ютерної техніки. До них можна віднести операторів засобів зв'язку, інженерів термінального обладнання, спеціалістів з комп'ютерного аудиту, інженерів електронного обладнання, інженерів зв'язку тощо;

– злочинці, які вчинюють злочини з використанням опосередкованого доступу до засобів комп'ютерної техніки. До них відносяться особи, які здійснюють організаційно-управлінські функції: керуючі комп'ютерною мережею чи системою; керівники операторів; баз і банків даних; робіт з програмного забезпечення; старші (головні) інженери, програмісти, ін.; керівники і начальники різних служб и відділів (інформаційно-аналітичного і т. ін.); співробітники служб безпеки; менеджери і т. ін.;

2) злочин вчинено зовнішнім користувачем, тобто суб'єктом, який звертається до інформаційної системи чи посередника за отриманням необхідної йому інформації та використовує її. Їх коло настільки широке, що його важко систематизувати чи класифікувати, адже ним може бути будь-яка, навіть випадкова людина. Наприклад, представник організації, що здійснює сервісне обслуговування, ремонт, розробку програмних засобів комп'ютерної техніки на договірній підставі, представники різних контролюючих і владних органів чи організацій, клієнти, хакери тощо.

Типовими окремими версіями про особу злочинця щодо статусу користувача мережі Інтернет:

1) зареєстрований (санкціонований) користувач;

2) незареєстрований (несанкціонований, незаконний) користувач.

Типовими окремими версіями про особу злочинця щодо ступеня виконання злочинного наміру:

1) злочин вчинено одноосібно;

2) злочин вчинено групою осіб;

3) злочин вчинено на замовлення (наприклад, керівника фірми, організації з кола конкурентів).

Типовими окремими версіями про ступінь підготовленості злочину:

1) злочин вчинено без підготовки;

2) злочин ретельно підготовлений, вжиті заходи щодо приховання слідів.

Типовими окремими версіями про місце знаходження злочинця при підгтовці, вчиненні та приховуванні слідів компютерних злочинів:

1) в момент підготовки, вчинення та приховання злочину злоинець (та його спільники) знаходився в Україні;

2) підготовка та вчинення мали місце при знаходженні злочинця в Україні, а приховання має місце на території іншої держави, у тому числі, за сприяння інших осіб;

3) в момент підготовки, вчинення та приховання злочину правопорушник (чи його спільники) знаходився за межами України.

При розслідуванні компютерних злочнів можуть бути висунуті й інші окремі версії залежно від конкретних обставин злочину та наявної у слідчого інформації.

Одержано 14.11.2013

УДК 343.98

Тетяна Анатоліївна ПАЗИНИЧ,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ПРО ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

На сучасному етапі існують неабиякі проблеми міжнародного співробітництва правоохоронних органів України у боротьбі із кіберзлочинністю, що має транснаціональний характер. Ці проблеми обумовлені рядом факторів, серед яких можна виділити наступні:

1) набувають поширення порівняно нові категорії злочинів, які вчинюються в середовищі Інтернет мережі (кіберсередовище), наслідки від яких, незалежно від місця вчинення, можуть наступити в будь-якій країні світу;

2) на даний момент відмічається недостатній досвід практичних підрозділів ОВС у застосуванні норм нового Кримінального процесуального кодексу України, особливо розділу IX Міжнародне співробітництво під час кримінального провадження;

3) мають місце суттєві прогалини у нормативному регулюванні виконання доручень і запитів про міжнародну правову допомогу у національному законодавстві;

4) немає єдиної системи підготовки, перепідготовки кадрів – працівників ОВС, які спеціалізувались би на розслідуванні транснаціональних злочинів (в тому числі кіберзлочинів) в рамках міжнародної співпраці;

5) існуючі форми міжнародної співпраці правоохоронних органів у боротьбі із транснаціональною злочинністю мають суттєві недоліки, в зв'язку з відсутністю єдиного підходу у процедурі формування, використання доказової бази у справах про такі злочини, а також у встановленні, розшуку і притягненні винних до відповідальності.

Аналіз спеціальної літератури, обговорення можливих шляхів вирішення зазначених вище проблем на конференціях, круглих столах, в рамках робочих груп дозволяє на даний момент сформувати власні пропозиції щодо удосконалення існуючого механізму боротьби із транснаціональною кіберзлочинністю.

Вважаю доцільним, запропонувати наступне.

Необхідно розширити завдання національного контактного пункту Управління боротьби із кіберзлочинністю МВС України (далі НКП) і покласти на його працівників обов'язок реєструвати в Єдиному реєстрі досудових розслідувань відомості про кримінальні правопорушення, про які повідомляють представники правоохоронних органів інших країн (відповідно до п. 2.1 Положення Про порядок ведення Єдиного реєстру досудових розслідувань) і ініціювати початок кримінального провадження, якщо кіберзлочини мають транснаціональний характер і зачіпають інтереси нашої держави, суспільства чи окремих громадян. Адже більшість кіберзлочинів – це злочини особливої категорії, для яких не існує рамок, що обмежують територію їх вчинення і настання наслідків.

Так, злочинець (шахрай, хакер, терорист тощо) може знаходитись в одній країні світу, а наслідки від його злочинних дій наставати в інших країнах світу (в одній або декількох). Відповідно, правоохоронні органи всіх держав повинні паралельно здійснювати заходи по припиненню і попередженню таких злочинів, переслідуванню і притягненню до відповідальності винних у їх вчиненні. Раз стираються рамки місця вчинення таких злочинів – повинні стиратися рамки місця проведення розслідування. Провадження повинно відбуватися в рамках спільного розслідування таких злочинів правоохоронними органами держав.

Відповідно положень ст. 35 Конвенції Ради Європи «Про кіберзлочинність» призначенням міжнародної мережі національних контактних пунктів є швидке реагування на кіберзлочини, а призначення національного контактного пункту

Управління боротьби із кіберзлочинністю МВС України тлумачиться – як «... надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення». Але, «надання допомоги у розслідуванні кіберзлочинів» – це тільки окрема форма реагування на них, і відповідно призначення НКП не повністю відповідає міжнародним стандартам внесеним Радою Європи.

На нашу думку, саме такий вузький підхід у тлумаченні загального призначення НКП, як тільки «надання допомоги», створює проблеми і труднощі в тому, щоб міжнародна співпраця з боку правоохоронних органів України була рівнозначною, саме тому порушується принцип взаємності, проголошений ст. 25 Конвенції РЄ «Про кіберзлочинність».

Вважаємо за необхідне, запропонувати інше розуміння призначення НКП, саме як швидке реагування на кіберзлочини. Реагування НКП повинно включати декілька форм:

– реєстрація відомостей про транснаціональні кіберзлочини (якщо є данні, що вказують про вчинення дій об'єктивної сторони громадянином України, на території України, або суспільно-небезпечні наслідки настали або загрожують інтересам України та її громадян) і забезпечення початку кримінального провадження в Україні по кожному такому факту;

– організація припинення кіберзлочину, попередження настання шкідливих наслідків, тощо (наприклад, при виявленні в мережі Інтернет дій осіб хворих на педофілію або осіб, що пропагують ворожнечу, настрої ксенофобії, заклики до розв'язання війни, тощо);

– надання допомоги у розслідуванні кіберзлочинів (якщо вони не несли загрозу інтересам України) за запитами правоохоронних органів іноземних держав в рамках надання оперативної або довідкової інформації, яка не відноситься до охоронюваної законом таємниці;

– проведення організаційних заходів (наприклад, вручення документів і підписання їх фізичними особами, повернення викраденого майна та незаконно придбаних предметів чи цінностей).

Мається на увазі, що ті запити правоохоронних органів іноземних держав, в яких містяться повідомлення про вчинення

злочинів, які представляють суспільну небезпеку для України і її громадян, повинні сприйматися НКП, як повідомлення про кримінальне правопорушення. Такі повідомлення повинні реєструватися і направлятися для проведення повноцінного провадження досудового слідства згідно кримінального процесуального законодавства України.

Впровадження такого порядку реагування на транснаціональні злочини правоохоронними органами України вирішить декілька внутрішніх проблем.

По-перше, слідчі, які будуть проводити комплекс необхідних слідчих (розшукових) дій, будуть не виконувати «позапланові, безпоказникові» завдання (що зараз має місце на практиці при виконанні запитів), а будуть здійснювати повноцінне провадження у таких справах. Відповідно, вони будуть мати повний спектр процесуальних повноважень, будуть зацікавленні у якості проведенні розслідування, будуть мати змогу налагоджувати особисті зв'язки у співпраці з представниками правоохоронних органів інших держав.

По-друге, слідчі ОВС будуть постійно піднімати рівень кваліфікації у розслідуванні транснаціональних злочинів в рамках міжнародного співробітництва, а не «топтатися на місці», намагаючись вирішити внутрішні проблеми співвідношення національного кримінального процесуального законодавства, міжнародного і законодавства кожної країни учасниці, що ратифікували Конвенцію РЄ «Про кіберзлочинність». Адже на даний момент дуже не вистачає нашим слідчим досвіду і кваліфікації у розслідуванні злочинів зазначеної категорії, а виконання окремих доручень по запитах про правову допомогу не дає змогу набувати їх.

По-третє, Україна буде сприйматися світовою спільнотою як повноцінний партнер у боротьбі з кіберзлочинністю, а не як «помічник» у цій справі, до речі не зовсім вдалий, виходячи із звіту і зазначених у ньому проблем.

Ті ж запити правоохоронних органів іноземних держав, в яких міститься прохання надати правову допомогу у справах про злочини, які не представляють суспільну небезпеку для України і її громадян, повинні сприйматися НКП як запити про правову допомогу. Саме по таких запитах завданням НКП є організація проведення окремих слідчих дій (направлених на встановлення окремих обставин злочину), організаційних заходів, надання довідкової інформації, тощо.

Одержано 15.11.2013

УДК 343.985

Михайло Григорович ЩЕРБАКОВСЬКИЙ,
кандидат юридичних наук, доцент,
доцент кафедри кримінально-правових дисциплін
факультету права та масових комунікацій
Харківського національного університету внутрішніх справ,
Микола Глібович ЧЕРНЕЦЬ,
кандидат юридичних наук, доцент,
викладач кафедри кримінально-правових дисциплін
факультету права та масових комунікацій
Харківського національного університету внутрішніх справ

СЛІДЧИЙ ЕКСПЕРИМЕНТ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Кіберзлочини (злочини, що вчинюються із використанням комп'ютерних технологій) відрізняються як механізмом скоєння, що обумовлено використанням високотехнологічних засобів, комп'ютерних програм, розмежуванням місця знаходження злочинця й місцем настання шкідливих наслідків, так й складністю їх розслідування. Аналіз криміналістичної літератури показує, що при розробці методик розслідування кіберзлочинів основну увагу науковці приділяють розгляду способів вчинення злочинів та їх слідів, першочерговим слідчим діям (огляду місця події та комп'ютерних засобів, обшуку, допиту підозрюваних), залученню спеціалістів до участі в слідчих діях, призначенню комп'ютерно-технічної експертизи. Як правило, поза увагою дослідників залишаються слідчі (розшукові) дії наступного етапу розслідування, до яких відноситься слідчий експеримент.

У ст. 240 КПК України зазначено, що з метою перевірки і уточнення відомостей, які мають значення для встановлення обставин кримінального правопорушення, слідчий, прокурор має право провести слідчий експеримент шляхом відтворення дій, обстановки. У криміналістичному аспекті експеримент використовується для встановлення сутності досліджуваних (пізнаваних) явищ, пов'язаних із розслідуванням кримінальних правопорушень. За сутністю і завданнями проведення слідчий експеримент може становити два різних види дій, що мають назву однієї слідчої (розшукової) дії, але відрізняються за приводами, підготовкою, тактичними прийомами проведення та правилами, порушення яких може викривити отримані результати і вплинути на їх оцінку слідчим,

прокурором, судом. Такими діями є проведення власне експерименту та перевірка в його межах раніше наданих показань особи в місці, про яке йде мова у цих показаннях. Проведення експерименту і перевірка показань на місці належать до групи перевірочних слідчих (розшукових) дій, призначених для перевірки фактичних даних, встановлених під час кримінального провадження.

На нашу думку, при розслідуванні кіберзлочинів власно слідчий експеримент проводиться для досягнення наступних цілей:

1) перевірка наявності у конкретної особи спеціальних знань та професійних навиків (перевірка можливості роботи з певними комп'ютерними засобами, програмами, здатність підключитися до певної комп'ютерної техніки або мережі, можливість подолання захисту й отримання безпосереднього доступу до комп'ютерної інформації та ін.);

2) перевірка можливості вчинення конкретною особою певних дій за певних просторово-часових умов (встановлення проміжку часу, необхідного на вимкнення технічних засобів захисту інформації, підключення до комп'ютерної мережі та здійснення певних дій тощо);

3) з'ясування можливості існування конкретного явища, процесу, факту за відповідних умов (перевірка можливості електромагнітного перехоплення; встановлення проміжку часу, необхідного для модифікації чи копіювання комп'ютерної інформації, перевірка можливості здійснення певних операцій за певний проміжок часу з допомогою конкретної комп'ютерної техніки та ін.).

З наведеного випливає, що експериментальні процедури можуть проводиться як з особою, чиї показання були раніше отримані при допиті, так й без неї. В останньому випадку всі дії з комп'ютерною технікою виконує спеціаліст. При цьому професійні навики особи, яка здійснює експеримент, повинні відповідати професійним навичкам безпосереднього учасника досліджуваної події.

Цілі перевірки показань особи на місці, про яке раніше надані свідчення, при розслідуванні кіберзлочинів, на наш погляд, не відрізняються якимось особливостями. Перевірка спрямована на співставлення дій особи із фактичною обстановкою, в якій вона діяла.

Конкретна тактика слідчого експерименту, застосування під час його проведення тактичних прийомів, комбінацій, дотримання тактичних рекомендацій тощо зумовлюється наявністю у слідчого, прокурора доказів на час проведення цієї слідчої (розшукової) дії, позицією, яку займають учасники кримінального провадження, слідчою ситуацією, що склалася на певному етапі досудового розслідування. Тактичні рекомендації щодо проведення слідчого експерименту конкретизуються залежно від його мети, обставин та способу вчинення кіберзлочину, особливостей особи, яка перевіряється і т. д.

Загальновідомими є основні тактичні прийоми проведення експериментальних дій: умови слідчої дії мають бути максимально наближені до умов реального перебігу досліджуваної події. При розслідуванні кіберзлочинів такими умовами є використання комп'ютерної техніки з характеристиками і станом програмного забезпечення, загальною конфігурацією комп'ютерної системи, програмно і технічно сумісного периферійного обладнання, тих же версій програмного забезпечення і т. п., як та, за допомогою якої вчинений кіберзлочин. У той же час, погодні умови, відстань між комп'ютерними засобами впливають лише на результати експериментів щодо перевірки можливості здійснення перехоплення інформації. Задля унеможливлення випадковості в результатах дослідних дій, їх треба проводити декілька разів, а особливо складні, тривалі за часом досліди повинні проводитись кількома етапами тощо. Слідчий експеримент не завжди пов'язаний з місцем події, а може бути проведений в іншому і навіть у службовому кабінеті слідчого, прокурора, де встановлено необхідне технічне обладнання. Вважаємо, що при проведенні таких експериментів обов'язковою є участь спеціаліста в області комп'ютерних технологій. Для фіксації дій та свідчень за допомогою відео зйомки доцільно залучати іншого спеціаліста.

Власно слідчий експеримент та перевірка показань раніше допитаної особи, маючи низку спільних рис, за своєю сутністю, порядком підготовки й проведення істотно відрізняються між собою. Перевірка показань завжди передбачає прибуття слідчого, прокурора з раніше допитаною особою на місце, про яке вона повідомила у своїх показання. А слідчий експеримент, як вказано вище, може бути проведений як безпосередньо на тому ж самому місці, де відбувалася

досліджувана подія, так і в іншому, якщо фактична навколишня обстановка не має суттєвого значення для з'ясування характеру й особливостей досліджуваного явища. При перевірці на місці, показ має супроводжуватися детальною розповіддю і демонстрацією дій. Суб'єкт перевірки повинен звертати увагу слідчого й учасників слідчої дії на ті чи інші предмети обстановки, про які він говорив на допиті. Слідчий може поставити йому запитання для уточнення, а також запропонувати продемонструвати певні дії. Неможна забувати, що проведення на місці необхідних пошукових дій може сприяти виявленню нових матеріальних слідів злочину – предметів (наприклад, магнітні, оптичні накопичувачі інформації тощо), документів, прихованих або залишених на місці під час підготовки або вчинення злочину.

Одержано 14.11.2013

УДК 343.122

Анастасія Володимирівна ДАНИЛЕНКО,
кандидат юридичних наук,
доцент кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ,
Олександра Олександрівна КОЧУРА,
старший викладач кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ЕЛЕКТРОННИЙ ДОКУМЕНТ ЯК ДЖЕРЕЛО ДОКАЗОВОЇ ІНФОРМАЦІЇ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Будь-яка діяльність людини передбачає прийняття певних раціональних та логічних рішень, які спрямовують її. Не є виключенням в даному випадку кримінальний процес, де діяльність спеціально уповноважених суб'єктів по розслідуванню та розгляду матеріалів кримінального провадження спрямовується певними рішеннями. Дані рішення можуть бути усними, наприклад, рішення слідчого про необхідність проведення допиту свідка, а можуть бути і письмовими, тобто оформлюватись складанням певних процесуальних документів.

Немає жодної сфери суспільного життя де б не використовувались документи, а тому вимоги, що ставляться до їх

зовнішньої форми та змісту суттєво різняться. Зазначене обумовлює відсутність однозначного визначення поняття документа. Даний термін має латинське походження і в перекладі слово «documentum» означає повчальний приклад, свідчення, доказ [1, с. 276]. В українській мові термін «документ» тлумачиться як: 1) діловий папір, що посвідчує певний юридичний факт, підтверджує право на що-небудь, служить доказом чого-небудь; 2) те, що підтверджує що-небудь [2, с. 314]. Аналогічно названий термін інтерпретується і в російській мові [3, с. 121]. Дещо ширший зміст у поняття документ вкладається у сфері діловодства, зокрема А. Б. Фельзер розуміє під ним матеріальний об'єкт з інформацією, закріпленою створеним людиною способом для її передачі у часі і в просторі [4, с. 9]. Щодо юридичної науки, то в даній сфері під документом розуміють «матеріальну форму відображення, поширення, використання і зберігання інформації, яка надає їй юридичної сили» [1, с. 276].

Документи також відрізняються між собою матеріалами та формами закріплення і відображення у них інформації. В. Я. Дорохов відзначає, що документ може бути виготовлений на папері, тканині, фотоплівці, кінострічці, магнітній стрічці, за допомогою літер, телеграфних та топографічних знаків, креслень, цифр, малюнків, зображень, а також іншими способами, що забезпечують однозначне розуміння змісту документа тим колом осіб, для якого він призначений [5]. Крім того на сучасному етапі розвитку суспільства правомірно говорити про те, що зазначений перелік матеріалів документів може бути значно розширений за рахунок електронних документів, тобто документів, інформація в яких зафіксована у вигляді електронних даних, включаючи обов'язкові реквізитидокумента [6]. Разом з тим, слід відзначити, що з розширенням можливості використання електронних систем та баз даних, для зберігання інформації у кримінальному провадженні, електронні документи набувають особливого значення. А тому положення ст. 8 Закону України «Про електронні документи та електронний документообіг» про те, що юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму і допустимість електронного документа як доказу не може заперечуватися виключно на підставі того,що він має електронну форму також має важливе значення у процесуальному доказуванні.

Електронний документ є новим джерелом доказової інформації у сучасному інформаційному суспільстві, який характеризується рядом ознак.

Перша група ознак електронного документи – це загальні ознаки:

– матеріальна форма;

– юридична сила;

– наявність реквізитів, визначених законодавством або державними стандартами;

– копії документа, автентичні оригіналу. За вимогою сторін підлягають нотаріальному посвідченню цифровим підписом нотаріуса.

Друга група ознак – це спеціальні ознаки. до яких належать:

– зміст електронного документа має електронну форму фіксації інформації за допомогою комп'ютерних засобів;

– створення документа відбувається у спеціальному електронному середовищі програмного забезпечення, поза якою документ не існує;

– електронному документу і документообігу притаманні риси динамічності електронно-цифрових процесів обробки, кодування інформації комп'ютерними засобами в електронному середовищі перебування;

– електронному документу і документообігу притаманна риса збереження, відображення, перекодування форми представлення та трансляції по комп'ютерних мережах;

– зміст, форма та вид електронного документа органами чуття людини не сприймаються, але його алгоритмічні програми можна дослідити, проаналізувати[7, с. 241].

Список використаних джерел:

1. Юридична енциклопедія : в. 6 т. Т. 2 : Д-Й / [редкол.: Ю. С. Шемшученко (голова редкол.) та ін.]. – К. : Укр. енцикл., 1999. – 744 с.

2. Великий тлумачний словник сучасної української мови [(з дод., допов. та CD) / [уклад. і гол. ред. В. Т. Бусел.]. – К. ; Ірпінь : Перун, 2009. – 1736 с.

3. Ожегов С. И. Словарь русского языка : ок. 53 000 слов / С. И. Ожегов ; под. общ. ред. проф. Л. И. Скворцова. – 24-е изд., испр. – М. : Оникс ; Мир и образование, 2007. – 640 с.

4. Фельзер А. Б. Делопроизводство : справ. пособие / А. Б. Фельзер, М. А. Миссерман. – 3-е изд. стер. – Киев :Изд-во «Вища школа», 1988. – 319 с.

5. Дорохов В. Я. Понятие документа в советском праве [Електронний ресурс] / В. Я. Дорохов // Известия вузов. Правоведение. – 1982. – № 2. – С. 53–60. – Режим доступу: http://www.law.edu.ru/magazine/article.asp?magID=5&magNum=2&magYear=1982&articleID=186661.

6. Про електронні документи та електронний документообіг : закон України від 22 трав. 2003 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/851-15.

7. Потомська Н. А. Визначення електронного документа як доказу у кримінальному процесі України / Н. А. Потомська, М. Є. Дирдін, Н. В. Лісова // Науковий вісник Національного університету державної податкової служби України. – 2011. – № 3 (54). – С. 238–243.

Одержано 19.11.2013

УДК 343.98:004

Юлия Александровна ЛАНЦЕДОВА,
кандидат юридических наук,
доцент кафедры гражданского и уголовного права и процесса
Черноморского государственного университета

НОВАЯ ДОКТРИНА РАБОТЫ С ИСТОЧНИКАМИ АНТИКРИМИНАЛЬНЫХ КИБЕРСВЕДЕНИЙ

Эффективному, рациональному и качественному противодействию киберпреступлениям способствует новая доктрина работы с личностными и вещественными источниками доказательств и иных видов антикриминальных сведений, в том числе и об обстоятельствах преступлений, связанных с применением компьютеров, которую можно представить следующим образом:

1. Выяснение сущности, последовательности и иных закономерностей работы с личностными и вещественными источниками антикриминальных сведений.

2. Взаимосвязанное версирование [выдвижение (построение), анализ, динамическое развитие и проверка версий], планирование и организация этой работы с указанными источниками.

3.1. Установление личностного источника:

3.1.1. Поиск (предположительное установление среди лиц, тех из них, которые могут стать личностным источником в контексте преодоления конкретного правонарушения).

3.1.2. Выявление:

3.1.2.1. Констатация аутентичности (установление наличия у предполагаемого личностного источника его трех базисных свойств).

3.1.2.2. Индивидуализация (установление анкетных данных личностного источника).

3.1.3. Розыск (установление места нахождения личностного источника с известными анкетными данными).

3.1.4. Встреча (любое практическое действие антидиктолога или личностного источника, которое может обеспечить в процессе общения или негласного контакта с личностным источником получение от него антикриминальных сведений).

3.2. Собирание вещественных источников:

3.2.1. Поиск (предположительное установление среди существующих материальных объектов, тех из них, которые могут стать вещественным источником).

3.2.2. Выявление:

3.2.2.1. Констатация аутентичности (установление признаков материального объекта, по которым можно сделать вывод о наличии субстанции или трассы, в последнем случае – какой именно трассы: отпечатка, диагностического отображения, ситуационного отображения).

3.2.2.2. Индивидуализация (установление тех признаков внешнего строения материального объекта, по которым его можно будет распознать среди иных материальных объектов).

3.2.3. Розыск (установление места нахождения вещественного источника с известными индивидуальными признаками).

3.2.4. Принятие (фактический переход вещественного источника через выемку из владения физического или юридического лица к антидиктологу).

3.2.5. Закрепление (применение таких физических и иных средств, которые должны полностью исключить или хотя бы предельно возможно минимизировать дальнейшую порчу или иное неконтролируемое и нежелательное изменение вещественного источника).

3.2.6. Изъятие (применение таких технических средств и манипуляций с вещественным источником, которые позволяют его перенести на любой иной носитель, в т. ч. в упаковку; о способе изъятия недвижимых и громоздких трассосубстанций).

3.2.7. Упаковка (применение таких технических средств и методов, которые позволяют искусственно индивидуализировать трассосубстанцию, исключить неконтролируемое проникновение к ней иных лиц, исключить или максимально минимизировать порчу и иное нежелательное и неконтролируемое изменение трассосубстанции).

3.2.8. Хранение (применение таких технических средств и создание таких условий, которые должны исключить или максимально минимизировать порчу и неконтролируемое и нежелательное изменение трассосубстанции).

3.2.9. Транспортировка (применение таких технических средств, которые позволяют безопасно и контролируемо перемещать трассосубстанцию из одного места в иное).

3.2.10. Истребование справок (истребование от юридических и не исключено и физических лиц любых справочных сведений) и/или получение от физических либо юридических лиц иных документов и трассосубстанций.

3.2.11. Получение образцов трассосубстанции для сравнительного исследования.

4. Получение антикриминальных сведений о факте в целом либо об его отдельной стороне от личностного источника либо посредством личного или экспертного исследования трассосубстанции либо изучения собственно документа проведением де-факто процессуальных или парапроцессуальных действий либо ордистических мероприятий или их комбинации.

5. Оценка антикриминальных сведений (определение через аналитическую деятельность или проведением при необходимости практических действий значимости, законности, допустимости и доброкачественности этих сведений, их согласованности и достаточности в совокупности с другими сведениями для принятия решения по противодействию общественно опасному деянию).

6. Использование антикриминальных сведений:

6.1. Выбор доказательственных фактов, т. е. фактов, подлежащих доказыванию в контексте принятия промежуточного или окончательного процессуального либо иного решения.

6.2. Группирование доказательств и других видов антикриминальных сведений в контексте обоснования определенного

промежуточного или окончательного процессуального либо иного решения.

6.3. Оперирование антикриминальными сведениями при обосновании или опровержении обстоятельств базового, специального или частного предмета доказывания и выделенных доказательственных фактов как цепочки тезисов данного доказывания.

6.4. Принятие промежуточного, окончательного процессуального, иного антиделиктного решения.

7. Документирование версирования, планирования, организации и обстоятельств установления личностных или собирания вещественных источников, процедуры получения от них антикриминальных сведений, их представления, оценки и использования в антикриминальном доказывании.

Одержано 14.11.2013

УДК 343.98

Влада Олександрівна ГУСЄВА,
кандидат юридичних наук,
доцент кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ,
Людмила Володимирівна ПАРХОМЕНКО,
слухач магістратури
Харківського національного університету внутрішніх справ

ЩОДО МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

На сьогоднішній день пропорційно розширенню Інтернету зростає кількість, так званих кіберзлочинів: спам, торгівля людьми, порнографія, електронні розкрадання стали невід'ємною рисою сучасних інформаційних процесів. Як свідчить правоохоронна практика, останніми роками у світі спостерігається значне зростання рівня злочинних актів щодо інформаційних систем, що утворює загрозу окремим організаціям, установам і фізичним особам, а також економіці кожної країни та суспільства в цілому.

Беручи до уваги той факт, що з кожним днем кіберзлочинність зростає та розповсюджується і жодна держава сьо-

годні вже не спроможна самостійно протистояти цій небезпеці з'являється необхідність активізації міжнародного співробітництва у цій сфері.

Крім того, актуальність дослідженого питання полягає в тому, що за механізмом і способами здійснення злочини у сфері інформаційних технологій є специфічними і мають високий рівень латентності. Так, за отриманими даними по кіберзлочинам, від 85 % до 97 % кримінальних посягань не виявляється. За оцінками інших експертів, латентність кіберзлочинів в США сягає 80 %, Великобританії – до 85 %, ФРН – 75 %, Росії та Україні – більше 90 %.

Згідно з працею В. В. Зимовець та Д. Е. Чувиріна, специфікою кіберзлочинів є географія їх скоєння, яка є досить широкою, але, враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає значна частка правопорушень.

Важливим кроком України на шляху до міждержавної співпраці у зазначеній сфері є ратифікація 7 вересня 2005 року Конвенції про кіберзлочинність від 23 листопада 2001 року, яка передбачає надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньодержавному, так і міжнародному рівнях, укладення домовленостей щодо дієвого міжнародного співробітництва.

Відповідно положень зазначеної Конвенції сторони працюють шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, а також внутрішньодержавного законодавства з метою розслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, збиранням доказів у електронній формі.

Зокрема, Конвенцією про кіберзлочинність передбачено конкретні принципи міжнародного співробітництва, а саме: термінове збереження комп'ютерних даних, термінове розкриття збережених даних про рух інформації, взаємна допомога щодо доступу до комп'ютерних даних, які зберігаються, транскордонний доступ до комп'ютерних даних, які зберігаються (за згодою або у випадку, коли вони є публічно доступними), взаємна допомога у збиранні даних про рух інформації

у реальному масштабі часу, взаємна допомога у перехопленні даних (змісту інформації).

Ратифікація даної Конвенції є дуже суттєвим кроком України на шляху протидії злочинам у сфері використання комп'ютерних технологій. Вона полягає у тому, що правоохоронні органи України зможуть отримувати необхідні данні за відкритими кримінальними провадженнями з закордону та за необхідністю передавати у зворотному порядку. Саме на даному етапі виникає проблема, яка полягає у тому, що правоохоронним органам країни-партнера знадобиться термінове збереження інформації, яка раніше передавалася комп'ютерними мережами, або розкриття раніше збереженої інформації, існує велика ймовірність того, що такий запит залишиться невиконаним. Проблема полягає в тому, що якщо в багатьох закордонних країнах інтернет-провайдери зобов'язані деякий час зберігати дані про трафік користувачів, а також певний обсяг трафіку, то в Україні таких норм не існує. Отже, фірми, що надають послуги доступу до світової мережі, самостійно визначають термін та обсяг зберігання вказаних даних. Йдеться не тільки про відсутність нормативно правової бази, що можна було б частково виправити певними домовленостями між правоохоронними органами та організаціями-провайдерами, але й про те, що таке термінове збереження вимагає значних фінансових витрат. Для зберігання інтернет-трафіку за місяць кожен провайдер має додатково встановити серверні станції, які здатні накопичувати десятки террабайт даних і найняти осіб, які будуть цим займатися. Звичайно, жоден інтернет-провайдер добровільно не піде на такі «незаплановані» витрати заради допомоги державним структурам.

Проте, деяких рубежів на шляху становлення українського законодавства щодо норм, закріплених у Конвенції про кіберзлочинність вдалося досягнути.

Зокрема, в останні декілька років Верховною Радою України прийнято закони України:

– «Про внесення змін до Закону України «Про платіжні системи та переказ грошей в Україні» від 6 жовтня 2004 року;

– «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» (щодо відповідальності за комп'ютерні злочини) від 23 грудня 2004 року;

– «Про внесення змін до Закону України «Про захист інформації в автоматизованих системах» від 31 травня 2005 року.

Отже, незважаючи на те, що України вже стала суб'єктом міжнародної співпраці в боротьбі з кіберзлочинами, але недосконаліть внутрішньодержавної законодавчої бази не дозволяє їй повноцінно виконувати всі взяті на себе зобов'язання, що вимагає законодавчого врегулювання спрямованого на усунення даного недоліку.

Одержано 14.11.2013

УДК 343.98

Костянтин Борисович ЛЕЩУК,
кандидат юридичних наук,
доцент кафедри цивільно-правових дисциплін
та правових основ підприємницької діяльності
Харківського економіко-правового університету

ОСОБЛИВОСТІ СПОСОБІВ ВЧИНЕННЯ ЗЛОЧИНІВ У СФЕРІ ОБІГУ ЦІННИХ ПАПЕРІВ З ВИКОРИСТАННЯМ МЕРЕЖІ ІНТЕРНЕТ І СПЕЦІАЛЬНО СТВОРЕНИХ КОМП'ЮТЕРНИХ ПРОГРАМ

Сьогодні комп'ютерні та телекомунікаційні технології охоплюють практично всі сфери життя суспільства. Не передбачаючи можливостей для зловживання, суспільство поставило ці технології собі на службу, що породило новий вид злочинності – комп'ютерної злочинності.

Проблема кіберзлочинності вже давно перейшла в світові масштаби. Віртуальна економіка займає все більшу частину реального сектору економіки, майже кожен суб'єкт економічної діяльності ЄОМ, спеціальні комп'ютерні програми, та мережу Інтернет (Internet) в своїй діяльності.

Разом з цим вже неможливо уявити вчинення економічних злочинів без використання ЄОМ, спеціальних комп'ютерних програм, та мережі Інтернет (Internet), в тій чи іншій мірі.

Особливості вчинення злочинів на ринку цінних паперів полягають у створенні спеціальних комп'ютерних програм, за допомогою яких злочинці проникають у бази даних реєстраційних і депозитарних компаній і змінюють інформацію, що зберігається там [1]. Зокрема, вони вносять зміни в реєстр

власників цінних паперів, вказуючи серед них прізвища членів організованої злочинної групи чи назву (ім'я) юридичної особи. Після цього новоявлені «власники» звертаються до компанії офіційно, проводять переоформлення незаконно приписаних цінних паперів на користь третіх осіб (продають), а гроші привласнюють.

Звичайно, даний спосіб включає в себе досить об'ємну попередню роботу, яка включає у себе наступні складові елементи:

– збирання максимальної кількості інформації про депозитарні або реєстраційні компанії (їх бази даних, комп'ютерні мережі, програмне забезпечення тощо);

– створення спеціального програмного забезпечення, яке б дозволяло отримати несанкціонований доступ до бази даних цих компаній;

– обрання місця і часу проникнення в бази даних тієї чи іншої депозитарної або реєстраційної компанії;

– реєстрація фіктивної фірми, на банківський рахунок якої планується перевести одержані від продажу цінних паперів грошові кошти;

– проведення за допомогою шкідливої комп'ютерної програми фіктивного списання цінних паперів з певної групи рахунків депозитарної або реєстраційної компанії на фіктивно створений рахунок;

– легальний переказ з фіктивно створеного рахунку «власником» або його довіреною особою цінних паперів новому набувачеві (можливо добросовісному);

– відновлення попереднього стану реєстру і знищення слідів впливу стороннього програмного забезпечення.

Наведений спосіб злочинів з використанням цінних паперів може розглядатися як важливий, елемент криміналістичної характеристики злочинів, вчинених у сфері застосування сучасних інформаційних технологій [2].

Також злочинці можуть використовувати для вчинення шахрайства мережу Інтернет (Internet), створюючи сайти, що пропонують українським інвесторам можливість торгівлі акціями іноземних емітентів. При цьому предметом злочинного заволодіння може виступати й комп'ютерна інформація [3]. Постійно створюються віртуальні біржі, цінні папери на яких є теж віртуальними, ці біржі будуються за принципом

«фінансової піраміди». При цьому анонімність, що надає своїм користувачам мережа Інтернет, можливість охоплення великої аудиторії, висока швидкість і набагато більш низька вартість поширення інформації у порівнянні з традиційними засобами, робить Інтернет найбільш зручним інструментом для шахрайських дій. Унікальність мережі Інтернет полягає в тому, що практично у всіх сегментах цієї мережі відсутнє державне регулювання, цензура й інші форми контролю за інформацією, що циркулює в Інтернет.

Для такого способу злочинної діяльності характерним є вчинення шахрайства (ст. 190 КК України,) як основного злочину поєднаного з такими злочинами: злочинами у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж (ст. 361–363-1 КК України); фіктивним підприємництвом (ст. 205 КК України); легалізацією доходів, одержаних злочинним шляхом (ст. 209 КК України); підробленням документів, печаток, штампів та бланків, їх збут, використання підроблених документів (ст. 358 КК України) та іншими підпорядкованими злочинами.

Останнім часом злочинці широко використовують інформаційний простір Інтернет, для поширення недостовірної інсайдерської інформації, яка істотно впливає на ціну акцій компанії-жертви, та наступним заволодінням ними, шляхом придбання по заниженій ціні. Різновидом даної групи способів є блокування роботи сайтів компанії-жертви, та умисна зміна інформації опублікованої на сайті компанії-жертви з ціллю дестабілізувати економічну діяльність, для наступного заволодіння даною компанією. Інформаційна війна майже завжди є одним з основних етапів рейдерських атак. Експерти комп'ютерних антивірусних лабораторій відмічають тісний зв'язок зі спадами, паніками на фондовому ринку, та збільшенням кібератак [4].

З вищенаведеного можна зробити висновки, що способи вчинення злочинів в сфері обігу цінних паперів постійно удосконалюються, та все більше вчиняються з обов'язковим використанням ЄОМ, спеціальних комп'ютерних програм, та мережі Інтернет (Internet).

Список використаних джерел:

1. Смаглюк О. Шахрайство, вчинене шляхом незаконних операцій з використанням обчислювальної техніки // Підприємство, господарство та право. – 2002. – № 6. – С. 82–86.

2. Поливанюк В.Д. Криміналістична характеристика злочинів, вчинених у банківській системі з використанням сучасних інформаційних технологій [Електронний ресурс] / В. Д. Поливанюк // Режим доступу: http://www.crime-research.iatp.org.ua/library/Polivan3.htm.

3. Кузнецов В. Комп'ютерна інформація як предмет крадіжки / В. Кузнецов // Право України. – 1999. – № 7. – С. 85–88.

4. Спад на фондовом рынке и экономическая киберпреступность [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/362521.php.

Одержано 15.11.2013

УДК 343.98

Оксана Василівна ПЧЕЛІНА,
кандидат юридичних наук,
доцент кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ОГЛЯДУ ЕЛЕКТРОННОГО ДОКУМЕНТА

На різних стадіях вчинення значної кількості злочинів – їх підготовки, безпосереднього скоєння та приховування, – використовується різного роду документація. Не є виключенням і злочини в сфері службової діяльності. Тому вважаємо актуальним висвітлити особливості огляду працівниками правоохоронних органів такого різновиду документів, як електронних.

У відповідності до ст. 5 Закону України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. При цьому обов'язковими реквізитами електронного документа є такі обов'язкові дані в цьому документі, без яких він не може бути підставою для його обліку та не матиме юридичної сили. Реквізити електронного документа повинні розміщуватись відповідно до чинних нормативних документів і стандартів. До обов'язкових реквізитів електронного документа відносяться найменування установи-автора документа; місцезнаходження установи-автора документа або поштова адреса; назва виду документа (крім листів); дата виготовлення документа; дата; реєстраційний

індекс документа; заголовок до тексту; текст; електронний цифровий підпис (код особи, яка виготовила чи затвердила документ). Під час підготовки й оформлення електронних документів можуть також застосовуватись й інші, не обов'язкові, реквізити, якщо це відповідає призначенню документа чи способу його опрацювання.

Тому слідчий під час огляду електронного документа повинен зафіксувати наявність, зміст і розміщення всіх реквізитів електронного документа. Особливу увагу слід звернути на кількість оригіналів електронного документа та його копій. Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним цифровим підписом автора. У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний із електронних примірників вважається оригіналом електронного документа. Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ і документ на папері, кожен із документів є оригіналом і має однакову юридичну силу. При цьому варто звірити відповідність їх змісту та форми одне одному. Досліджуючи документ на папері, слідчий перевіряє наявність відмітки про наявність документа в електронній формі. Остання містить повне ім'я файлу і його місце зберігання, код оператора та інші пошукові дані. Її ставлять у центрі нижнього краю лицьового боку першого аркуша документа.

Важливим питанням, що підлягає з'ясуванню під час огляду електронного документа, є встановлення часу його складання (створення) та/чи його наявності на певний момент часу. З цією метою слід зафіксувати наявність приєднаної до електронного документа (електронних даних) або логічно поєднаної з ним позначки часу. Остання формується за допомогою особистого ключа центру сертифікації. Час, який використовується в позначці часу, встановлюється акредитованим центром сертифікації ключів і центром сертифікації ключів за київським часом на момент її формування та синхронізований із Всесвітнім координованим часом з точністю до однієї секунди.

Електронний документ перевіряється на зараження його вірусом, на цілісність і справжність усіх накладених на нього

електронних цифрових підписів, включаючи ті, що накладені (проставлені) згідно із законодавством як аналоги печатки. Також перевіряється наявність супровідної документації – заповненої реєстраційно-контрольної картки в електронній і/чи паперовій формі, повідомлення про прийняття та реєстрацію електронного документа.

Так як обов'язковим реквізитом електронного документа є електронний цифровий підпис, який накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа, слідчому потрібно паралельно перевірити наявність і правильність ведення журналів аудиту щодо подій, пов'язаних із генерацією, використанням і знищенням особистого ключа; порядок і умови розміщення, зберігання, доступу та використання особистого ключа; порядок і умови розміщення, зберігання та доступу до резервної копії особистого ключа; порядок реєстрації (формування сертифіката ключа) центру сертифікації ключів і його відповідність політиці сертифікації та регламенту роботи; порядок і умови зберігання сформованих сертифікатів ключів, а також сертифікатів та документованої інформації, яка підлягає обов'язковій передачі центрами сертифікації ключів у разі припинення їх діяльності; відповідність змісту сформованих сертифікатів установленим законодавством вимогам; факт і порядок розміщення на електронному інформаційному ресурсі документів та інформації, установлених політикою сертифікації; наявність і правильність ведення журналів аудиту щодо подій, пов'язаних з формуванням, скасуванням, блокуванням і поновленням сертифікатів ключів; функціонування електронного інформаційного ресурсу щодо надання доступу до основних даних (реквізитів) акредитованих центрів, центрів сертифікації ключів, переліку сертифікатів центрів сертифікації ключів, а також інформації про статус сертифікатів.

Оскільки дослідження електронного документа потребує наявності спеціальних знань у сфері комп'ютерних технологій, рекомендується до огляду таких документів залучати відповідних спеціалістів (комп'ютерного техніка чи програміста). Доцільніше залучати в якості спеціалістів тих осіб, які в подальшому будуть проводити відповідні судові експертизи.

Одержано 18.11.2013

УДК 343.13

Ганна Василівна РОСЬ,
кандидат юридичних наук,
доцент кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ ТА ЇХ РОЗСЛІДУВАННЯ

Внаслідок розвитку інформаційних та телекомунікаційних технологій сучасне суспільство все більше залежить від управління різними процесами комп'ютерною технікою. Використання інформаційних технологій поширюється майже на усі сфери людської діяльності – від контролю за повітряним та наземним транспортом до вирішення проблем національної безпеки. Інформація, як один з основних елементів цього процесу, відіграє все більш суттєву роль як в житті окремої людини, так і в житті всього суспільства і кожної держави.

Небажаним наслідком технічного прогресу, пов'язаного із запровадженням сучасних інформаційних технологій, є виникнення нових видів злочинів та такого небезпечного антисоціального явища, яке отримало назву – «кіберзлочинність». У КК України зазначені види злочинів визначаються зокрема розділом XIV «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361), створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361[1]) та інші.

При цьому в літературі слушно відмічається, що використання інформаційних систем у злочинних цілях за своїми наслідками може порівнятися з дією зброї масового знищення. Тож на сьогоднішній день кіберзлочинність розглядається як швидко зростаюча загроза безпеці, як для окремих держав, так і для світового співтовариства в цілому.

Відтак проблема протидії кіберзлочинності та напрацювання й удосконалення практики розслідування даних видів злочинів є першочерговими.

З метою запобігання злочинам, вчиненим у сфері інформаційних технологій, 23 листопада 2001 року в Будапешті була підписана Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації [2], більш відома в Україні під назвою «Конвенція про кіберзлочинність».

Згідно цієї Конвенції злочини в сфері інформаційних технологій (кіберзлочини) класифіковано на чотири групи:

1) злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;

2) злочини, пов'язані з використанням комп'ютерних засобів;

3) злочини, що здійснюються шляхом виробництва (з метою розповсюдження через комп'ютерну систему), надання пропозицій для користування, поширення та придбання різних видів дитячої порнографії, а також володіння дитячою порнографією, що знаходиться в пам'яті комп'ютера певної особи;

4) злочини, пов'язані з порушенням авторського права і суміжних прав (щодо програмного забезпечення)

Факторами, що ускладнюють діяльність із запобігання та розслідування даної категорії злочинів є, перш за все, їх надзвичайно висока латентність (переважна більшість протиправних дій у сфері сучасних інформаційних технологій залишається не тільки не розкритими, але навіть не виявленими). До таких факторів відносяться, крім того, транснаціональність таких злочинів, тенденція до їх збільшення, високий професіоналізм осіб, які вчиняють подібні правопорушення, комплекс юридичних і технічних питань, пов'язаних як з недосконалістю законодавчої бази, так і відсутністю необхідних технічних засобів протидії кіберзлочинам.

Специфіка протидії кіберзлочинності полягає в тому, що, як правило, ці злочини мають міжнародний характер і, в цілому, не підпадають під юрисдикцію якої-небудь конкретної держави. В той же час, системи кримінального правосуддя, зокрема, вітчизняне законодавство, пов'язує кримінальну відповідальність за вчинення злочину з територіальною ознакою його вчинення. У зв'язку з цим, труднощі у визначенні територіальної підслідності впливають на оперативність початку досудового розслідування та проведення невідкладних слідчих (розшукових) дій, а відповідно на виявлення та

фіксацію доказів, як вчинення самого правопорушення, так і вчинення його певною особою, а в підсумку на притягнення винних осіб до відповідальності за вчинені правопорушення.

Суттєвою проблемою є також виявлення та фіксація доказів протиправних дій в телекомунікаційних мережах, зважаючи на легкість знищення та зміни комп'ютерної інформації, тобто слідів злочину, неможливість вилучення «віртуальних» слідів злочину, які можливо лише скопіювати, короткочасність зберігання слідів кіберзлочинів на серверах компаній (операторів телекомунікаційних мереж), складність проведення невідкладних дій, спрямованих на виявлення факту правопорушення та ідентифікації осіб, причетних до злочинної діяльності в комп'ютерних мережах.

Тож окреслені питання потребують подальшої розробки та якнайшвидшого вирішення.

Список використаних джерел:

1. Кримінальний кодекс України // Відомості Верховної Ради України. – 2001. – № 25. – Ст. 131. – Станом на 04.07.2013.

2. Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 : ратиф. Верховною Радою України із застереженнями і заявами Законом № 2824-IV від 07.09.2005 // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.

Одержано 18.11.2013

УДК 343.98

Олександр Анатолійович СЕВІДОВ,
кандидат юридичних наук,
доцент кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

КРИМІНАЛІСТИЧНА КЛАСИФІКАЦІЯ СУБ'ЄКТІВ КІБЕРЗЛОЧИНІВ ТА ЇХ ОСОБЛИВОСТІ

Глобальна комп'ютеризація сучасного суспільства, яка стосується практично всіх сторін діяльності держави, людей, підприємств і організацій, породила нову сферу суспільних відносин, яка, на жаль, нерідко стає об'єктом протиправних дій.

Кіберзлочинність – це злочинність у так званому віртуальному просторі. Віртуальний простір можна визначити як змодельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети,

факти, події, явища і процеси, представлені в математичному, символьному чи будь-якому іншому вигляді які знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки та передачі. Це визначення відповідає рекомендаціям експертів ООН. На їх думку, терміну «кіберзлочинність «відповідає будь-який злочин, який може здійснюватися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі чи проти комп'ютерної системи або мережі. Таким чином, до кіберзлочинів може бути віднесено будь-який злочин, скоєний в електронному середовищі.

Ведучи мову про особистість злочинців, важливо підкреслити, що даному типу людей притаманний високий рівень інтелектуального розвитку, нестандартність мислення, професіоналізм, висока зацікавленість новими комп'ютерними технологіями, винахідливість, багата фантазія і скритність. Більшість таких осіб знають декілька мов програмування, мають значний досвід роботи на комп'ютері, в минулому до кримінальної відповідальності не притягувався, є яскравою, мислячої особистістю, здатної приймати відповідальні рішення. Вони здатні чітко формулювати будь-яку професійну задачу, але часто характеризується хаотичним поведінкою в побуті; мають розвинене формально-логічне мислення, яке часто підводить у реальному житті; прагнуть до точності, чіткості і однозначності у мові, постійно задають уточнюючі питання і перепитують, що викликає роздратування співрозмовника; постійно використовують комп'ютерний жаргон, незрозумілий оточуючим.

Правопорушники у сфері комп'ютерної інформації можуть бути розділені на дві вікові групи: перша – 14–20 років, друга – з 21 року.

Представники першої вікової групи – це старші школярі або студенти молодших курсів вищих або середніх спеціальних навчальних закладів, які активно шукають шляхи самовираження і знаходять їх, занурюючись у віртуальний світ. При цьому найчастіше ними рухає цікавість і бажання перевірити свої сили. До числа особливостей, які вказують на вчинення комп'ютерного злочину особами даної категорії,

можна віднести: відсутність цілеспрямованої, продуманої підготовки до злочину; оригінальність способу; невжиття заходів до приховування злочину; факти невмотивованих пустощів.

Комп'ютерні злочинці, що входять у другу вікову групу – це вже цілком сформовані особистості, що володіють високими професійними і стійкими злочинними навичками, а також певним життєвим досвідом. Це зазвичай висококваліфіковані фахівці з вищою математичною, інженерно – технічною або економічною освітою, що входять в організовані злочинні групи і спільноти, для яких характерні мобільність, висока технічна оснащеність, чіткий розподіл ролей, яскраво виражена корислива мотивація, добре продумана система приховування слідів злочинних діянь. Найбільшу небезпеку і складність для розкриття та розслідування представляють злочини вчинені групою осіб, у складі яких присутні висококваліфіковані фахівці, що володіють спеціальними знаннями в області негласного отримання та захисту комп'ютерної інформації. Велика частина злочинів, скоєних зазначеними суб'єктами, залишаються латентними.

Виділення типових категорій злочинців, знання їх основних рис дозволяє оптимізувати процес пошуку злочинця і дозволяє точніше встановити і викрити конкретного правопорушника.

За цілями та сферою злочинної діяльності всіх осіб, які намагаються отримати доступ до чужої інформації, доцільно розділити на окремі підгрупи:

1) хакери (hackers);
2) кракери (crackers);
3) кардери (carders);
4) фішери (fishers);
5) спамери (spammers);
6) фрікер (phone + break = phreak);
7) кіберкруки (cybercrooks);
8) комп'ютерні пірати.

1. Хакери, здійснюючи діяння, що не спрямовані на отримання матеріальної вигоди, прагнуть перевірити власні здібності в області інформаційних технологій, випробувати нові знання, заробити повагу серед їм подібних. Основне завдання хакера полягає в тому, щоб, досліджуючи обчислювальну систему, виявити слабкі місця в її безпеці, інформувати

про це користувачів і розробників системи, внести пропозиції щодо її удосконалення.

2. Кракер здійснює злом комп'ютерної системи з метою отримання несанкціонованого доступу до чужої інформації та матеріальної вигоди. Наприклад, викрадення паролів доступу в Інтернет, номерів інтернет-пейджерів, адрес електронної пошти а також конфіденційної інформації для подальшого збуту. Нерідко послугами кракерів можуть користуватися зацікавлені треті особи, наприклад, для отримання інформації про плани конкурентів або з'ясування відомостей про реєстрацію ТЗ.

Кракерів у свою чергу можна поділити на три групи:

а) «Вандали» – злочинці які поширюють шкідливі програми – віруси, авторами яких вони найчастіше виступають. Їх основна мета полягає у зломі комп'ютерної системи для її подальшого руйнування, знищення файлів, форматування жорсткого диска комп'ютера та ін.;

б) «Жартівники» – найбільш нешкідлива, з точки зору шкоди для комп'ютерної інформації, частина кракерів. Їх основна мета – злом комп'ютерної системи і внесення до неї різних звукових, шумових, візуальних ефектів (музикальних фрагментів; тремтіння, перевертання зображення; поява різних написів, всяких картинок і т. п.).;

в) «Зломщики» – професійні кракери, здійснюють злом комп'ютерної системи з метою розкрадання коштів, промислового та комерційного шпигунства, розкрадання програмного забезпечення і т. п. Ця група осіб має стійкі злочинні навички, здійснювані ними злочини носять серійний характер. Можуть діяти як у своїх інтересах, так в інтересах інших осіб.

3. Кардери – це особи, які займаються викраденням номерів кредитних карт з подальшим отриманням доступу до рахунків осіб, чиї номери і коди карт були викрадені. Цією групою використовуються різні методи, від елементарного підглядання коду карти з наступною крадіжкою самої карти, до крадіжки номерів з пам'яті ПК, створення підставних банкоматів та Інтернет магазинів.

4. Фішери створюють підставні сайти (наприклад копії сторінки банку), заходячи на який власник карти, бажаючий перевірити свій рахунок, вводить конфіденційні дані, які згодом використовуються зловмисниками.

5. Спамери займаються масовим розсиланням непотрібних (рекламних, шкідливих і т. д.) повідомлень по мережі (пошта, інтернет-пейджери). Як правило, діють в інтересах третіх осіб за матеріальну винагороду.

6. Фрікери проникають в телефонні мережі або інші захищені телекомунікаційні системи. Спеціалізуються на використанні телефонних систем з метою уникнення оплати телекомунікаційних послуг. Їх злочинна діяльність спрямована на отримання кодів доступу, розкрадання телефонних карток і номерів доступу з метою перенести оплату на рахунок іншого абонента.

7. Кіберкруки – злочинці, які спеціалізуються на розрахунках. Використовують комп'ютери для крадіжки грошів, отримання номерів кредитних карток та іншої цінної інформації. Нерідко отриману інформацію вони продають іншим особам.

8. Комп'ютерні пірати спеціалізуються на незаконному зломі систем захисту ліцензійних комп'ютерних програмних продуктів, які потім поширюються за гроші.

Також існують такі особи, які не розбираються в інформаційних технологіях, але в силу збігу обставин отримали доступ до конфіденційної інформації, яка може бути цікава третім особам.

У разі вчинення злочину у сфері комп'ютерної інформації стосовно юридичної особи, кіберзлочинців можна також класифікувати на:

1) зовнішніх – особи, не пов'язані трудовими відносинами з організацією-жертвою;

2) внутрішніх – особи, пов'язані трудовими відносинами з організацією-жертвою (інсайдери):

– співробітники організації, що займають керівні (відповідальні) пости;

– співробітники – користувачі ЕОМ, що зловживають своїм становищем.

Інсайдер – особа, що має в силу свого службового становища, доступ до конфіденційної інформації установи, організації, компанії. Як правило, інсайдером є співробітник даної установи, організації. Це – оператори ЕОМ, периферійних пристроїв і засобів зв'язку; програмісти; інженери – системотехніки; інженери – електроніки; адміністратори баз даних; посадові та інші особи, які мають доступ до ЕОМ, системі

ЕОМ або їх мережі. Злочинець з числа співробітників організації є зразковим службовцям, які мають відповідну освіту. Зазначені особи, як правило, раніше не скоювали ніяких злочинів. Нерідко – це керівники різного рангу, які мають розпорядчі функції, але безпосередньо не відповідають за конкретні ділянки роботи з комп'ютерною інформацією та ЕОМ.

Одержано 15.11.2013

УДК 343.1:004

Александра Сергеевна ТУНТУЛА,
кандидат юридических наук,
доцент кафедры гражданского и уголовного права и процесса
Черноморского государственного университета

НОВЫЕ ПРОЦЕССУАЛЬНЫЕ СТАТУСЫ ЛИЧНОСТНЫХ ИСТОЧНИКОВ АНТИКРИМИНАЛЬНЫХ КИБЕРСВЕДЕНИЙ

Антикриминальные сведения об обстоятельствах совершений киберпреступлений получают от личностных и вещественных источников.

Наибольшую значимость имеют такие процессуальные статусы личностных источников антикриминальных киберсведений:

1. Свидетель – лицо, в отношении которого главный субъект не имеет обоснованных сведений об его участии в макроправонарушении, которое не потерпело от этого деяния и сохраняет в памяти любые сведения, имеющие значение для правильного разрешения антикриминального дела, когда по способу восприятия и содержанию этих сведений такого рода лица делятся на:

1.1. Очевидца – лицо, которое непосредственно наблюдало обстоятельства приготовления или совершения макроправонарушения или сокрытия его следов, не несет ответственности за недонесение или которое сообщило антиделиктные органы об обстоятельствах данного деяния.

1.2. Параочевидца – аналогичное лицо, которое знает об указанных обстоятельствах из других источников.

1.3. Парасвидетеля – лицо, которое может дать показания по любым другим значимым для решения антикриминального дела юридическим фактов (обстоятельствам).

2. Потерпевший – физическое лицо, которому макроправонарушением причинен физический, имущественный или

моральный вред, или юридическое лицо, которому при этих же обстоятельствах причинен имущественный или моральный вред, когда по отношению к деянию этого макроправонарушения и к восприятию процесса причинения вреда такого рода лица делятся на:

2.1. Де-факто потерпевшего – лицо, которому макроправонарушением такой вред причинен непосредственно, и которое сознательно наблюдало данное деяние.

2.2. Де-факто парапотерпевшего – лицо, которому макроправонарушением такой вред причинен непосредственно, но которое в силу бессознательного состояния или невменяемости, ограниченной вменяемости, отсутствии на месте или по другим причинам не могло сознательно наблюдать данное деяние.

2.3. Де-юре потерпевшего – лицо, которому макроправонарушением такой ущерб причинен косвенно, признано потерпевшим в силу закона и которое непосредственно наблюдало данное деяние.

2.4. Де-юре парапотерпевшего – лицо, которому макроправонарушением такой ущерб причинен косвенно, признано потерпевшим в силу закона и которое в силу изложенных причин не могло наблюдать данное деяние.

3. Преследуемый – лицо, в отношении которого у главного субъекта имеются обоснованные сведения о подготовке или совершении им определенного макроправонарушения, с началом и степенью доказанности чего в предусмотренном УПК Украины порядке процессуальный статус указанного лица меняется на:

3.1. Подозреваемого – с началом доказывания такого рода обстоятельств по базисному, специальному или частному предмету доказывания путем проведения любого де-факто процессуального или де-юре процессуального действия, в т. ч. направление данному лицу уведомления о подозрении и внесение в Единый реестр досудебных расследований заявления или сообщения о подготовке или совершении им макроправонарушения, которое еще длится или уже завершилось, допроса преследуемого по поводу указанных обстоятельств или проведение с ним по этому поводу любого иного де-факто или де-юре процессуального действия, задержание этого лица по подозрению в подготовке или совершении макроправонарушения либо избрание ему определенной меры пресечения.

3.2. Обвиняемого – с доведением вины преследуемого в совершении состава деяния конкретного макроправонарушения, в силу чего безотлагательно должно быть вынесено постановление о предъявлении ему обвинения и данное лицо должно быть допрошено.

3.3. Подсудимого – с завершением процедуры доказывания всех обстоятельств и судебной подготовки, необходимых для правильного судебного разбирательства антикриминального дела, что обусловливает безотлагательное назначение дела для такого рассмотрения.

3.4. Осужденного – с вынесением обвинительного приговора либо окончательного решения следователя о закрытии антикриминального дела производством по нереабилитирующим обстоятельствам, предусмотренным определенной нормой УК Украины.

3.5. Оправданного – с вынесением оправдательного приговора или окончательного решения следователя о закрытии антикриминального дела производством по реабилитирующим обстоятельствам, предусмотренным определенной нормой УК Украины.

3.6. Причастного – с вынесением нейтрального приговора или окончательного решения следователя о закрытии антикриминального дела производством за недоказанностью вины преследуемого, то есть когда все возможности для формирования внутреннего убеждению главного субъекта о виновности или невиновности данного лица уже исчерпаны.

3.7. Парапричастного – с вынесением окончательного судебного решения о привлечении несовершеннолетнего, не достигшего возраста назначения наказания, к карательно-воспитательной (принудительных мер воспитательного характера) и к восстановительной и сопутствующей антикриминальной ответственности, которую за малолетнего несет опекун либо лицо или учреждение, его заменяющие.

3.8. Квазипричастного – с вынесением окончательного судебного решения о привлечении невменяемого или ограниченно вменяемого лица к карательно-воспитательной (применение принудительных мер медицинского характера), а опекуна или попечители либо лица или учреждения, его заменяющих – к восстановительной и к сопутствующей антикриминальной ответственности.

3.9. Квазипарапричастного – с вынесением окончательного судебного решения о привлечении к восстановительной и сопутствующей антикриминальной ответственности лица, совершившего общественно опасное деяние, которое не предусмотрено Особенной частью УК Украины.

Одержано 14.11.2013

УДК 343.98:004

Юлія Анатоліївна ЧАПЛИНСЬКА,
кандидат юридичних наук,
доцент кафедри кримінально-правових дисциплін
Дніпропетровського державного університету внутрішніх справ

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОБШУКІВ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Протидія кіберзлочинності на сьогодні має низку невирішених правових, організаційних і тактичних проблем. Неухильне зростання кіберзлочинності, зрощування її з державним апаратом, підвищення технічної оснащеності злочинців, ускладнення зв'язку між ними, використання різноманітного сучасного радіозв'язку та інші негативні чинники, безумовно, ускладнюють і без того непросту діяльність правоохоронних органів і, насамперед, органів внутрішніх справ, зі своєчасного та якісного розкриття, розслідування та профілактики кіберзлочинності. Злочинці не можуть обійтися без надійної організаційно-технічної бази, що робить їх менш вразливими для правоохоронних органів, більш мобільними в одержанні необхідної для злочинної діяльності інформації, що слід враховувати під час підготовки та проведення обшуків.

Узагальнення правоохоронної практики, вивчення кримінальних проваджень свідчить про те, що під час розслідування кіберзлочинів обшуки проводилися у 92 % випадках. За кримінальними правопорушеннями вказаної категорії обшуки мають свою специфіку та складнощі. Так, нерідко під час обшуків у злочинців виявляють комп'ютерну техніку, у якій може міститися інформація, яка має важливе значення для кримінального провадження.

Під час обшуку огляд комп'ютерної техніки має певну специфіку. Це обумовлюється об'єктивною можливістю швидко знищувати інформацію, яка у них міститься. Готуючись до обшуку, необхідно отримати інформацію про наявність

комп'ютерної техніки, її можливості, технічні характеристики і запросити фахівця з комп'ютерних систем.

Усі дії щодо роботи з комп'ютером повинен виконувати тільки спеціаліст, щоб уникнути можливості знищення наявної інформації [1, с. 98]. Тому для запобігання негативних наслідків необхідно забезпечити охорону засобів комп'ютерної техніки, а також даних і цінної інформації, що знаходиться в операційній системі. Необхідно блокувати роботу виробничого процесу, припинити надходження та виток будь-якого роду інформації з операційної системи.

Особливо уважно необхідно спостерігати, щоб ніхто із працівників установи, де проводиться обшук, не міг внести зміни до роботи комп'ютерної системи. У зв'язку з цим, на думку О. І. Мотлях, необхідно заборонити:

– усім працівникам торкатися до засобів комп'ютерної техніки з метою запобігання можливості пошкодження або знищення інформації;

– вимикати з мережі електропостачання технічні засоби;

– переставляти (переносити) з одного робочого місця окремі вузли технічного оснащення на інше або за межі приміщення;

– без дозволу слідчого телефонувати або відповідати на телефонні дзвінки, оскільки діалог може послужити відповідним сигналом для знищення інформації та ін. [2, с. 157].

Слідчому до вимикання комп'ютерної техніки рекомендується скласти її схему та схему підключення до мережі (якщо така має місце) і провести фото- чи відеозйомку усього устаткування та всіх монтажних з'єднань (мається на увазі задню стінку системного блоку та адаптеру мережі) [3, с. 79].

У тих випадках, коли наявність комп'ютерної техніки виявляється після прибуття на місце проведення обшуку, необхідно негайно вжити заходів для запрошення фахівця. Усі вилучені під час обшуку предмети необхідно зосереджувати в одному місці і залишати під постійним наглядом. Слід зазначити, що під час вилучення предметів повинні зберігатися ознаки, які вказують на причетність осіб, що обшукуються, до злочинної діяльності.

Підсумовуючи, слід зазначити, що протидіючи кіберзлочинності, необхідно враховувати, що злочинці не завжди можуть комп'ютерні техніку, інші засоби, що значення для кримінального провадження, за місцем проживання, а

користуються послугами осіб, які не брали безпосередньої участі у вчинених злочинах або не входять до складу злочинних груп, але здатних за певну винагороду зберігати у себе вказані об'єкти. Такі особи, як правило, приховують свої зв'язки зі злочинцями, тому під час підготовки до проведення обшуків важливо виявити таких осіб, застосовуючи оперативно-розшукові заходи. Це дозволяє економити час, сили та засоби і тим самим сприяє реалізації принципу наступальності у боротьбі з кіберзлочинністю.

Список використаних джерел:

1. Журавель В. А. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом : наук.-практ. посіб. / В. А. Журавель. – Х. : Одіссей, 2005. – 312 с.

2. Мотлях О. І. Тактичні основи проведення обшуку у злочинах, пов'язаних з інформаційними технологіями / О. І. Мотлях // Вісник Академії праці і соціальних відносин Федерації профспілок України. – 2002. – № 2. – С. 157–159.

3. Горбаньов І. М. Особливості огляду місця події при розслідуванні незаконного використання комп'ютерних програм / І. М. Горбаньов // Вісник Луганської академії внутрішніх справ України. – 2005. – Спец. вип. : Виявлення, фіксація та використання доказів у процесі досудового слідства : у 2 ч. – Ч. 2. – С. 75–81.

Одержано 08.11.2013

УДК 343.98

Тетяна Іванівна САВЧУК,
кандидат юридичних наук, старший викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

ПРЕДМЕТ ДОПИТУ ПІДОЗРЮВАНИХ У ВЧИНЕННІ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Комп'ютерні злочини – це одна із нагальних проблем сучасного суспільства, яка досить швидко поширюється. Це зумовлене технологічним розвитком у сфері комп'ютеризації та розширенням сфери застосування комп'ютерної техніки, яка впроваджується в різноманітні галузі людської діяльності та виконує найважливіші функції сучасного суспільства. До даного виду злочинів належать найрізноманітніші прояви злочинів, які вчиняються з допомогою комп'ютерних технологій, але найчастішими їх проявами є розповсюдження

комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем тощо.

Ці злочини можуть бути вчинені як із корисливих чи хуліганських мотивів так і для перевірки власних професійних умінь та самоствердження. Іноді такі особи не переслідують якоїсь відповідної мети, а просто бажають пожартувати. Саме характер злочину та мотиви його вчинення і обумовлюють поведінку підозрюваних під час допиту та особливості тактики проведення вказаної слідчої дії.

Зважаючи на специфічність комп'ютерних злочинів та наявність у злочинця професійних знань і навичок, під час планування допиту необхідно проконсультуватись зі спеціалістом або ж самостійно ознайомитись зі спеціальною літературою у вказаній сфері. Ці дії допоможуть правильно визначили коло обставин, що підлягають встановленню. В окремих випадках доцільно запросити спеціаліста для участі у слідчій дії.

Предмет допиту підозрюваних у вчиненні кіберзлочинів повинні складати обставини загального характеру та специфічні обставини, відповідно до конкретного вчиненого комп'ютерного злочину. До обставин загального характеру повинні входити наступні:

– наявність у підозрюваного навичок поводження з комп'ютером, де, коли і за яких обставин набув навичок роботи з комп'ютерною технікою і з конкретним програмним забезпеченням;

– де працює на комп'ютері: за місцем роботи, проживання чи використовує комп'ютери інших осіб, або комп'ютерні клуби;

– місце роботи та посада підозрюваного, чи має правомірний доступ до комп'ютерної техніки і якщо так, то до яких видів програмного забезпечення;

– які операції з комп'ютерною інформацією виконує на робочому місці;

– чи має правомірний доступ до мережі Інтернет та чи працює в Інтернеті;

– чи закріплені за ним по місцю роботи або проживання ідентифікаційні коди та паролі для роботи в комп'ютерній мережі;

– які операції виконує на своєму персональному комп'ютері за місцем проживання або інших персональних комп'ютерах, де і у кого придбав програми для свого комп'ютера;

– які обставини, що передували вчиненню злочину: коли виник умисел на вчинення злочину, мотиви та мета вчинення вказаного злочину; чому злочинне посягання було направлено саме на даний конкретний об'єкт;

– які конкретні злочинні дії вчинені злочинцем з використанням комп'ютерних технологій;

– чи вчинявся злочин підозрюваним самостійно або ж у співучасті, якщо у співучасті, то який розподіл ролей, хто ініціатор вчинення злочину і які конкретні дії здійснював кожен із учасників;

– чи отримав підозрюваний матеріальну винагороду за вчинення злочину, якщо так то у якій сумі.

Залежно від виду злочинного посягання при допиті підозрюваного повинні бути встановлені обставини щодо конкретної злочинної технології та програмних продуктів і обладнання використаного підозрюваним. Крім того, необхідно також встановити місцезнаходження вказаних об'єктів з метою їх вилучення, дослідження та використання у процесі розслідування. Особливе значення має також встановлення місця та часу отримання доступу до комп'ютерної інформації, способу подолання системи захисту та часу несанкціонованого перебування у комп'ютерній системі. У випадку розповсюдження вірусних програм необхідно крім вказаних обставин також встановити способи розповсюдження вказаних програм, а також можливість їх саморозповсюдження.

Під час допиту також повинні бути встановлені обставини, що характеризують особу злочинця. Так в деяких випадках вказані злочини вчиняються особами, які мають певні види психічних відхилень – інформаційні хвороби, так звані «комп'ютерні фобії». Зважаючи на те, що допит одна із слідчих дій, які передбачають тісне спілкування слідчого із підозрюваним, то саме при проведенні цієї слідчої дії і передбачається можливим встановлення ознак психічних відхилень та необхідності проведення психіатричної експертизи підозрюваних.

Враховуючи викладене можна підсумувати, що допит підозрюваних у вчиненні кіберзлочинів є особливо складною слідчою (розшуковою) дією, проведення якої повинно ретельно

плануватись за участю спеціалістів у сфері комп'ютерних технологій. Обставини, що підлягають встановленню під час допиту доцільно зафіксувати у письмовому плані, так як вони є специфічними та можуть містити велику кількість спеціальної термінології.

Одержано 18.11.2013

УДК 343.98

Денис Андрійович САФОНОВ,
кандидат юридичних наук,
старший викладач кафедри криміналістики,
судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ЗАВІДОМО НЕПРАВДИВИМ ПОВІДОМЛЕННЯМ ПРО ЗАГРОЗУ БЕЗПЕЦІ ГРОМАДЯН

В останні роки в Україні значно почастішали випадки вчинення кримінальних правопорушень, пов'язаних з із завідомо неправдивим повідомленням про загрозу безпеці громадян. Суспільна небезпека таких злочинів полягає у тому, що зловмисник своїми діями не тільки штучно створює обстановку страху серед населення і дестабілізує роботу підприємств, організації, установ, але й призводить до марного використання сил та засобів правоохоронних органів по пошуку небезпечних речовин або вибухових пристроїв.

Серед основних чинників, які сприяють поширенню явища «телефонного тероризму» відносяться: а) складність встановлення особи, яка через засоби дротового або мобільного зв'язку передає неправдиве повідомлення; б) неочевидний характер вчинення протизаконних дій, а саме відсутність в свідків тощо; в) складнощі з доведення вини особи.

Криміналістична характеристика даного виду злочину, як система взаємопов'язаних між собою криміналістично значущих елементів, повинна формуватися на підставі дослідження матеріалів судово-слідчої практики. Це дозволить наблизитися до встановлення закономірних зв'язків між структурними елементами характеристики з метою отримання більш прийнятних даних про особу злочинця, особливості

способу вчинення злочину, обстановку та сліди кримінального правопорушення.

Так, при дослідженні матеріалів кримінальних проваджень було встановлено, що у 20 % випадків, зловмисники повідомляли про знаходження вибухового пристрою у приміщенні пасажирських вокзалів (аеропорт); у 27 % випадків об'єктом «мінування» виступали торгово-розважальні центри або розважальні заклади (нічні клуби, дискотеки); та інші об'єкти, серед яких приватні будинки, помешкання окремих громадян (14 %); заклади освіти (14 %); ринки (8 %); будівля адміністрації Президента України (6 %); місцеві органи влади (3 %); будівлі правоохоронних органів та суди (3 %); заклади охорони здоров'я (2 %); приватні транспортні засоби (2 %).

За способом надання неправдивої інформації до правоохоронних органів розрізняються повідомлення здійсненні зловмисниками з використанням:

а) власних мобільних телефонів;

б) телефонів, що належать знайомим або стороннім особам;

в) стаціонарних телефонів, за місцем мешкання зловмисника;

г) телефонних апаратів та таксофонів, розташованих на об'єктах, «мінування».

В структурі криміналістичної характеристики даного виду злочинів, одне з головних місць займає дослідження особи «телефонного терориста». Узагальненням матеріалів практики було встановлено, що частіше за все повідомлення надходять від чоловіків 20–45 років, раніше не засуджених, з середньою або середньо-спеціальною освітою, які проживають в районі знаходження об'єктів «терористичного» посягання.

Мотивами повідомлення в більшості ситуацій є хуліганські спонукання, в деяких випадках це пов'язано з бажанням особи помститися окремим громадянам або завдати матеріальних збитків адміністрації підприємств, установ, розважальних закладів. Слід сказати, що переважаюча кількість неправдивих повідомлень вчиняється особами, яка знаходяться в стані алкогольного сп'яніння. Зауважимо, що трапляються і випадки в яких зловмисники, розуміючи кримінальну відповідальність свідомо вказують свої особисті дані, з метою подальшого засудження та потрапляння у місця позбавлення волі. Такі ситуації, пов'язані з особами які були раніше засудженні,

та виявляють бажання повернутися у спеціальні заклади в яких вони, за час перебування значно адаптувалися.

До типових слідів по даній категорії проваджень слід віднести власне сліди особи (відбитки пальців рук, взуття) на місці вчинення кримінальних правопорушень. Досить вдало використовуються звукозаписи голосової інформації фіксовані на спеціальні пристрої у чергових частинах правоохоронних органів. Одне з головних місць у розслідуванні таких злочинів, займають питання взаємодії органів внутрішніх справ з відділами державного зв'язку, операторами мобільного зв'язку та телекомунікаційних систем.

Підводячи висновки, звернемо увагу на те, що подальші наукові розробки питання протидії даного виду злочинів є досить актуальними і потребують поглибленого дослідження науковцями в галузі криміналістики.

Одержано 07.11.2013

УДК 343.98

Богдан Анатолійович БУРБЕЛО,
викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

КРИМІНАЛІСТИЧНІ ОСНОВИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Боротьба з кіберзлочинністю є однією з актуальних проблем в світі. З розвитком і вдосконаленням глобальних комунікаційних мереж, комп'ютерного забезпечення відбувається і еволюція кримінального середовища як окремо взятої держави, так і всього світового співтовариства в цілому.

Нині жертвами осіб, які вчиняють злочини у віртуальному просторі, можуть стати не лише окремі люди чи юридичні особи, а й цілі відомства і навіть держави. Кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі Інтернет, вона поширюється на всі види злочинів вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати предметом злочинних посягань, середовищем, в якому відбуваються правопорушення і засобом або знаряддям злочину. Це і дитяча порнографія, шахрайства, несанкціоноване втручання в роботу комп'ютерних і телекомунікаційних мереж, виготовлення та поширення

шкідливих програм, викрадення ідентифікаційних даних осіб, електронне вимагання та інші.

Боротьба з кіберзлочинністю ускладнена наявними особливостями – латентністю кіберзлочинів; можливістю знищення або зміни комп'ютерної інформації, що є доказом вчинення злочину; виникненням проблеми огляду комп'ютерних систем, вилучення і дослідження слідів вчинення кіберзлочинів, які зберігаються в пам'яті технічних пристроїв, в електромагнітному полі, на машинних носіях комп'ютерної інформації; короткочасністю зберігання інформації, здатної виступити як доказ на серверах компаній – операторів телекомунікаційних мереж тощо.

Враховуючи суспільну небезпеку, виражену латентність, складність розслідування неправомірного доступу до комп'ютерної інформації, а так само наявний світовий досвід, особливу увагу, на наш погляд, необхідно приділяти питанням попередження та профілактики даних злочинів.

Результати наукових досліджень свідчать, що протидія злочинності в широкому розумінні включає у себе загальнодержавні заходи економічного, політичного, виховного та іншого характеру, а також комплекс спеціальних заходів, спрямованих на безпосереднє подолання злочинності. У такому розумінні система протидії злочинності корелюється з класичними гарантіями законності. Акцентуючи увагу на протидії кіберзлочинності, їх можна узагальнено представити у вигляді системи гарантій законності в інформаційній сфері, яка є правовою стороною системи діяльності по забезпеченню інформаційної безпеки. Для цього необхідний постійний активний процес розробки дієвих заходів, спрямованих на правове, організаційне, включаючи криміналістичне, технічне, забезпечення боротьби зі злочинами у сфері комп'ютерної інформації, а також вдосконалення методики їх розслідування та попередження.

На нашу думку, ефективними способами профілактики кіберзлочинності є вдосконалення науково-технічних засобів, тактичних прийомів і методів розслідування неправомірного доступу до комп'ютерної інформації; своєчасне виявлення і припинення як розпочатих злочинів, так і неправомірного доступу до комп'ютерної інформації на стадії замаху або підготовки до нього; встановлення обставин, що сприяли вчиненню кожного злочину, розробка і вдосконалення методів і прийомів виявлення таких обставин.

Першочерговим завданням слідчого на початковому етапі розслідування кіберзлочинів є аналіз інформаційного середовища вчинення злочину:

– визначення типу ЕОМ (типу носія), де зберігалася або оброблялася комп'ютерна інформація, до якої здійснено неправомірний доступ (Web-сервер, персональний комп'ютер, мобільний телефон, електронна кредитна карта), що визначить напрямок всього подальшого розслідування;

– встановлення типу операційної системи комп'ютера (сервера), до якого здійснено неправомірний доступ (Unix, Linux, Netware, Windows), а також використаного для вчинення злочину програмного забезпечення, що значною мірою допоможе звузити коло можливих підозрюваних;

– визначення апаратного та програмного забезпечення, яке піддалося впливу в ході неправомірного доступу, а також інформації про засоби і знаряддя вчинення такого доступу, що дозволить скласти об'єктивну картину інформаційних слідів злочину.

У ході розслідування неправомірного доступу до комп'ютерної інформації слідчому необхідно максимально використовувати спеціальні знання експертів і фахівців, а також оперативну інформацію. Проведенню кожної слідчої дії повинна передувати ретельна підготовка, що включає в себе: вивчення та аналіз матеріалів кримінального провадження, вибір місця, часу проведення слідчої дії, визначення складу учасників та їх інструктаж, підбір технічних засобів фіксації результатів проведення слідчої дії, а при необхідності також підготовку комп'ютерно-технічних, програмних та інших засобів.

З метою зниження ризику несанкціонованого доступу до комп'ютерної інформації юридичних осіб необхідно: наявність посадової особи або підрозділу, що відповідає за безпеку комп'ютерної інформації; контролювання доступу співробітників до елементів управління засобів комп'ютерної техніки; використання складних паролів і їх своєчасна зміна; укладання договорів з працівниками на предмет нерозголошення охоронюваної комп'ютерної інформації; періодичне створення резервних копій комп'ютерної інформації, а також дотримання термінів їх зберігання тощо. Власники і користувачі комп'ютерної інформації повинні приділяти достатню увагу питанням захисту власних інформаційних комп'ютерних

ресурсів, періодично оновлювати програмне і апаратне забезпечення (особливо, засоби захисту комп'ютерної інформації), що здатне мінімізувати ризики несанкціонованих замахів, тобто попередити злочин.

Також необхідно на базі існуючих єдиних стандартів вищої юридичної освіти включити в курси кримінального права, кримінально-процесу, криміналістики, інформатики теми, присвячені характеристиці неправомірного доступу до комп'ютерної інформації, особливостям його розслідування в цілому, проведення окремих слідчих дій та попередження даних злочинів. Необхідною умовою підготовки фахівців належної кваліфікації для боротьби з кіберзлочинністю є тісний взаємозв'язок навчального процесу з науковими дослідженнями і практикою правоохоронної діяльності, розширення міжнародних зв'язків.

Одержано 19.11.2013

УДК 343.121.5

Віталій Володимирович РОМАНЮК,
викладач кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

УМОВИ ОБҐРУНТОВАНОСТІ ЗАСТОСУВАННЯ ПРИМУСУ ЩОДО НЕПОВНОЛІТНІХ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Введення в дію Кримінального процесуального кодексу України пов'язано із необхідністю правильного сприйняття та застосування слідчими, прокурорами, суддями його норм, що зокрема стосується норм, якими врегульовано кримінальне провадження щодо неповнолітніх. Завданням кримінальної процесуальної науки є розробка теоретичних рекомендацій і практичних пропозицій щодо належного застосування нових за змістом та формою норм КПК України, у тому числі і щодо кримінального судочинства стосовно дітей. Одним з таких питань, яке має істотне значення для забезпечення прав неповнолітніх у кримінальному судочинстві, є питання застосування до них процесуального примусу під час розслідування кіберзлочинів.

Слід відзначити, що новий КПК України передбачає істотно інші підходи до застосування примусу. Так, у кримінальному

судочинстві застосування примусу здійснюється, по-перше, за наявності відповідних підстав та в порядку, передбаченому законом, а по-друге, за умови «щоб жодна особа не була піддана необґрунтованому процесуальному примусу» (ст. 2 КПК України). Тобто застосування процесуального примусу, виходячи зі змісту ст. 2 КПК України повинно бути обґрунтованим та здійснюватися в порядку та на підставах, передбачених законом. Це не тільки обмежує випадки безпідставного застосовування щодо особи заходів правообмежувального характеру, а й передбачає необхідність доведення з боку слідчого, прокурора або суду потреби у їх застосуванні. Такий підхід у більшому ступені відповідає правовому та демократичному характеру нашої держави.

Що ж стосується такої специфічної категорії громадян України та особливих учасників кримінального провадження як неповнолітні, то застосування примусу щодо них, окрім загальних підстав та умов, має власну специфіку. У рекомендації Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 18.07.2013 № 223-1134/0/4-13 прямо вказано, що кримінальне провадження щодо неповнолітніх здійснюється у загальному порядку з урахуванням особливостей, передбачених главою 38 КПК, та із дотриманням принципу забезпечення реалізації неповнолітніми особами права користуватися додатковими гарантіями, встановленими вітчизняним законом та міжнародними договорами. Такий підхід відповідає положенням основних міжнародно-правових актів в сфері прав дитини. Зокрема, ст. 3 Конвенції ООН «Про права дитини» визначає, що в усіх діях щодо дітей першочергова увага приділяється якнайкращому забезпеченню інтересів дитини, а ст. 37 Конвенції встановлює вимогу, щоб жодна дитина не піддавалась катуванням та іншим жорстоким, нелюдським або принижуючим гідність видам поводження чи покарання. У свою чергу в п. 54 Керівних принципів ООН для попередження злочинності серед неповнолітніх (Ер-Ріядські керівні принципи) передбачено умову, щоб ніяка дитина або молода людина не повинна піддаватися грубим або принижуючим гідність покаранням в сім'ї, в школі або в інших установах. Нарешті, п. 5.1. Мінімальних стандартних правила ООН, що стосуються відправлення правосуддя щодо неповнолітніх («Пекінські правила») передбачає правило, згідно якого система правосуддя щодо

неповнолітніх спрямоване в першу чергу на забезпечення благополуччя неповнолітнього і забезпечення того, щоб будь-які заходи впливу на неповнолітніх правопорушників були завжди сумірні як з особливостями особистості правопорушника, так і з обставинами правопорушення.

З аналізу міжнародно-правових актів та положень чинного КПК України можна зробити висновок, що до умов застосування примусу до неповнолітнього можна віднести наступні положення:

– виключність застосування примусу як заходу впливу на неповнолітнього;

– дотримання при цьому честі та гідності неповнолітнього;

– відповідність заходу примусу тяжкості та обставинам кримінального правопорушення;

– врахування особливостей особистості неповнолітнього;

– якнайкраще забезпечення інтересів дитини в разі застосовування примусу;

– обґрунтованість слідчим, прокурором, суддею необхідності застосування примусу;

– дотримання вимог процесуальної форми при застосуванні до неповнолітнього примусу.

На підставі наведеного ми можемо відзначити, що застосування щодо неповнолітніх заходів примусу – це здійснюване на підставах та в порядку передбаченому КПК України обґрунтоване застосування до неповнолітнього процесуального примусу з метою досягнення дієвості цього провадження з одночасним дотриманням прав та свобод такої особи та за умови якнайкращого забезпечення його інтересів.

Вважаємо, що таке розуміння та підхід до застосування примусу щодо неповнолітніх під час розслідування кіберзлочинів не тільки відповідатиме тим підходам, що визнані у міжнародній практиці та практиці Європейського суду з прав людини (Справа "Свершов проти України"), а й знайде своє відображення у новому КПК України. Мова йде про положення ч. 2 ст. 484 КПК України, яка орієнтує слідчого, прокурора та суддю на те, що під час кримінального провадження щодо неповнолітнього вони зобов'язані здійснювати процесуальні дії в порядку, що найменше порушує звичайний уклад життя неповнолітнього та відповідає його віковим та психологічним особливостям та вживати всіх інших

заходів, спрямованих на уникнення негативного впливу на неповнолітнього. Вважаємо, що «здійснювати процесуальні дії» повністю може бути віднесено до застосування заходів примусу щодо неповнолітнього.

Одержано 22.11.2013

УДК 343.98

Андрій Володимирович МИРНИЙ,
старший слідчий
СУ ГУМВС України в Харківській області

РОЗКРИТТЯ ШАХРАЙСТВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ОСОБАМИ, ЯКІ ЗНАХОДЯТЬСЯ В МІСЦЯХ ПОЗБАВЛЕННЯ ВОЛІ

Останнім часом широкого розповсюдження набрало вчинення шахрайств з використанням електронно-обчислювальної техніки особами, які знаходяться в місцях позбавлення волі. Кожного дня до органів внутрішніх справ масово надходять звернення громадян про викрадення коштів з їх карткових банківських рахунків, заволодіння їх коштами під приводом затримання їх родичів та близьких співробітниками міліції або сплачення не існуючої заборгованості перед банком.

Як свідчить статистика, більша кількість таких злочинів так і залишається нерозкритими насамперед у зв'язку із тим, що із часом способи скоєння шахрайств оновлюються, а методики розкриття та розслідування шахрайств потребують удосконалення.

Так, наприклад, в провадженні СУ ГУМВС України в Харківській області знаходилось кримінальне провадження щодо заволодіння благодійними грошовими коштами, які, за оголошеннями, розміщеними в мережі Інтернет, батьки збирали на лікування онкохворих дітей. Вказані злочини було вчинено учасниками організованої групи з числа п'яти осіб, троє з яких знаходились в місцях позбавлення волі, а двоє раніше засуджених діяли на волі на території м. Харкова.

Так, особи, які знаходились в місцях позбавлення волі, протягом року користувалися засобами мобільного зв'язку із доступом до мережі Інтернет та за оголошеннями про надання благодійної допомоги встановлювали анкетні дані потерпілих, а також номери їх карткових банківських рахунків,

після чого під виглядом благодійників або співробітників банку телефонували потерпілим та обманним шляхом отримували від них анкетні дані, а також таємне слово, зазначене в банку для керування рахунком, та номер телефону, зазначений в банку як основний фінансовий номер клієнта. Після цього учасники організованої групи, які знаходились в м. Харкові, отримували дублікат сім-картки потерпілого, активували його в своєму мобільному терміналі та за допомогою функції «конференцзв'язок» здійснювали одночасні з'єднання із номером телефону осіб, які знаходились в колонії, та центром обслуговування клієнтів банку, під час якого комп'ютерною технікою банку визначалося, що дзвінок здійснюється саме з номеру клієнта. Учасники групи від імені клієнта надавали його анкетні дані, таємне слово та давали вказівку оператору на незаконне списання коштів з рахунку потерпілого на рахунки учасників групи та підшуканих ними осіб з числа осіб, які зловживають наркотиками в м. Харкові. Наступним етапом було «відмивання» викрадених коштів, тобто приховування їх злочинного походження. Учасники групи в м. Харкові знімали кошти в банкоматах, після чого з використанням банківських терміналів знеособлено відправляли вказані кошти на рахунки по телефону зазначені учасникам групи, які знаходились на волі засудженими, які знаходились в місцях позбавлення волі.

Вказану злочинну схему було викрито повністю, встановлені всі особи, причетні до скоєння злочинів, та детально викрито схему руху викрадених коштів, починаючи з незаконного їх списання з рахунків потерпілих і закінчуючи кінцевими отримувачами «відмитих» коштів.

Розкриття вказаних злочинів стало можливим завдяки проведенню наступних слідчих (розшукових) дій.

Отримано тимчасовий доступ до інформації операторів мобільного зв'язку за номерами телефонів потерпілих та встановлено номери мобільних телефонів, з яких потерпілим здійснювалися телефонні дзвінки під час викрадення коштів з їх карткових рахунків. Було встановлено, що під час здійснення телефонних дзвінків абоненти, які телефонували потерпілим, знаходились в зоні дії базових станцій операторів, місцезнаходження яких співпадає із місцезнаходженням виправної колонії. Після цього було отримано інформацію операторів мобільного зв'язку щодо номерів *imei* мобільних терміналів, з

якими працювали вказані номери телефонів в місцях позбавлення волі.

Проведено огляди реєстрів телефонних дзвінків за номерами, які працювали на території виправного закладу; під час огляду застосовувався доступ до мережі Інтернет і декілька десятків тисяч номерів телефонів, з яких здійснювалися телефонні дзвінки, були перевірені на наявність про них інформації мережі Інтернет шляхом вводу до вікна інтернет-браузера у різних комбінаціях цифр. Під час проведення вказаних оглядів знайдено інтернет-сторінки, з яких отримано інформацію про: всіх потерпілих або осіб, стосовно яких планувалося здійснення шахрайських дій (їх номери телефонів були зазначені в оголошеннях про збір благодійних коштів); осіб, з якими велися неодноразові телефонні переговори, а саме з особистих оголошень, розміщених в мережі Інтернет та на сторінках в соціальних мережах; крім того були встановлені сторінки в соціальних мережах деяких засуджених, які, відбуваючи покарання у виправних закладах, розміщували в соціальних мережах свої особисті анкети, а також фотознімки, зроблені в місцях позбавлення волі. Крім того, під час огляду були встановлені номери телефонів, з якими найчастіше здійснювалися телефонні з'єднання в період, який співпадає із періодом скоєння шахрайств.

Після цього були отримані тимчасові доступи до речей і документів в банку, а саме за номерами телефонів, з якими найчастіше велися телефонні з'єднання абонентами, які знаходились у виправному закладі, та було отримано анкетні дані власників вказаних телефонних номерів, їх фотознімки, особисті документи та реєстри руху коштів за рахунками, дослідженням яких встановлено, що на їх рахунки мали місце надходження коштів з банківських терміналів в м. Харкові, які здійснювалися за часом саме після отримання викрадених в потерпілих коштів з карткових рахунків учасників групи в м. Харкові. Вказані відомості були досліджені та підтверджені ревізійним шляхом, а також виведено схему руху коштів шляхом співставлення часу та операцій із списання коштів з операціями із зарахування коштів.

Після цього були витребувані відомості з виправного закладу про те, кого із засуджених відвідували вказані особи та кому передавали передачі. Таким чином було встановлено круг осіб, які причетні до скоєння злочинів, після чого під час

проведення слідчих дій із вказаними особами вони підтвердили факти отримання коштів на їх рахунки на прохання засуджених осіб, а також здійснення подальших операцій з вказаними коштами – перерахування на інші рахунки, отримання в банкоматах та придбання за них передач засудженим.

У виправному закладі було отримано інформацію про номери мобільних телефонів, якими користуються співробітники колонії. Аналізом вказаних телефонних номерів було встановлено, що ряд співробітників колонії неодноразово в період вчинення злочинів вели телефонні переговори з абонентами, з номерів телефонів яких здійснювалися телефонні дзвінки потерпілим та дзвінки до банку під час вчинення злочинів. Подальшим відпрацюванням вказаних співробітників було встановлено, що вони отримували винагороду за те, що учасники групи користувалися мобільними телефонами в місцях позбавлення волі, на карткові рахунки, відкриті на ім'я своїх знайомих та родичів в банку, і особисто отримували кошти з указаних карткових рахунків, що підтверджується фотознімками, зробленими банкоматами під час зняття викрадених коштів.

Під час отриманого в банківській установі тимчасового доступу до речей і документів вилучено фонограми із записами телефонних розмов осіб, які телефонували від імені потерпілих до банку під час вчинення злочинів. У кола осіб, з числа засуджених, стосовно яких малася інформація про можливу причетність до скоєння шахрайств, було відібрано зразки голосу, а під час проведення ряду судово-фоноскопічних експертиз встановлено конкретних осіб, які телефонували до банку та від імені потерпілих надавали вказівки про незаконне списання коштів з їх рахунків.

У зв'язку із викладеним вважаємо, що при розкритті шахрайств, пов'язаних із використанням електронно-обчислювальної техніки, скоєних особами, які відбувають покарання в місцях позбавлення волі, необхідно:

– широко застосовувати при проведенні слідчих (розшукових) дії можливості мережі Інтернет, доступ до якої застосовувати під час проведення оглядів інформації, вилученої в операторів мобільного зв'язку;

– отримувати тимчасовий доступ до речей і документів в банківських установах щодо інформації про власників номерів

телефонів, на які найчастіше здійснюються телефонні дзвінки зловмисниками під час здійснення дзвінків потерпілим;

– в операторів мобільного зв'язку отримувати повну інформацію стосовно телефонних з'єднань, і не тільки за мобільними номерами телефонів, а й за номерами *imei* мобільних терміналів, з якими працювали вказані телефонні номери;

– своєчасно вживати заходів щодо встановлення та вилучення в банківських установах та операторів мобільного зв'язку записів телефонних розмов між зловмисниками та їх співробітниками при вчиненні злочинів, оскільки сервери вказаних установ накопичують інформацію для службового користування, але термін її зберігання обмежений у зв'язку із великою кількістю дзвінків.

Розслідування вказаних злочинів повинно здійснюватися слідчими, які спеціалізуються на розкритті кіберзлочинів, із оперативним супроводженням управління боротьби із кіберзлочинністю.

Одержано 20.11.2013

УДК 614.2

Роман Олегович ЖЕЖЕРУН,
оперуповноважений сектору ДСБЕЗ
Соснівського РВ в м. Черкаси УМВС України в Черкаській області

ПРОЦЕСУАЛЬНІ ПРОБЛЕМИ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ЩОДО КІБЕРЗЛОЧИНІВ

На сьогодні прямі щорічні втрати від кіберзлочинності у всьому світі становлять близько 114 млрд дол., тому все більшої актуальності набувають питання попередження та подолання кіберзлочинів. В Україні протидія кіберзлочинам регулюється низкою нормативно-правових актів, а саме: Конституцією України від 28.06.1996; Конвенцією про кіберзлочинність від 23.11.2001, ратифікованою Законом України від 07.09.2005 № 2824-IV; Кримінальним процесуальним кодексом України від 13.04.2012 № 4651-VI; Кримінальним кодексом України від 05.04.2001 № 2341-III; законами України «Про інформацію» від 02.10.1992 № 2657-XII, «Про державну таємницю» від 21.01.1994 № 3855-XII, «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР, «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006

№ 3475-IV, «Про основи національної безпеки України» від 19.06.2003 № 964-IV; Стратегією національної безпеки України від 12.02.2007 № 105/2007; Доктриною інформаційної безпеки України від 08.07.2009 № 514/2009 та ін.

Проблеми протидії кіберзлочинам активно обговорюються як зарубіжними, так і вітчизняними науковцями, досить швидко розвивається практика їх розслідування та застосування відповідних норм законодавства про кримінальну відповідальність. Однією з особливостей розслідування кіберзлочинів є те, що інформація, яка може сприяти розкриттю злочину та притягнення винних осіб до кримінальної відповідальності, зберігається протягом короткого проміжку часу. Так, Ір-адреса, з якої здійснювався вихід правопорушника до всесвітньої мережі Інтернет, зберігається у провайдерів в середньому протягом 2-4 тижнів. Дана інформація, як правило, дає змогу ідентифікувати місцезнаходження зловмисника (номер будинку, квартири, офісу тощо).

Особливості розслідування кіберзлочинів визначено в Кримінальному процесуальному кодексі України [2], який набрав чинності 20 листопада 2012 року та вніс численні зміни в хід розслідування кримінальних правопорушень як на етапі досудового слідства, так і на етапі судового розгляду. Раніше за Кримінально-процесуальним кодексом України [3] слідчий органів внутрішніх справ одразу ж після порушення кримінальної справи наділявся правом за своїм запитом отримувати ряд важливої інформації. Так, згідно п. 17 ст. 11 Закону України «Про міліцію», слідчий був вправі одержувати безперешкодно і безоплатно від підприємств, установ і організацій незалежно від форм власності та об'єднань громадян на письмовий запит відомості необхідні у справах про злочини, що знаходяться у провадженні міліції [4]. Після прийняття Кримінального процесуального кодексу України одержати таку інформацію слідчий може у порядку тимчасового доступу до речей та документів. Даний порядок регулюється главою 15 Кримінального процесуального кодексу України [2], тому слідчий не може застосувати положення п. 17 ст. 11 Закону України «Про міліцію», оскільки має в провадженні не кримінальну справу, а кримінальне провадження. Це у порівнянні з нормами Кримінально-процесуального кодексу України [3] призводить до певного затягування ходу розслідування кримінального провадження через необхідність підготування

відповідного клопотання про тимчасовий доступ до речей та документів слідчим, погодження його з прокурором та отримання ухвали від слідчого судді. Тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та, у разі прийняття відповідного рішення слідчим суддею, судом, вилучити їх (здійснити їх виїмку) [2].

На практиці трапляються випадки затягування слідчим такої першочергової дії, як отримання тимчасового доступу до речей та документів, а саме: до інформації щодо IP-адреси, з якої здійснювався вихід правопорушника до всесвітньої мережі Інтернет. В свою чергу, це призводить до втрати важливих доказів, які дають змогу розкрити злочин та встановити особу правопорушника.

Таким чином, враховуючи вищевикладене, слід зазначити, що з урахуванням стрімкого розвитку комп'ютерної техніки нормативно-правові акти повинні відповідати сучасним вимогам та європейським стандартам. Тому, нагальною є необхідність внесення змін до п. 17 ст. 11 Закону України «Про міліцію» або подальшого вдосконалення глави 15 Кримінального процесуального кодексу України щодо швидкого отримання першочергових даних, які сприяють розкриттю злочину та притягнення винних осіб до кримінальної відповідальності.

Список використаних джерел:

1. Кримінальний кодекс України : закон України від 05.04.2001 № 2341-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14.

2. Кримінальний процесуальний кодекс України : закон України від 13.04.2012 № 4651-VI [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17.

3. Кримінально-процесуальний кодекс України : закон України від 28.12.1960 № 1001-05 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/1001-05.

4. Про міліцію : закон України від 20.12.1990 № 565-XII [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/565-12.

Одержано 05.11.2013

УДК 343.122(477)

Сергій Євгенович АБЛАМСЬКИЙ,
ад'юнкт
Харківського національного університету внутрішніх справ

ПРОБЛЕМНІ ПИТАННЯ ЗАХИСТУ ПРАВ ПОТЕРПІЛОГО ВІД КІБЕРЗЛОЧИННОСТІ

Сьогодні проблеми злочинності у сфері використання комп'ютерної техніки активно обговорюються науковцями, спеціаліста, юристами та практиками. Насамперед, це пов'язано з тим, що досить стрімко розвиваються норм законодавства щодо відповідальність за скоєння злочинів у даній сфері. Однак, в практичному житті виникають проблеми щодо їх застосування.

За дослідженням, це пов'язано з тим, що з кожним днем все більше збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Дійсно, з одного боку значний прогрес та прискорення розвитку науки й технологій у сфері комп'ютеризації максимально спростили та полегшили технічні процеси суспільного життя, а з іншого, супроводжуються й негативними явищами – зростанням злочинності.

Українська кіберзлочинність за півроку виросла вдвічі – за шість місяців 2013 року виявлено близько 2 тис. випадків шахрайства в мережі. Це приблизно ж стільки, скільки було зафіксовано за весь 2012 рік. Раніше повідомлялося про інші «досягнення» в цій сфері: Україна увійшла в число країн-лідерів за кількістю кібератак – вона посіла четверте місце у світі (після Росії, Тайваню й Німеччини). Такі дані змушують неодноразово звертатися до питань безпеки користувача та регулювання Інтернету [1].

Експерти говорять про тривожну тенденцію. За їх словами за останні роки кіберзлочинність стала більш організованою і почала мати форму бізнесу. Дії хакерів орієнтовані на отримання довгострокового доходу. Більше того, до збитків компаній можна віднести не лише пряму втрату від дій хакерів, але і витрати на оборону від кібератак.

Як зазначив начальник Управління боротьби з кіберзлочинністю МВС України Максим Літвінов, є злочини, за яких люди постраждали від дій шахраїв на невеликі суми, а є злочини, не пов'язані з матеріальним збитком, але більш цинічні

і навіть жорсткі: порнографія, наприклад, особливо - дитяча. Виділити якийсь окремий напрямок роботи, більш важливий, також складно, як і оцінити збиток в 100 тис. грн або 100 грн, оскільки на сьогодні суб'єкти досить різні.

Крім того, аналіз структури кіберзлочинів, вчинених упродовж 2012-го та першого півріччя 2013 років, свідчить про те, що третину з них становлять шахрайські прояви. Також, спостерігається тенденція до збільшення кількості таких кримінальних правопорушень. Водночас, урізноманітнюються схеми заволодіння коштами громадян та методи маскування злочинної діяльності в Інтернеті. Упродовж 2012 року правоохоронцями зареєстровано понад 2 тисячі злочинів, вчинених із використанням високих технологій. У першому півріччі 2013 року до ЄРДР внесено майже 1,9 тисячі заяв та повідомлень про такі злочини, а їхнє розкриття становить близько 50 відсотків [2].

Слід відмітити, що в науковій літературі найчастіше зустрічаються два терміни: кіберзлочини та комп'ютерні злочини. Оскільки вони використовуються для назви одних і тих самих суспільно-небезпечних діянь, то їх можна вважати синонімами та рівнозначними. У зв'язку з ратифікацією Україною Конвенції про кіберзлочинність 7 вересня 2005 року вважається за доцільне вживати термін кіберзлочини [3].

У науковій літературі зазначається, що поняття «кіберзлочини» молоде і утворено сполученням двох слів: «кібер» і «злочин». Термін «кібер» має на увазі поняття кіберпростору (у літературі частіше зустрічаються терміни «віртуальний простір», «віртуальний світ») та інформаційний простір, що моделюється за допомогою комп'ютера. Тобто кіберзлочини – це суспільно небезпечні діяння, які так чи інакше пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами. Такі злочини характеризуються наступними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, транснаціональною складовою в основному з використанням інформаційної мережі Інтернет, високим збитком навіть від одиничного злочину [4, с. 134].

У зв'язку з цим, підтримаємо думку В. Г. Хахановського, що потерпілими від кіберзлочинів найчастіше є юридичні особи. Це зумовлено тим, що процес комп'ютеризації широко

охоплює, насамперед, юридичних осіб (організації, установи), а значно меншою мірою – фізичних осіб [5].

У зв'язку з цим, М. І. Панова, В. Ю. Шепітько, В. О. Коновалова та ін. виокремлюють три головні групи потерпілих від таких злочинів:

1) власники комп'ютерної системи (79 %);

2) клієнти, що користуються їх послугами (13 %);

3) інші особи (8 %).

При цьому зазначається, що потерпіла сторона, особлива та, що належить до першої групи, доволі часто неохоче повідомляє (або не повідомляє зовсім) правоохоронним органам про злочинні факти у сфері комп'ютерної інформації з наступних причин: через недостатню компетентність правоохоронних органів у розслідуванні цієї категорії злочинів; остраху розкриття в процесі досудового провадження системи безпеки фірми; остраху виявлення власних незаконних дій та ін. Такого роду дії і створюють високий рівень латентності цієї категорії злочинів та істотно ускладнюють процес їх розкриття, розслідування та профілактику [6, с. 525], що ми цілком підтримуємо.

Дійсно, зазначені фактори значно ускладнюють розслідування таких кримінальних проваджень. На нашу думку, перш за все, це пов'язано з тим, що під час розслідування даного виду злочину можуть стати відомі факти, які в подальшому зможуть вплинути на репутацію, ділову діяльність особи, а також відомості щодо таємниці підприємницької діяльності юридичної особи.

З урахуванням цього, для більш дієвого захисту потерпілих від даного виду злочину на законодавчому рівні, наприклад, слід закріпити норму, яка б передбачала, що за заявою фізичної особи або представника юридичної особи судове провадження таких злочинів має здійснюватись в закритому засіданні.

В той же час, підняті проблеми є неостаточні та підлягають окремому комплексному дослідженню.

Список використаних джерел:

1. Дорош М. Як зупинити розквіт кіберзлочинності [Електронний ресурс] / М. Дорош. – Режим доступу: http://osvita.mediasapiens.ua/material/23587.

2. Тиченко З. Союзник кіберзлочинів – анонімність [Електронний ресурс] / Зофія Тиченко // Іменем Закону. – 10.09.2013. – Режим доступу: http://www.imzak.org.ua/articles/article/id/3324.

3. Конвенція про кіберзлочинність : від 23.11.2001 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

4. Комп'ютерна злочинність : навч. посіб. / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – К. : Атіка, 2002. – 240 с.

5. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів / В. Г. Хахановський // Юридичний часопис НАВС. – 2011. – № 1 [Електронний ресурс]. – Режим доступу: http://www.naiau.kiev.ua/chasopis/materials/24.

6. Настільна книга слідчого / М. І. Панова, В. Ю. Шепітько, В. О. Коновалова [та ін.]. – 3-тє вид., переробл. і доповн. – К. : Ін Юре, 2011. – 736 с.

Одержано 17.11.2013

УДК 343.1

Олександр Миколайович КОСИЙ,
здобувач
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ КРИМІНАЛЬНОГО ПЕРЕСЛІДУВАННЯ ОРГАНАМИ ПРОКУРАТУРИ У ПРОТИДІЇ І ЗАПОБІГАННІ КІБЕРЗЛОЧИНАМ

Відзначена річниця вступу в чинну дію нового кримінального процесуального законодавства України 2012 року. Певна кількість новел призвела до наукових дискусій у багатьох напрямах, у тому числі і стосовно кримінального переслідування з боку правоохоронних органів, і зокрема органів прокуратури. Незважаючи на дискусію щодо вказаних питань чинний КПК України визначив окремі досить конкретні положення щодо розглянутого питання. Втім, підтримуючи напрями дискусійних питань слід все ж таки зазначити, що окремі, його положення потребують свого наукового й законодавчого уточнення і удосконалення.

Розглядаючи окремі наукові думки вчених слід зазначити, що М. С. Строгович, В. М. Савицький, М. Л. Шифман, Г. В. Остафійчук зазначали, що функція нагляду несумісна з функцією кримінального переслідування органів прокуратури. Вони наполягають, що ніякі застереження, що прокурор як обвинувач об'єктивно піклується про інтереси захисту не можна брати до уваги. Обвинувачення завжди спрямовано на доведення винності, а нагляд має бути не пов'язаний з обвинуваченням. Ці функції не можуть бути паралельними,

якщо вони здійснюються тією ж самою особою, тобто прокурором.

Г. В. Остафійчук, аналізуючи чинний КПК України все ж таки пропонує окреслити функцію прокурора щодо кримінального переслідування відповідно до ст. 36 КПК України, а саме, що прокурор повинен прийняти заходи щодо забезпечення кримінальної відповідальності підозрюваного, який вчинив кримінальне правопорушення, затвердити обвинувальний акт, або скласти новий обвинувальний акт, направити кримінальне провадження до суду. При цьому прокурор повинен дотримуватися і забезпечувати гарантії прав, свобод людини та громадянина. Прокурор – не тільки обвинувач, але він є стороною в кримінальному процесі. Він повинен додержуватися принципу презумпції невинуватості, змагальності, диспозитивності кримінального процесу. Він наголошує, що з повноважень прокурора слід вважати, що функції правового статусу прокурора слід диференціювати. По-перше, механізм дії процесуального статусу прокурора щодо нагляду за досудовим розслідуванням під час реєстрації заяви про вчинення кримінального правопорушення у Єдиному реєстрі досудового розслідування; при проведенні самого досудового розслідування; викритті та усуненні порушень кримінального процесуального законодавства. По-друге процесуальні повноваження прокурора для прийняття процесуальних рішень, зокрема таких, як «згоден», «затверджую», а також надання слідчому вказівок про проведення розслідування. По-третє державне обвинувачення з моменту складання повідомлення про підозру. По-четверте, включає до себе механізм повноважень, що встановлено ст. 290, 291 КПК України, тобто повноваження прокурора при отриманні обвинувального акта.

Вказані проблеми напряму відносяться й до питань протидії злочинам у сфері використання комп'ютерної техніки, що активно обговорюються практичними працівниками правоохоронних органів, науковцями, досить швидко розвивається практика застосування відповідних норм законодавства про кримінальну відповідальність. На початку незалежності нашої держави, коли змінювалися стереотипи та методи протидії зі злочинністю, народилася ідея створення підрозділу боротьби з кіберзлочинністю. Цей підрозділ було створено у структурі головного управління по боротьбі з

економічною злочинністю. Його діяльність орієнтувалася на два основні напрямки – захист інтелектуальної власності та боротьба з кіберзлочинністю. У другій половині 90-х років Україна піддавалась критиці за велику кількість контрафактної продукції на її території, тому робота у цьому управлінні, в основному, зосереджувалася на захисті прав інтелектуальної власності та боротьбі з незаконним поширенням контрафактної продукції [1].

І хоча дана категорія злочинів поки що нова, проте протидія кіберзлочинцям вимагає відповідної підготовки та технічної оснащеності правоохоронців.

З урахуванням положень нового Кримінального процесуального кодексу України безпосередню участь у розслідуванні даної категорії кримінальних правопорушень забезпечує прокурор, здійснюючи процесуальне керівництво за станом досудового розслідування. Вказане свідчить про спільну роботу працівників органів міліції та прокуратури спрямовану на виявлення причин та умов, що сприяють вчиненню даної категорії кримінальних правопорушень, встановлення осіб причетних до їх вчинення, збирання доказів з метою їх подальшого надання до суду, доказування винуватості та притягнення осіб до визначеної Законом відповідальності за вчиненні ними протиправні діяння.

В науковій літературі найчастіше зустрічаються два терміни: кіберзлочини та комп'ютерні злочини. Оскільки вони використовуються для назви одних і тих самих суспільно-небезпечних діянь, то їх можна вважати синонімами та рівнозначними. У зв'язку з ратифікацією Україною Конвенції про кіберзлочинність 7 вересня 2005 року вважається за доцільне вживати термін кіберзлочини. Поняття «кіберзлочин» молоде і утворено сполученням двох слів: «кібер» і «злочин». Термін «кібер» має на увазі поняття кіберпростору (у літературі частіше зустрічаються терміни «віртуальний простір», «віртуальний світ») та інформаційний простір, що моделюється за допомогою комп'ютера. Тобто кіберзлочини – це суспільно небезпечні діяння, які так чи інакше пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами. Такі злочини характеризуються наступними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, транснаціональною складовою в основному з використанням

інформаційної мережі Інтернет, високим збитком навіть від одиничного злочину [2, с. 134]. Це пов'язано з необхідністю відшукування, фіксування, вилучення та збирання доказів в електронній формі. Також комп'ютерні технології широко використовуються для проведення оперативно-розшукових заходів. Кіберзлочини можна класифікувати на два види: традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету (шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації і т. д.), та нові злочини, що стали можливі завдяки новітнім комп'ютерним технологіям (злочини передбачені Розділом XVI Кримінального кодексу України).

Кіберзлочинність – це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера інформаційний, у якому перебувають відомості про особи, предмети, факти, подіях, явищах і процесах, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [4, с. 32].

Сьогодні в Україні кіберзлочинність регулюють такі нормативно-правові акти: Конвенція про Кіберзлочинність, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Кримінальний Кодекс України та інші.

Однак, на думку експертів, кіберзлочинність не є негайною загрозою для українців. Наша країна в особливому становищі, адже має один із найнижчих у Європі рівнів підключення до Інтернету. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв. За даними НБУ, тільки у 2011 році кількість протиправних операцій за платіжними картами українських банків зросла до 7,6 тис. порівняно з 2,9 тис. роком раніше. Обсяг неправомірно списаних коштів збільшився майже в півтора рази – з 6,3 млн до 9,1 млн грн. І це лише офіційна статистика, до того ж за 2011 рік [5].

Прокуратура, СБУ і МВС опинилися на вістрі війни з «кіберами». На жаль, їхніх зусиль щодо протидії замало. Особливо,

зважаючи на наші українські реалії. Якщо раніше українські програмісти-хакери писали вчинені віруси для злому і розкрадання даних в багатих західних країнах, то тепер у зв'язку з посиленням боротьби американської і європейської влади з комп'ютерними злочинами їхня увага звернулася і на Україну. Так, за оцінками експертів, в останні місяці в управлінні з боротьби з кіберзлочинністю тільки в Києві фіксується до двадцяти випадків крадіжки грошей через клієнт-банк. Суми становлять від 20 тис. до 40 млн грн. Однак подібні факти замовчуються, повідомлень в ЗМІ про них практично немає. Ні потерпілим, ні банкам, ні міліції не вигідний галас навколо того, що відбувається. У ряді випадків бувають ситуації, коли такі шахрайські схеми реалізуються організованими групами, у які входять представники банків та силових структур [6].

Законодавство у сфері захисту інформації, на думку Ю. Омельченка, вимагає доопрацювання. «Потенційно існує ймовірність того, що кіберзлочинність буде виштовхуватися з Європи, то вона буде перебиратися в Україну. Та й уже цей процес відбувається», – зазначив експерт [6]. Слід звернути увагу на те, що все вищевказане потребує не аби яких зусиль правоохоронних органів на вказаному напрямі роботи задля оперативного та якісного реагування на існуючі проблеми.

Важливе значення у вирішені питання кіберзлочинності заслуговує світовий досвід. Так, 09.09.2009 підписано меморандум про співпрацю між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом.

Проаналізувавши вказаний документ можна простежити основні ключові аспекти. України та Королівство Нідерланди в межах своєї компетенції відповідно до законодавства своїх держав будуть здійснювати співробітництво в сфері боротьби з кіберзлочинністю, організованою злочинністю і відмиванням доходів, одержаних злочинним шляхом. Співробітництво в межах цього Меморандуму здійснюється країнами шляхом обміну інформацією і документами стосовно злочинів, пов'язаних з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом, і причетних до них осіб. Країни дотримуючись вимог конфіденційності, обмінюються інформацією про громадян своїх держав,

іноземних громадян та осіб без громадянства, які перебувають під слідством у зв'язку із вчиненням злочинів, пов'язаних з кіберзлочинністю, організованою злочинністю, а також у зв'язку з відмиванням доходів, одержаних злочинним шляхом, оскільки вказані злочини стосуються національних інтересів країн.

Україна та Королівство Нідерланди будуть вживати всіх можливих заходів в межах повноважень, щоб сприяти ефективному і своєчасному виконанню клопотань про правову допомогу у кримінальних справах про кіберзлочинність, організовану злочинність та відмивання доходів, одержаних злочинним шляхом, якщо такі клопотання прийняті компетентними органами країни, яка надала такий запит. У ході виконання вказаних завдань потребує розширення професійних контактів між співробітниками з метою ефективного використання та удосконалення досвіду і обміну інформацією з питань чинного законодавства, зокрема, текстами законодавчих та інших нормативних актів, аналітичними матеріалами і статистичними даними та повідомленнями, що стосуються боротьби з кіберзлочинністю, організованою злочинністю і відмиванням доходів, одержаних злочинним шляхом. Співробітництво в рамках цього Меморандуму здійснюється на підставі запитів про надання інформації. Однак, без попереднього прохання можна надіслати інформацію, яка може допомогти іншій країні, якій вона надається, в порушенні кримінальної справи чи проведенні розслідування.

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

Світовий досвід з вказаного питання потребує не аби якого значення для України. Органи прокуратури України вживають значну кількість заходів, спрямованих на вирішення нагальних проблем кіберзлочинності.

Професійний рівень органів прокуратури в цілому, та кожного співробітника прокуратури особисто, повинен

постійно зростати. Тільки при використанні світового досвіду, національного законодавства, праць вчених, напрацювань практичних працівників, органи прокуратури зможуть забезпечити на належному рівні якісний рівень процесуального керівництва за станом досудового розслідування кримінальних проваджень вказаної категорії злочинів. Втім вказані питання потребують окремого дослідження.

Список використаних джерел:

1. Інтерв'ю з начальником ВБК УМВС України в Сумській області майором міліції Стирковим Є. М. [Електронний ресурс]. – Режим доступу до сайту: http://mvs.gov.ua.

2. Комп'ютерна злочинність : навч. посіб. / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – К. : Атіка, 2002. – 240 с.

3. Кримінальний кодекс України : закон України від 05.04.2001 № 2341-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14.

4. Біленчук Д. П. Кібрешахраї – хто вони? / Д. П. Біленчук // Міліція України. – 1999. – №7–8. – С. 32–34.

5. Кіберзлочинність можна зупинити тільки разом // Україна: бізнес-ревю. – 2013. – № 5–6.

6. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ / В. Прохоренко // Економічна правда. – 26 лют. 2013 р.

7. Меморандум про співпрацю між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/528_031.

Одержано 14.11.2013

УДК 343.1

Олена Василівна МАРТОВИЦЬКА,
здобувач
Харківського національного університету внутрішніх справ

УДОСКОНАЛЕННЯ ПРОЦЕСУАЛЬНОГО І КРИМІНАЛЬНО-ПРАВОВОГО ЗАХИСТУ ОСІБ ТА ДЕРЖАВНИХ УСТАНОВ ВІД КІБЕРЗЛОЧИНІВ

На протязі останнього року, після вступу в чинну дію КПК України, як серед працівників органів внутрішніх справ, так і серед науковців – юристів всіх рівнів одним з найбільш дискусійних питань є проблемні питання щодо протидії і запобігання кіберзлочинності, та впровадження нового Кримінального процесуального кодексу України у

практичну діяльність правоохоронних органів і зокрема ОВС. Крім того, поширеною дискусією є питання з нового Кримінального процесуального кодексу України, щодо запровадження Єдиного реєстру досудових розслідувань (далі – ЄРДР). Але оскільки ЄРДР, з одного боку це створена за допомогою автоматизованої системи електронна база даних, порядок формування та ведення якої регулюється законом і нормативними актами правоохоронних органів, то з іншого боку це процесуальний інструмент усього слідства України, адже відповідно до ч. 2 ст. 214 КПК України факт внесення відомостей до Єдиного реєстру прирівнюється до рішення про початок досудового розслідування, що є гарантією щодо забезпечення особі, що звернулась у підрозділи досудового розслідування щодо повного, об'єктивного і неупередженого розслідування кримінального правопорушення вчиненого проти неї і це в повній мірі стосується й тих, що вчинені із застосуванням новітніх інформаційних технологій тощо.

На нашу думку, проблемою у функціонуванні ЄРДР на перспективу перш за все може стати незаконне втручання в його роботу ззовні, тобто так звані «хакерські атаки», тому що ні для кого не є таємницею, що перша «хакерська атака» на Пентагон була вчинена ще у середині 1970-х років, і це було зроблено із хуліганських мотивів, а на сьогодні ЄРДР – це автоматизована комп'ютерна система, яка напряму пов'язана із функціонуванням великого державного апарату, зокрема слідчого та правоохоронних органів у цілому, оскільки вся інформація ЄРДР концентрується в Генеральній прокуратурі України. Проблема кіберзлочинності у всьому світі є дійсно досить важливою проблемою, що підтверджується постійним зростанням кількості особового складу спеціальних підрозділів по боротьбі з кіберзлочинністю і збільшення країн, якими було ратифіковано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 (більш відомої в Україні під назвою «Конвенція про кіберзлочинність»). Крім того, про збільшення загрози автоматизованим комп'ютерним системам, що обслуговують підприємства, установи та організації усіх форм власності свідчить і те, що за даними Nua Internet Surveys кількість користувачів глобальної мережі Інтернет з 80 тисяч у 1988 році зросла до 2,7 мільярдів на кінець 2013 року.

У розділі XVIII Кримінального кодексу України передбачено статтю 376-1 «Незаконне втручання в роботу автоматизованої системи документообігу суду», але немає спеціальної статті, яка б передбачала настання кримінальної відповідальності за незаконне втручання в роботу автоматизованої системи документообігу конкретно слідчих і правоохоронних підрозділів, тобто в роботу ЄРДР. Ймовірно, що у випадку незаконного втручання в роботу такої автоматизованої системи, як ЄРДР, дії злочинця необхідно буде кваліфікувати за відповідною додатково введеною новою статтею розділу XVI Кримінального кодексу України Зокрема ми вважаємо, що більш доречним було б введення в законодавство про кримінальну відповідальність України саме спеціальної статті, наприклад такої, як: стаття 376-2 «Незаконне втручання в роботу автоматизованої системи документообігу слідчих і правоохоронних органів».

За дослідженням окремих вчених виникають проблемні питання щодо подальшого кримінального провадження щодо ст. 361-2 КК України «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або носіях такої інформації», що вилучена із підслідності служби безпеки України згідно чинного КПК України, але охорона інформації з обмеженим доступом є одним з основних елементів забезпечення контр розвідувального режиму в державі, а сама інформація з обмеженим доступом є першочерговим об'єктом розвідувальних спрямувань з боку іноземних спецслужб, організацій та осіб. Крім того, в залежності від обставин вчинення кримінального правопорушення, злочинні дії можуть містити ознаки інших статей КК України, зокрема статей 111, 114, 328, 330, 442 КК, що залишилися у підслідності СБУ України. У зв'язку з викладеним слід підтримати позицію О. О. Юхна і Д. О. Максимуса та інших вчених і практиків щодо доцільності введення в ст. 216 КПК України змін з метою повернення ст. 361-2 КК України до підслідності органів безпеки України. Крім цього, до вже вказаного розділу XVI КК України ми також підтримуємо пропозиції вказаних та інших науковців про доцільність додаткового введення ст. 361-3 КК України щодо встановлення кримінальної відповідальності за «Несанкціоноване втручання в роботу державних

електронних інформаційних ресурсів або критичної інформаційної інфраструктури держави» та ст. 362-1 КК України за «Несанкціоновані дії з інформацією яка обробюється в державних електронних інформаційних ресурсах або технологічною інформацією в критичній інформаційній інфраструктурі держави, вчинені особою, яка має право доступу до неї».

Втім, підняті питання не є остаточними, підлягають окремому дослідженню або науковому вивченню.

Прошу учасників наступної Міжнародної науково-практичної конференції прийняти участь у обговорені наданих пропозицій.

Список використаних джерел:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/254к/96-вр.

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К. : Юрінком Інтер, 2012. – 608 с.

3. Кіберзлочинність в Україні: перспективи протидії [Електронний ресурс] / Комітет протидії корупції та організованій злочинності. – Режим доступу: http://kpk.org.ua/2007/02/05/kberzlochinnst_v_ukran_perspektivi_protid.html.

4. Максимус Д. О. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій : навч. посіб. / Д. О. Максимус, О. О. Юхно. – Х. : ХНУВС, 2013. – 102 с.

Одержано 13.11.2013

УДК 343.98

Оксана Іванівна ТРИГУБЧАК,
здобувач
Харківського національного університету внутрішніх справ

СТРУКТУРА ТА ЗМІСТ ТИПОВОЇ МЕТОДИКИ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Вчинення кіберзлочинів супроводжується виникненням специфічних слідів, які в криміналістичній літературі називають «віртуальними», «цифровими», «електронними» та ін. Це обумовлене тим, що вказані сліди є нетрадиційними, візуально не сприймаються, а виявляються в результаті проведення експертних досліджень. Експертиза, за допомогою якої встановлюються сліди кіберзлочинів іменується в літературі комп'ютерно-технічною. Згідно з Інструкцією Міністерства

юстиції України про призначення та проведення судових експертиз відповідні дослідження здійснюються в межах експертизи комп'ютерної техніки і програмних продуктів та експертизи телекомунікаційних систем та засобів.

Об'єктами дослідження є носії комп'ютерної інформації, мережі і їх складові частини, мобільні термінали та ін. Очевидно, що розвиток комп'ютерної техніки призведе до появи нових носіїв інформації і відповідно до нових видів комп'ютерно-технічної експертизи.

Розвиток будь-якій судової експертизи пов'язаний із розробкою типових методик дослідження. Методика експертного дослідження – одне із суттєвих понять теорії судових експертиз. Особливо, це питання набуває актуальності на сучасному етапі розвитку судової експертизи в Україні у світлі судової реформи, зокрема прийняття нового Кримінального процесуального кодексу, атестації та державної реєстрації експертних методик тощо.

У спеціальній літературі існують різні тлумачення щодо поняття методики експертного дослідження. Загальним для існуючих в літературі визначень експертної методики є вказівка на те, що змістом будь-якої методики є використання сукупності (системи) методів дослідження. Сама ж методика являє собою програму рішення експертного завдання (або певного кола завдань), що складається з послідовного ряду операцій, дій, спрямованих на вивчення ознак, пізнання властивостей і зв'язків досліджуваних об'єктів. Іншими словами, система методів експертного дослідження виражає, реалізує себе в програмі рішення експертного завдання (завдань) у вигляді послідовних розумових і фізичних операцій.

Таке розуміння характеризує експертну методику насамперед як систему приписів, тобто систему вказівок. Вказівки можуть мати категоричний або альтернативний характер (рекомендаційний, необов'язковий), що залежить від альтернативності вибору методів та засобів, що рекомендуються, і послідовності їх застосування. Категоричні приписи утворюють жорстку систему дій, альтернативні надають можливість вибору з декількох програм. Для нестандартних експертних ситуацій можуть бути створені евристичні методики дослідження.

Для атестації та державної реєстрації методик комп'ютерно-технічної експертизи важливе значення має їх зміст та

структура. В цьому сенсі методика розглядається як документ, в якому прописаний алгоритм, послідовність операцій дослідника. Це – нормативне виробничо-практичне видання (видання норм, правил і вимог з конкретних сфер виробничо-практичної діяльності), що регламентує послідовність застосування системи методів і засобів, а також правил при виконанні певної роботи.

Типова методика повинна відбивати всі стадії (етапи) експертного дослідження. В літературі відокремлюють від чотирьох до шести стадій експертного дослідження. Проведений аналіз сучасного теоретичного та практичного досвіду у галузі судової експертизи дозволяє визначити наступні стадії експертної методики:

1) попереднє дослідження;

2) роздільне дослідження;

3) експертний експеримент;

4) порівняльне дослідження;

5) оцінка результатів проведеного дослідження та формулювання висновків;

6) оформлення ходу та результатів експертного дослідження у висновку експерта.

Залежно від того, які експертні завдання (ідентифікаційні, діагностичні, класифікаційні, ситуалогічні) вирішуються, стадії експертного експерименту, порівняльного дослідження можуть бути відсутніми. Крім того, стадія експертного експерименту, при необхідності її проведення, може слідувати за стадією роздільного дослідження або за стадією порівняльного дослідження.

Експертна методика повинна складатися із таких блоків:

1. Загальний. У загальній частині експертної методики доречні такі її змістовні елементи: назва задача (з варіантами формулювань питань, якими реалізується ця задача) та система підзадач; опис сутності методики (чи принципу її дії); опис об'єкта дослідження; опис ознак досліджуваного об'єкта.

2. Технічний. В технічній частині експертної методики мають бути вказані такі змістовні елементи: перелік комплексу необхідних науково-технічних засобів, іншого обладнання, а також вимірювальних пристроїв; описи умов застосування методів; перелік необхідних витратних матеріалів та речовин; дані про порівняльні зразки; довідкові дані, в тому числі, перелік основної та додаткової літератури; вимоги щодо

необхідного рівня підготовки суб'єкта (судового експерта); аспекти вивчення матеріалів справи; коло спеціалістів суміжних спеціальностей.

3. Операційний. В операційний частині експертної методики міститься: опис оптимальної послідовності дій суб'єкта (експерта) в процесі дослідження з метою отримання результату.

4. Документальний. У документальній частині даються: рекомендації щодо оформлення висновку експерта чи висновку експертного дослідження; рекомендації щодо викладення в даному документі проміжних та кінцевих результатів; особливості формулювання висновків; рекомендації щодо оцінки висновків слідчим та судом.

Одержано 11.11.2013

УДК 343.1

Римма Володимирівна СУВОРОВА,
слухач магістратури
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

У зв'язку із розвитком сучасних інформаційних технологій, а також рівня інформаційної обізнаності злочинного елементу, все більше зростає актуальність протидії кіберзлочинам. Поняття кіберзлочину є поки незвичним для правоохоронних органів, проте злочинні дії, в яких використовується глобальна комп'ютерна мережа Internet, містять в собі велику суспільну небезпеку.

Кіберзлочини (кібернетичні злочини) пропонується розглядати як: а) злочини у кіберпросторі; б) злочини, пов'язані з протиправним використанням кібернетичних комп'ютерних систем. При цьому, під кіберпростором (кібернетичним простором) розуміється штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене у результаті функціонування кібернетичних комп'ютерних систем управління та обробки інформації, реалізованих на основі комп'ютерних мереж [1].

Неможливо уявити досудове розслідування кіберзлочинів без застосування оперативно-розшукових заходів. Правову

основу боротьби з кіберзлочинами становлять Конституція України, Кримінальний та Кримінально-процесуальний кодекси України, інші законодавчі та підзаконні акти, а також міжнародно-правові угоди і договори, учасницею яких є Україна.

Метою оперативно-розшукового забезпечення досудового розслідування злочинів у сфері кіберзлочинності є: здобуття оперативної інформації в інтересах розкриття та розслідування злочинів, виявлення й оперативне документування всіх епізодів злочинної діяльності особи (групи осіб), стосовно якої проводяться оперативно-розшукові заходи, легалізація матеріалів, отриманих в результаті оперативно-розшукової діяльності, захист осіб, які беруть участь у кримінальному провадженні, членів їх сімей та близьких родичів, якщо виникає реальна загроза їх життю та здоров'ю, житлу, майну, а також відповідних працівників правоохоронних органів та близьких родичів у зв'язку із службовою діяльністю цих працівників, ужиття заходів щодо усунення причин та умов, що сприяли вчиненню злочинів.

Аналіз повноважень підрозділів, які здійснюють оперативно-розшукову діяльність (ст. 8 Закону України від 18 лютого 1992 р. «Про оперативно-розшукову діяльність») дозволяє зробити висновок про їх недостатність для ефективної протидії злочинності у кіберпросторі. Як вбачається, за наявності відповідних знань та програмно-технічних засобів працівники оперативних підрозділів можуть у кіберпросторі здійснювати такі заходи: опитувати осіб за їх згодою, використовувати їх добровільну допомогу; проводити контрольну та оперативну закупівлю та постачання товарів, предметів та речовин, у тому числі заборонених для обігу, у фізичних та юридичних осіб незалежно від форм власності з метою виявлення та документування фактів протиправних діянь; знімати інформацію з каналів зв'язку, застосовувати інші технічні засоби отримання інформації; контролювати шляхом відбору за окремими ознаками телеграфно-поштові відправлення (за умови віднесення до поштових відправлень повідомлень електрозв'язку, у тому числі електронних листів) [2].

Здійснення оперативно-розшукових заходів у сфері кіберзлочинності потребує більш розширеного та оновленого підходу, так на думку автора слід приділити увагу дослідженням засобів та методів ОРД. До засобів ОРД, крім «класичних»,

слід віднести низку додаткових засобів, які є новітніми й використовуються в ОРД нещодавно або ж застосовуються тривалий час, але з різних причин перебувають поза увагою дослідників. До таких засобів належать, зокрема: спеціальні комп'ютерні програми, засоби маскування та імітації, неоперативні обліки, підприємства та організації, створені з метою конспірації, спеціально навчені тварини тощо. Новітні методи ОРД ґрунтуються на використанні сучасних інформаційно-телекомунікаційних технологій. Вони потребують ретельного дослідження; їх наукове опрацювання є необхідною умовою розроблення новітніх методик отримання та аналізу оперативно-розшукової інформації оперативними підрозділами, які працюватимуть в умовах розвинутого інформаційного суспільства [3, с. 16].

Крім того, для якісного розслідування кіберзлочинності необхідно приділити увагу взаємодії оперативних підрозділів та слідчого при їх розслідуванні.

У практиці взаємодії слідчого й органу дізнання за оперативно-розшукового забезпечення досудового розслідування злочинів у сфері кіберзлочинності широко застосовуваними є такі організаційні (непроцесуальні) форми: спільне планування слідчих дій та оперативно-розшукових заходів; обмін інформацією за повідомленнями про вчинені злочини та ті, що готуються, а також з інших питань слідчої й оперативно-розшукової діяльності; координація слідчих дій й оперативно-розшукових заходів; консультації; спільний аналіз причин та умов, які сприяли вчиненню злочинів, тощо [4, с. 169].

Оперативно-розшукова діяльність спрямована не лише на розслідування кіберзлочинів, а й на їх профілактику.

Профілактикою у таких видах злочину слід розуміти певний метод ОРД, оснований на комплексі оперативно-розшукових (оперативно-профілактичних) заходів, спрямованих на недопущення вчинення кіберзлочину. При цьому, слід виділити такі характерні риси оперативно-розшукової профілактики кіберзлочинів: необхідність здійснення оперативно-профілактичних заходів, окрім реального середовища, у кіберпросторі (віртуальному середовищі); взаємопов'язаність цих заходів у реальному та віртуальному середовищах за метою, часом, змістом тощо [1].

Крім того, необхідно виділити, що актуальним залишається питання щодо недостатнього кадрового забезпечення

практичних органів кваліфікованими фахівцями у сфері боротьби з кіберзлочинністю. Удосконалення освіти, розробка навчальних програм, формування та розширення спеціальних факультетів по підготовці фахівців по боротьбі з кіберзлочинністю, що потребує матеріального забезпечення з боку держави, стало б шляхом вирішення даного питання.

Проаналізувавши викладене, можна зробити висновок, що дедалі більше зростає актуальність боротьби з кіберзлочинами, що є наслідком розвитку сучасних інформаційних технологій. При цьому, розслідування таких злочинів потребує чіткої організації оперативних підрозділів та їх взаємодії з слідчими органами. Необхідно приділяти увагу засобам, методам та тактиці проведення оперативно-розшукових заходів при розслідуванні таких злочинів. Важливим є питання щодо підготовки оперативних працівників, із наявністю певних наукових, технічних та інших спеціальних знань для розуміння сутності інформаційних процесів у кіберпросторі та виявлення ознак злочинів.

Список використаних джерел:

1. Оперативно-розшукова профілактика кіберзлочинів: попередження злочинів суб'єктами оперативно-розшукової діяльності [Електронний ресурс] / В. П. Шеломенцев. – Режим доступу: http://zavantag.com/docs/html.

2. Федотова О. А. Щодо поняття поняття злочинів у сфері комп'ютерних технологій [Електронний ресурс] / О. А. Федотова // Економіка, фінанси, право. – 2010. – № 4. – С. 37–39. – Режим доступу до сайту: http://inter.criminologi.onua.ua.

3. Орлов Ю. Ю. Актуальні напрями наукових досліджень у сфері оперативно-розшукової діяльності / Ю. Ю. Орлов // Науковий вісник національної академії внутрішніх справ. – 2013. – № 3. – С. 12–19.

4. Деревягін О. О. Оперативно-розшукове забезпечення розслідування злочинів у сфері кіберзлочинів / О. О. Деревягін // Проблеми правознавства та правоохоронної діяльності. – 2012. – № 2. – С. 167–173.

Одержано 19.11.2013

УДК 343.98

Юлія Олегівна ШУЛЬЖЕНКО,
слухач магістратури
Харківського національного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ВСТАНОВЛЕННЯ ЧАСУ НЕПРАВОМІРНОГО ДОСТУПУ ДО КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

XXI століття відкрило нову еру панування комп'ютерів та обчислювальної техніки. Майже всі процеси на сучасному етапі не можуть існувати без машин та програмного забезпечення. Розвиток науково-технічного прогресу суттєво скоротив зусилля людини для виконання завдань. Проте там, де зароджується щось позитивне, паралельно з ним виникає й негатив. Так, удосконалення комп'ютерних технологій призвело до виникнення нових видів злочинів, зокрема й неправомірний доступ до комп'ютерної інформації. Вчиняються вони новим типом злочинців, названих «кіберзлочинцями», які підходять до планування та вчинення злочину з особливим ентузіазмом, продумуючи кожен крок. При розслідуванні кримінальних проваджень по даній категорії злочинів необхідно встановити факт самого неправомірного доступу до комп'ютерної інформації, місце, час та способи несанкціонованого доступу. Так, особливих зусиль вимагає встановлення саме моменту, коли ж було вчинено правопорушення, так як він міг і не співпадати, наприклад з безпосереднім запуском програми для доступу, наприклад програми віддаленого доступу TeamViewer. Тому розробка рекомендації щодо комплексу слідчих (розшукових) дій по встановленню точного часу несанкціонованого доступу до охоронюваної законом комп'ютерної інформації є одним із важливих завдань криміналістичної науки.

Неправомірним слід визнати доступ в закриту інформаційну систему особи, яка не є законним користувачем або не має дозволу для роботи з даною інформацією. При розслідуванні даного виду злочинів під час допиту підозрюваного важливим питанням є з'ясування місця його знаходження під час несанкціонованого доступу. А, отже, під час огляду комп'ютерної техніки потрібно належним чином зафіксувати точний час нелегального втручання в роботу машини.

За допомогою комп'ютерних програм загальносистемного призначення можна встановити поточний час роботи комп'ютерної системи. Це дозволяє за відповідною командою вивести на екран дисплея інформацію про день, години, хвилини та секунди виконання тієї або іншої операції. При вході до системи чи мережі (в тому числі й несанкціонованому) час роботи на комп'ютері будь-якого користувача та час виконання конкретної операції автоматично фіксуються в оперативній пам'яті та відображаються, як правило, у вихідних даних на дисплеї, лістингу, дискеті чи вінчестері.

Враховуючи дане, час несанкціонованого доступу можна встановити шляхом огляду комп'ютера, роздруківок чи дисків. Його доцільно виконувати за участю фахівця в галузі комп'ютерної техніки та технологій – програміста-математика. Необережне поводження або дії недосвідченої особи можуть випадково знищити інформацію, яка знаходиться в оперативній пам'яті комп'ютера або на диску.

Час неправомірного доступу до комп'ютерної системи можна встановити також шляхом опитування свідків з числа співробітників організації, де було встановлено цей факт. При цьому слід з'ясувати, коли саме кожен з них працював на комп'ютері, якщо це не було зафіксовано автоматично або в журналі обліку роботи на комп'ютері.

Важливим є встановлення не лише часу безпосереднього доступу до охоронюваної інформації, а й часу необхідного правопорушнику для проникнення в приміщення, закриту зону, підключення до комп'ютерної мережі, модифікації та копіювання комп'ютерної інформації. Для встановлення вказаних обставин доцільним буде проведення слідчого експерименту, результати якого визначать скільки часу потрібно було правопорушнику для того, щоб проникнути в приміщення, потрапити в закриті зони, ввімкнути програмне забезпечення, подолати паролі та отримати доступ до комп'ютерної інформації.

Так, в першу чергу необхідно провести огляд місця події з залученням спеціаліста. При цьому, використовуючи програми загальносистемного призначення, можна визначити час підключення до програмного забезпечення, час несанкціонованого доступу до комп'ютерної інформації, момент її копіювання, модифікації. Далі доцільним є проведення допитів, особливо осіб, які безпосередньо працюють з цією

комп'ютерною інформацією, щоб визначитися в який момент часу вони працювали з інформацією, чи є паролі, чи важко отримати доступ до інформації, скільки часу на це можливо витратити. Суттєву допомогу розслідуванню може надати проведення слідчого експерименту, результати якого визначать скільки часу потрібно було правопорушникові для того, щоб проникнути в приміщення, потрапити в закриті зони, ввімкнути програмне забезпечення, подолати паролі та проникнути до комп'ютерної інформації.

Одержано 18.11.2013

УДК 343.98

Дмитро Олександрович ЧЕРНИШ,
курсант
Харківського національного університету внутрішніх справ;
науковий керівник – викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ Владлена Олександрівна Приходько

ОСОБЛИВОСТІ МЕХАНІЗМУ ВЧИНЕННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З ВИКРАДЕННЯМ КОШТІВ ІЗ КРЕДИТНИХ КАРТОК

В останній третині XX століття у різні сфери людської діяльності увійшли комп'ютери та інформаційні технології, що обумовило появу нових суспільно-небезпечних діянь – кіберзлочинів. Одним із видів таких злочинів проти власності є крадіжки коштів з кредитних карток. Ці злочини є відносно молодими на території України ніж в країнах Європи чи Америки, що пояснюється відносно недавнім поширенням кредитних карток та системи безготівкової оплати в Україні.

Механізм вчинення крадіжок коштів з кредитних карток можна поділити на три етапи, кожен з яких характеризується певними виконавцями, діями, часом і знаряддями вчинення цих дій.

На першому етапі особа або декілька осіб, що виконують функції організатора, розроблюють план злочинних дій, визначаються з колом співучасників, враховують можливі ризики, пов'язані з діяльністю правоохоронних органів, банківських установ, пересічних громадян. Організаторами також вирішуються питання з приводу забезпечення засобами

зв'язку широкого кола співучасників з метою запобігання безпосереднього контакту одного з одним, а також технічними засобами, що виступають знаряддям вчинення крадіжки (скіммером, міні камерою або накладкою на клавіатуру), для кожного етапу злочину. Особи, які виконують функції організаторів, можуть володіти знаннями в сфері комп'ютерних технологій, діяльності банківських установ та правоохоронних органів, не виключається їх обізнаність в юриспруденції. Вони дистанційно керують діями інших учасників злочину, виконуючи при цьому основну роль, і саме тому цих осіб найважче встановити, а тим паче притягти до кримінальної відповідальності, оскільки, в багатьох випадках, співучасникам невідомі анкетні дані організаторів.

Другий етап характеризується діями співучасників з одержання необхідних даних, а саме магнітного коду кредитної картки та Pin-коду для виготовлення дублікатів кредитних карток. Для того, щоб одержати таку інформацію злочинцям необхідно встановити на банкомати відповідне обладнання – скіммер, що зчитує магнітний код, та міні камеру або накладку на клавіатуру для запису Pin-коду.

Виконавцями зазначених дій на цьому етапі, як правило, є фізично розвинуті молоді особи чоловічої статі, які володіють мінімальними навичками в сфері комп'ютерних технологій, використанні злочинного обладнання. Такі особи піддаються найбільшому ризику викриття та затримання, а тому можуть носити при собі засоби для здійснення опору. Також ними можуть бути особи, що раніше притягалися до кримінальної відповідальності, особи, які не мають постійного місця роботи.

Отримавши необхідне обладнання та інструкції з його використання, злочинці обирають банкомат для встановлення скіммера. При цьому вони враховують вид банкомату (частіше використовують зовнішні ніж внутрішні), рівень його захищеності (кількість камер у банкоматі, наявність антискіммінгових накладок), місце його розташування (переваги надаються тим, що знаходяться в курортних районах, поблизу елітних готелів та закладів розваг), наявність камер на прилеглій території. Після встановлення такого обладнання в обов'язковому порядку злочинці ведуть спостереження за даним банкоматом, з метою запобігання вилученню обладнання сторонніми особами, як правило звичайними громадянами.

Завершується даний етап пересиланням отриманої інформації (магнітного коду та Pin-коду) організатору чи особі, що виготовляє дублікати кредитних карток.

Третій етап включає в себе виготовлення дублікатів кредитних карток та безпосереднє зняття коштів, тобто – отримання реальних грошей.

Виготовляють дублікати або організатори з подальшим пересиланням особам, що будуть знімати кошти, або ж безпосередньо ці особи. Для виготовлення дублікатів злочинцям необхідне обладнання для запису магнітного коду на пусту кредитну картку, так званий «білий пластик». З цією метою ними може бути використане обладнання типу MSR-350, призначене для виготовлення дисконтних карт, яке, до речі, є у вільному продажі.

Чималих підготовчих дій потребує зняття грошей з банкоматів і залежить від кількості матеріалу (кредитних карток, обсягу номінальної вартості коштів, що знаходяться на рахунках), співучасників та банкоматів з яких одночасно будуть зніматися кошти, а також рівня підготовки служб безпеки банківських установ. До підготовчих заходів по зняттю коштів також належить обрання банкоматів з яких вони в подальшому будуть зніматися, засобів маскування (наклейки на камери, сонцезахисні окуляри). Зняття коштів відбувається, як правило, пізно ввечері або близько 4-5 години ранку, що пояснюється відсутністю небажаних свідків.

Після викрадення грошей з рахунків громадян виконавці надсилають відповідну частину організаторові (як правило більше половини), а організатор, в свою чергу, відправляє частку іншим співучасникам. Гроші пересилаються через різноманітні платіжні системи, як правило Webmoney.

На підставі вищевикладеного можна дійти наступних висновків: злочини, пов'язані із викраденням коштів з кредитних карток є доволі складними та потребують великих зусиль при розслідуванні; вони вчиняються як у простій співучасті, так і злочинними організаціями з великою кількістю злочинців; вчиняються у декілька етапів, кожному з яких притаманні певні виконавці, спеціальні технічні засоби.

Одержано 13.11.2013

УДК 343.98

Анастасія Сергіївна ШАПОВАЛ,
курсант
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ШАХРАЙСТВ З БАНКІВСЬКИМИ КАРТКАМИ В МЕРЕЖІ ІНТЕРНЕТ

На сучасному етапі розвитку українського суспільства банківські пластикові картки впевнено займають одне з головних місць в системі фінансово-економічних відносин громадян. Проте разом з перевагами використання даного засобу електронного розрахунку або зберігання грошового капіталу, пересічний громадянин може стикнутися з деякими проблемними ситуаціями, що можуть загрожувати його економічному добробуту. Однією з таких проблем є шахрайство з використанням віртуального електронного простору (кіберпростору), коли зловмисник з одного боку використовує конфіденційні реквізити електронних платіжних карток для особистого збагачення, а з іншого використовує пластикові електронні картки для отримання коштів, які були зараховані на рахунок від довірливих громадян.

Статистика МВС України свідчить про те, що об'єм даних злочинів в загальній кількості зареєстрованих злочинів становить 7,6 %. Матеріальна шкода, яку зазнали потерпілі від даного виду шахрайства за 2 роки становить приблизно 116 млн грн [1].

Взагалі-то, способів шахрайства з використанням пластикових карт існує велика кількість. Це зумовлено цілою чергою чинників, що сприяють поширенню шахрайств, наприклад в сфері благодійності до них слід віднести: а) легкий доступ до електронної мережі Інтернет в яких розміщуються оголошення про надання допомоги; б) шахрайство не вимагає спеціальної освіти, потрібні лише елементарні знання роботи з банківськими картками та мережею Інтернет; в) особа, що вчиняє шахрайські дії залишається невідомою для потерпілої особи; г) після вчинення даного злочину залишаються специфічні сліди за якими складно встановити конкретну особу злочинця.

Предметом злочину є гроші, які знаходяться на рахунку платіжної картки потерпілої особи, якою може бути будь яка

особа, котра розміщує оголошення про необхідність отримання благодійної допомоги для вирішення своїх особистих або проблем інших осіб (рідних тощо).

Щодо особи злочинця, можна зазначити наступне – злочинцями виявляються переважно безробітні, які були раніше засуджені за корисливі злочини. Морально-етичні показники таких осіб дістали примітивного розвитку. Жадібність та потяг до легкого збагачення домінують над загальнолюдськими цінностями доброти, самопожертви, співчуття тощо. Вік шахрая в більшості випадків становить від 16 до 40 років. При цьому чоловіки виступають суб'єктами даного виду шахрайств в більшості випадків (70 %). Для вчинення злочину зловмисники розраховують на кмітливість та знання людського психології.

Нерідко, для проведення шахрайських дій злочинці користуються консультаціями з боку працівників банку. Дана консультація має своєю метою отримати інформацію, щодо того яким чином можна змінити пароль картки та які реквізити для цього потрібні (ідентифікаційний код, номер телефону, паспорт тощо); який необхідно провести алгоритм дій щоб відкрити нову банківську картку та яким чином відбувається перерахунок коштів з картки на картку.

Розглянемо спосіб вчинення злочину за допомогою системи «Приват-24» на конкретному прикладі. Спосіб вчинення злочину полягає у наступному: зловмисник реалізуючи свій злочинний задум, під час телефонної розмови із потерпілим під приводом надання матеріальної допомоги на лікування, отримує інформацію про номер картки, телефону до якого прив'язана картка, ідентифікаційний код та пароль, надісланий банком у вигляді текстового смс-повідомлення. Внаслідок цього отримана конфіденційна інформація дає можливість здійснювати керування рахунками потерпілої особи від її імені в системі розрахунків «Приват24». Гроші шахрай перераховує із рахунків осіб, відшуканих ним в соціальних оголошеннях, наступним чином: за допомогою конфіденційної інформації, яку отримав від потерпілої заходить до системи обирає операцію по зміні паролю, після чого система «Приват-24» відправляє смс-повідомлення у вигляді 8 цифр на номер телефону потерпілого. Зателефонувавши до власника карти, зловмисник отримує 8 цифр, які надійшли на телефон потерпілого і змінює пароль картки на новий і цим самим

отримує змогу перераховувати кошти на підшукані заздалегідь картки [2].

Сліди від даного виду шахрайства є специфічними і бувають двох видів. До першого виду належать ідеальні сліди, які залишаються в пам'яті людини і мають вигляд телефонних розмов із шахраєм. До другого виду відносяться матеріальні сліди – це безпосередньо записи шахраєм номерів телефонів, карток потерпілих, а також створення злочинцем нових карток для переміщення на них коштів отриманих злочинним шляхом.

Свідками стають особи з близького кола оточення злочинця, ними можуть бути сусіди, друзі, співмешканці в яких шахрай може брати банківську картку для пересилання на них грошей потерпілих.

Для того щоб зменшити кількість вчинених злочинів за допомогою банківських карток потрібно – підвищити ступінь захисту доступу до банківських карток, а також проводити профілактичні бесіди з особами, які мають у своєму володінні банківські картки.

Список використаних джерел:

1. Стан та структура злочинності в Україні України / Міністерство внутрішніх справ України [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/index.

2. Вирок Таращанського районного суду Київської області від 06.09.2013 : спр. № 379/1357/13-к [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/33328487.

Одержано 15.11.2013

УДК 343.101

Олексій Олександрович ДВОЙНІКОВ,
ад'юнкт
Харківського національного університету внутрішніх справ

КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНІ ОСОБЛИВОСТІ ВСТАНОВЛЕННЯ ОСОБИ, ЯКА ВЧИНИЛА ЗЛОЧИН ЗА ДОПОМОГОЮ ІНТЕРНЕТ-САЙТУ

В період глобалізації швидкий розвиток інформаційних технологій і нових систем телекомунікацій та комп'ютерних мереж супроводжується зловживаннями цими технологіями із злочинною метою. Тому набуває пріоритетного значення вдосконалення кримінального процесуального законодавства,

яке регулює здійснення досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також інших видів злочинів, які вчиняються за допомогою глобальної мережі Інтернет.

Інтернет утворює глобальний інформаційний простір, слугує фізичною основою доступу до різноманітної електронної інформації логічно взаємопов'язаної на основі електронних посилань (адресації).

Здебільшого електронна інформація мережі Інтернет надається користувачу у вигляді веб-сторінок, які складаються із окремих електронних документів, що містять інформацію у вигляді тексту, графіки, звуку, відео, тривимірних об'єктів, електронних посилань та інших інформаційних об'єктів і можуть бути переглянуті з допомогою спеціальних комп'ютерних програм – веб-переглядачів (браузерів: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera тощо).

Сукупність веб-сторінок, об'єднаних за змістом і навігацією, доступ до комп'ютерного перегляду яких надається за визначеною мережевою адресою (адресами), називається веб-сайтом. Інформація, що є доступною у мережі Інтернет, у тому числі й та, що міститься на веб-сайтах, фізично розміщена на комп'ютерному обладнанні, об'єднаному каналами зв'язку з цією мережею, і кожне таке обладнання має IP-адресу – ідентифікатор (унікальний номер, який складається з набору чотирьох 8-бітних чисел), що використовується для адресації комп'ютерів у мережі.

Протиправна діяльність на веб-сайтах виражається, в основному, шляхом надання публічного доступу на сайтах інформації, поширення якої заборонено (наприклад, інформації, що пропагує порнографію, культ насильства і жорстокості, наркоманію, токсикоманію, анти суспільну поведінку та ін.), та небажаної інформації для неповнолітніх (жорстокі ігри, онлайн-казино, сайти, що пропагують насильство та ін.).

В Україні діяльність, спрямована на поширення більшості вказаної інформації, визнається злочинною, наприклад, ст. 300 КК України «Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію»,

ст. 301 КК України «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів».

Специфіка протиправної діяльності на веб-сайтах обумовлює специфіку досудового розслідування та прийняття процесуальних рішень за його результатами.

Збирання та фіксування правопорушення в мережі Інтернет потребує від працівників ОВС, зокрема слідчих і оперативних працівників використання наукових, технічних та інших спеціальних знань в галузі сучасних новітніх технологій, а також відповідного ліцензійного програмно-технічного забезпечення. Під час фіксування готуються такі документи, що підтверджують факт знаходження протиправного контенту на сайті: 1) рапорт (лист) працівника органів внутрішніх справ про виявлення та встановлення наявності знаходження протиправної інформації на сайті; 2) протокол зі скріншотами (копії сторінки сайту з екрана), що підтверджує наявність протиправної інформації на сайті; 3) документ (файл) для перегляду сторінки сайту в режимі он-лайн; 4) додається посилання на сторінку сайту у каталозі обраного в Microsoft Internet Explorer; 5) створюється копія сторінки сайту на жорсткому диску за допомогою спеціальної утиліти; 6) готується інформаційна довідка про ідентифікаційні дані сайту (IP-адреса, URL), інтернет-провайдера (електронна адреса, номери телефонів) тощо.

Аналізуючи викладене можна сформулювати наступний кримінально процесуальний механізм встановлення особи, яка вчинила злочин за допомогою веб-сайту. По-перше, досудове розслідування даного виду злочинів розпочинається із надходження до органу досудового розслідування повідомлення про виявлення факту протиправної діяльності на веб-сайті, та внесення відомостей про виявлений факт до Єдиного реєстру досудових розслідувань. По-друге, керуючись ст. 237 КПК України, необхідно невідкладно провести огляд зазначеного в повідомленні веб-сайту, за участю спеціаліста, з метою фіксування в протоколі огляду об'єктивних даних про наявність або відсутність на веб-сайті інформації, поширення якої заборонено законодавством України. В ході даного огляду необхідно обов'язково встановити домен сайту, встановити інтернет-провайдера, тобто провайдера телекомунікацій, який надає послуги доступу до мережі Інтернет та до вказаного сайту. По-третє, керуючись нормами Глави 15 КПК

України, отримати тимчасовий доступ до документів, що знаходяться у провайдера телекомунікацій та містять охоронювану законом таємницю, а саме інформацію про особу, яка зареєструвала веб-сайт, IP-адресу ЕОМ, з якої було здійснено реєстрацію веб-сайту, IP-адреси ЕОМ, з яких здійснювалось управління веб-сайтом та наповнення веб-сайту забороненим контентом, точний час доступу адміністратором до веб-сайту, який нас цікавить. По-четверте, за допомогою отриманої від інтернет-провайдера інформації, керуючись положеннями ст. 237 КПК України, маючи тимчасовий доступ до комп'ютера чи сервера, здійснити огляд за участю спеціаліста. В ході даного огляду за допомогою інтернет-сервісу «Whois» встановити провайдера, якому належать IP-адреси вищевказаних.

Після цього, керуючись положеннями Глави 15 КПК України, необхідно отримати у слідчого судді ще один тимчасовий доступ до документів, в яких міститься охоронювана законом таємниця, а саме інформація про абонента, який користується ЕОМ із зазначеними IP-адресами.

В ході подальшого досудового розслідування слідчим перевіряється та аналізується отримана інформація, в тому числі про фізичну адресу розміщення ЕОМ, якою користувалась особа під час вчинення злочину, після цього приймається рішення про необхідність отримання у слідчого судді ухвали про обшук за вказаною адресою та проведення інших слідчих дій та негласних слідчих (розшукових) дій. В разі встановлення в діях особи ознак складу злочину, передбаченого ст. 300 або ст. 301 КК України, вчиненого за допомогою веб-сайту, після збирання достатньої кількості доказів, кримінальне провадження підлягає направленню до суду, в тому числі із обвинувальним актом.

Таким чином, на даному етапі розвитку суспільства значну роль відіграє розповсюдження інформації за допомогою глобальної мережі Інтернет. Одночасно з цим актуальною стала проблема протидії розповсюдженню в мережі Інтернет на веб-сайтах інформації ксенофобного характеру, а також ту, що пропагує культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, а також порнографічних предметів. Протидія такому розповсюдженню має свої кримінально процесуальні особливості, обумовлені наданням доступу громадянам до веб-сайтів за

допомогою мережі Інтернет. Втім, підняті питання не є остаточними і підлягають окремому дослідженню, або науковому вивченню.

Список використаних джерел:

1. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – К. : Скіф, 2012. – 728 с.

2. Кримінальний процесуальний кодекс України : прийн. Верховною Радою України Законом № 4651-VI від 13.04.2012 : станом на 1 верес. 2013 р. – Х. : Право, 2013.

Одержано 20.11.2013

УДК 343.101

Юлія Володимирівна БУБИР,
ад'юнкт
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ЩОДО ПІДОЗРЮВАНОГО У ВЧИНЕННІ КІБЕРЗЛОЧИНУ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Як свідчить історія розвитку світового науково-технічного прогресу, будь-яка технічна новація, зокрема в галузі засобів комунікації, неминуче притягувала до себе людей, які намагалися і намагаються використати її для вчинення кримінального правопорушення. Не є винятком з цього також інформатизація та її складова – комп'ютеризація, тобто впровадження комп'ютерних технологій в різні сфери суспільної діяльності. Саме вона породила новий вид злочинів, які одержали умовну назву «кіберзлочини». Специфіка даного виду злочинності полягає у тому, що готування та вчинення злочину здійснюється, практично не відходячи з дому, оскільки комп'ютерна техніка постійно стає більш доступною, їх можна вчинювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати і вилучити інформацію, яка має значення при виконанні слідчих (розшукових) дій і негласних слідчих (розшукових) дій для використання її в якості речового доказу. Усі такі можливості, безумовно, використовуються кіберзлочинцями.

Найчастіше з використанням комп'ютера та мережі Інтернету вчиняються такі традиційні злочини як: порушення

авторського права і суміжних прав (ст. 176 КК України); шахрайство (ст. 190); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200); ухилення від сплати податків, зборів (обов'язкових платежів) (ст. 212); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231); ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301); а також злочини передбачені розділом XVI Кримінального кодексу України (зокрема ст. 361–363).

Число користувачів мережі Інтернет продовжує зростати, а разом з цим зростає і кількість атак, яких щодня зазнають комп'ютерні системи із зовнішнього середовища. Так, згідно статистики у 2011 році станом на 20 листопада кількість зареєстрованих злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку складала 129, в 2012 році за той самий період зареєстровано 138 злочинів, тоді як в 2013 році за підсумками 10 місяців до ЄРДР було внесено вже 555 кримінальних правопорушень в даній сфері, з яких особам вручено повідомлення про підозру лише в 226 випадках. Крім того в 2013 році в 11 випадках кримінальні правопорушення були скоєні групою осіб, а в 28 випадках особами, які вже вчиняли кримінальні правопорушення.

Особливістю кіберзлочинів є те, що вчиняються вони здебільшого психічно здоровими людьми, виключно із корисливих мотивів, а також цікавістю і усвідомленням свого розумового розвитку, цілком усвідомлено, з прямим умислом. Також до специфічних особистісних рис потенціальних кіберзлочинців можна віднести демонстративне, усвідомлене нехтування чинних правил людського поводження в соціумі; скептичне ставлення до суспільства чи громади, презирство та неповага до соціального укладу, влади; загострена зацикленість на собі, що характерно для осіб молодого віку.

При встановлені особи, яка вчинила кримінальне правопорушення, необхідно пам'ятати, що при спілкуванні в інформаційних мережах усі учасники спілкування майже завжди діють під псевдонімом та ніколи повністю та правдиво не заповнюють реєстраційні форми. Про жодну з осіб – учасників

мережного спілкування не можна сказати ким вона є насправді та де мешкає.

Для вирішення питання про обрання запобіжного заходу окрім доказів, що викривають певну особу, як таку, що вчинила кримінальне правопорушення, повинні бути також достатні підстави вважати, що підозрюваний, перебуваючи на волі, буде переховуватись від органів досудового розслідування та суду;знищить, сховає або спотворить будь-яку із речей и документів,які мають істотне значення для встановлення обставин кримінального правопорушення; незаконно впливатиме на потерпілого, свідка, іншого підозрюваного обвинуваченого, експерта, спеціаліста у цьому ж кримінальному провадженні; перешкоджатиме кримінальному провадженню іншим чином; вчинить інше кримінальне правопорушення чи продовжить кримінальне правопорушення, у якому підозрюється. Даний перелік є вичерпним і міститься він в ч. 1 ст. 177 КПК України, проте при вирішенні питання про обрання запобіжного заходу також можуть вплинути обставини перелічені в ст. 178 КПК України, а саме: вагомість наявних доказів про вчинення підозрюваним кримінального правопорушення; тяжкість покарання, що загрожує відповідній особі у разі визнання підозрюваного винуватим у кримінальному правопорушенні, у вчиненні якого він підозрюється, обвинувачується; вік та стан здоров'я підозрюваного; міцність соціальних зв'язків підозрюваного в місці його постійного проживання, у тому числі наявність в нього родини й утриманців; наявність у підозрюваного постійного місця роботи або навчання; репутацію підозрюваного; майновий стан підозрюваного; наявність судимостей у підозрюваного; дотримання підозрюваним умов застосованих запобіжних заходів, якщо вони застосовувалися до нього раніше; наявність повідомлення особі про підозру у вчиненні іншого кримінального правопорушення; розмір майнової шкоди, у завданні якої підозрюєтьсяособа, або розмір доходу, в отриманні якого внаслідок вчинення кримінального правопорушення підозрюється особа, а також вагомість наявних доказів, якими обґрунтовуються відповідні обставини.

Проблема протидії кіберзлочинності – це комплексна проблема. Злочини у галузі використання інформаційних технологій не піддаються результативному розслідуванню тими засобами і заходами, що були ефективні у минулому столітті,

коли інформатизація нашого суспільства тільки починалась. Закони повинні сьогодні відповідати тим вимогам, що пред'являє сучасний рівень розвитку технологій, щоб відправлення правосуддя відбувалося у незалежності від того, чи був такий злочин вчинений за допомогою звичайних засобів або персонального засобу супутникового зв'язку та мережі Інтернет. Для цього повинні продовжуватись наукові дослідження, напрацювання рекомендацій для слідчих і оперативних працівників.

У чинному КПК України є певні неузгодженості щодо такого учасника кримінального провадження, як підозрюваного. Так непоодинокими є випадки, коли слідчому відома особа, яка вчинила кіберзлочин, однак вона ухиляється від органів досудового розслідування. У такому разі згідно з положеннями КПК України слідчий повинен задіяти механізм вручення повідомлень. Найчастіше способом такого повідомлення є його направлення за місцем проживання особи. Направлення повідомлення є неможливим у випадку відсутності постійного місця проживання особи. У зв'язку з цим пропонується вважати особу підозрюваним не з моменту повідомлення їй про підозру, а з моменту складення та належного оформлення такого повідомлення. У разі ухилення підозрюваного від органів досудового розслідування слідчий зможе оголосити його в розшук.

Список використаних джерел:

1. Кримінальний кодекс України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14. – Станом на 04.07.2013.

2. Кримінальний процесуальний кодекс України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17. – Станом на 11.08.2013.

3. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М.Бутузов, В. В. Василевич та ін.]. – К. : Скіф, 2012. – 728 с.

Одержано 20.11.2013

УДК 343.657

Юрій Валерійович ГНУСОВ,
кандидат технічних наук,
доцент кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ,
Віталій Миколайович КІЙКОВ,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ШАХРАЙСТВА З БАНКІВСЬКИМИ ПЛАТІЖНИМИ КАРТКАМИ

Одним із видів злочинів, що вчиняються у фінансово-банківській сфері, є скімінг (анг. skimming), коли під час використання ATM (automated teller machine), POS (point-of sale), PIN-паду (далі – термінал) з банківської платіжної картки сторонніми особами нелегально і потайки копіюється зміст магнітної стрічки такої картки. Скімінг з'явився на початку 90-х років минулого сторіччя і з того часу тільки набирає обертів, як з кількості скоєних злочинів, так і в плані безперервного удосконалення прийомів та технічних засобів, що використовуються злочинцями.

На актуальність боротьби з даним видом злочинів в Україні вказує створення Управління боротьби з кіберзлочинністю МВС України та відповідних підрозділів ГУМВС, УМВС (указ Президента України від 6 квітня 2011 року № 383/2011), однією з функцій яких є розкриття злочинів пов'язаних з банківською сферою та платіжними системами.

Розрізняють два типи скімінгового обладнання. В першому випадку, скімінгове обладнання приєднується до слоту карткового приймача терміналу і зчитує інформацію замість самого пристрою. У цьому випадку користувач картки доступу до рахунку не отримує. В іншому випадку, людина отримує доступ до рахунку, але згодом дізнається про несанкціоноване зняття коштів. В обох випадках зловмисники різними способами також дізнаються про ПІН-код картки, наприклад, шляхом використання прихованих камер, накладних клавіатур тощо. Інформація з магнітної стрічки переноситься на нову пластикову картку і використовується

при безпосередньому знятті грошей через банкомат, оплаті товарів чи послуг через Інтернет, або продається третім особам. Такі ж схеми можуть траплятись і на точках продажу, де покупці розплачуються за послуги картками. Відповідно до статистики, зловмисники не залишаються на одному місці. Данні зчитуються і майже одразу виготовляється клон-картка та проходить нелегальне знімання коштів, злочинець(ці) переїжджає на інше місце (іншу країну). В більшості випадків несанкціоновані операції здійснюються у вечірній або нічний час, а також у вихідні дні, коли банківські установи не працюють і факт крадіжки встановлюється згодом [1].

Цікавим для України є досвід країн північної Америки де відповідальність за втрати від шахрайства по карті несе її емітент. Так, відповідно до інструкцій Федерального резерву США у разі виявлення факту незаконної діяльності з картковим рахунком (при скімінгу) і незалежно від суми збитку, максимальну суму, що клієнт може заплатити складає 50 дол., але більшість великих банків, як, наприклад «Bank of America», беруть на себе 100 % відшкодування за втрату коштів від шахрайства і таким чином несуть відповідальність за своє обладнання. У зв'язку з наростанням сум, втрачених клієнтами, в Україні дана проблема також потребує врегулювання на законодавчому рівні, тому що на даний час ошукані клієнти самотужки, через судові позови намагаються повернути втрачені кошти і у кожному випадку існує проблема з доказуванням провини сторін [2].

Серед різноманітної інформації стосовно правил безпечної поведінки особи щодо запобігання скімінгу можна виділити наступні аспекти: звертати увагу на підозрілі предмети на терміналі, не застосовувати силу при вкладанні картки у приймач банкомату, негайно інформувати банк про будь-яку підозру. Безперечно, факт невиявлення скімінгового обладнання клієнтом не виключає відповідальності банківської установи стежити за відсутністю нелегально встановленого обладнанням на власному терміналі: кардрідерами, накладками на клавіатуру, камерами тощо [4].

Деякі фірми-виробники виготовляють термінали з приймачем пластикової картки, що конструктивно ускладнює приєднання зовнішнього зчитувального пристрою. Також виробники використовують сигналізацію, що спрацьовує при спробі несанкціонованого приєднання скімінгового обладнання до терміналу.

Інша технологія запобігання скімінгу – коли швидкість з якою картка входить до терміналу змінюється і не є постійною, що є важливим для вдалого зчитування інформації скімінговими пристроями. Також, картка примусово рухається в зад і вперед під час зчитування.

Ще один спосіб боротьби зі скімінгом отримав назву Magneprint, що полягає в використанні притаманної тільки для даної магнітної стрічки унікальної характеристики «шуму» для диференціювання поміж справжньою карткою та її клоном [3].

В процесі еволюції боротьби зі скімінгом, на шляху до впровадження технології EMV (Europay, MasterCard and Visa), була використана технологія «Chip and PIN system», мета якої полягає в ідентифікації і підтвердженні власника картки за допомоги мікрочипу, що розміщується на платіжній картці.

Додатково фінансові установи використовують програмне забезпечення і проводять моніторинг транзакцій на рахунок, розміру та географії витрат, встановлюють обмеження на суму транзакції.

Одним із дієвих напрямків боротьби зі скімінгом є перехід на мікропроцесорні пластикові картки (EMV-технологія) і відмова від магнітної стрічки. На даний час процес остаточного переходу на чипові технології не завершився, термінали працюють комбіновано і приймають магнітні стрічки, що і сприяє скімінгу. В таких умовах для боротьби з проблемою підробки картки із забезпеченням збереження ПІН-коду (коли зловмисник з різних причин не володіє ПІН-кодом) полягає у використанні виробниками і власниками терміналів удосконалених і більш захищених способів оновлення сесійних ключів в алгоритмі 3DES (стандарт ANSI X9.24) та шифрування даних для ПІН-коду (стандарт ANSI X9.8). Як відомо, передавання даних ПІН-блоку від терміналу до хостової системи банку відбувається у зашифрованому вигляді. Найбільш захищеним на даний час вважається алгоритм шифрування 3DES який і має використовуватись у процесінгових системах банків.

Таким чином, ефективним способом викорінення скімінгу є глобальний перехід банківської системи на EMV-картки та невикористання магнітної стрічки для запису і зчитування інформації.

Список використаних джерел:

1. Schmidt L. Warning signs [Електронний ресурс] / Lucinda Schmidt. – Режим доступу: http://moneymanager.smh.com.au/articles/2003/10/15/1065917445606.html.

2. Wisconsin Bankers Association Warns Consumers, Asks for Help In Identifying ATM Card Skimming Scam [Електронний ресурс]. – Режим доступу: http://www.wisbank.com/Media/Press%20Releases/PR_ATM_Card_Skimming_Scam.htm.

3. Costa C. MasterCard International Hosts First Global Risk Management Symposium [Електронний ресурс] / Christina Costa. – Режим доступу: http://www.mastercardintl.com/cgi-bin/newsroom.cgi?id=706.

4. How to be ATM «Streetwise» [Електронний ресурс]. – Режим доступу: http://nsi.org/Tips/atmtips.html.

Одержано 18.11.2013

УДК 343.98

Юрій Миколайович ОНИЩЕНКО,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ПОСЛУГИ З ПЕРЕКАЗУ КОШТІВ ЯК СПОСІБ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ ВІД КІБЕРЗЛОЧИНІВ

Сучасний стан інформаційних та телекомунікаційних технологій і швидкість здійснення фінансових транзакцій (переказу грошей з рахунку на рахунок) дає можливість здійснення кримінальних фінансових операцій через мережу Інтернет.

Чим вище рівень інформатизації в країні, тим більшу загрозу представляє кіберзлочинність. Більшість великих традиційних постачальників послуг з переказу грошових коштів, наприклад, «WebMoney», «MoneyGram», «Western Union», «PayPal» здійснюють їх он-лайн з використанням мережі Інтернет. Якщо контроль над легальними фінансовими інститутами забезпечений в переважній більшості країн, то неформальні системи розрахунків, що оперують досить невеликими сумами, до недавнього часу знаходилися поза увагою органів фінансового моніторингу і спецслужб. Рух коштів в таких системах здійснюється поза увагою існуючих систем контролю фінансових потоків. Також частиною міжнародного обороту

нелегальних грошових потоків у сучасному світі є система, відома у арабському світі під назвою «хавала». Система хавала заснована на переказі грошових коштів шляхом одноразових повідомлень і підтверджень по електронній пошті, факсу або телефонними дзвінками. Останнім часом в якості лідера комунікацій в цій сфері використовується skype-зв'язок, як найбільш конфіденційний спосіб зв'язку. Матеріальні цінності у вигляді грошей, золота і коштовних каменів переміщаються з країни в країну без супровідних фінансових документів. Враховуючи, що усі фінансові транзакції здійснюються методом взаємозаліку або при особистих зустрічах, то відстежити ці потоки державні контрольні органи не в змозі [1]. Використання постачальників послуг з переказу грошових коштів – це звичайний метод для відмивання доходів, отриманих від кіберзлочинів.

Оскільки велика частина грошових переказів, яка здійснюється через таких постачальників, виплачується готівкою, то це дає можливість злочинцям ввести у фінансову систему доходи, отримані незаконним шляхом. При цьому абсолютна більшість законних операцій з готівковими грошовими коштами, здійснених вказаним способом, надає прекрасну можливість для приховання діяльності по відмиванню грошей на стадії розміщення.

Такі фінансові послуги мають спрощені зобов'язання по ідентифікації клієнтів. Спрощена процедура відправки/отримання грошових коштів дає можливість використати їх необмеженому колу осіб: від злочинців, що відмивають доходи від кіберзлочинів, «грошових мулів» або «фінансових агентів» до неосвічених людей, яким дуже важко взаємодіяти із занадто «зарегульованою» фінансовою установою. Грошовий мул (money mool) – це людина, яка погоджується виступати фінансовим посередником і використати свій банківський рахунок для переказу грошей з рахунків постраждалих на рахунки зловмисників. Звичайно це люди, які шукають роботу і не підозрюють, що вони стають співучасниками кіберзлочинів [2]. Часто послуги з переказу грошових коштів – це частина складної схеми, у рамках реалізації якої проводиться хоч б одна операція з готівковими грошовими коштами з тим, щоб зруйнувати ланцюжок і приховати слід грошей. Також в таких схемах усвідомлено або ні беруть участь грошові мули.

Постачальники послуг з переказу грошових коштів роблять їх за невелику плату і часто використовують не такі захищені програми, ніж застосовують традиційні фінансові установи. Зазвичай такі постачальники укладають договори з банками з тим, щоб забезпечити безпечні і захищені контактні точки зі своїми клієнтами.

Типологія, проведення таких операцій наступна:

– на пошту користувача приходить неправдива пропозиція про роботу (спам), заявника вербують по телефону або іншим способом, що виключають особистий контакт. Зазвичай ця робота пов'язана з фінансовими питаннями або роботою вдома;

– доходи від кіберзлочинів переказуються на рахунок грошового мула, який повинен зняти готівкові грошові кошти і потім направити їх певному одержувачеві з використанням грошового переказу. Сума зазвичай нижче порогового значення з тим, щоб уникнути її подальшого відстежування;

– такі грошові перекази використовуються для того, щоб перевести готівку їх кінцевому отримувачу.

В результаті можна зробити наступні висновки: постачальники послуг з переказу грошей використовуються для відмивання доходів, отриманих від кіберзлочинів; вони використовуються у схемах по відмиванню грошей спільно з грошовими мулами; вони є найбільш врегульованими посередниками, залученими у відмивання грошей від кіберзлочинів і таким чином, мають усі можливості для передачі цінної інформації в правоохоронні органи для запобігання кіберзлочинам.

Поєднання заходів протидії відмиванню грошей і фінансових розслідувань з розслідуванням кіберзлочинів і комп'ютерною криміналістикою створює додаткові можливості для міжнародної співпраці в галузі боротьби з кіберзлочинністю.

Список використаних джерел:

1. Хавала (Hawala). Отмывание денег в исламских странах / [Електронний ресурс]. – Режим доступу: http://www.taxc.com.ua/hawala.html.

2. Активизация атак Zeus и жертвы денежных махинаций / [Електронний ресурс]. – Режим доступу: http://www.newsdesk.pcmag.ru/node/29801.

Одержано 14.11.2013

УДК 343.224.1:004

Руслан Вікторович ЄДИН,
викладач кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ОБРАННЯ ЗАПОБІЖНИХ ЗАХОДІВ ЩОДО НЕПОВНОЛІТНІХ ПІДОЗРЮВАНИХ У ВЧИНЕННІ КІБЕРЗЛОЧИНІВ

Процесуальний механізм у кримінальних провадженнях про злочини і суспільно небезпечні діяння вчинені неповнолітніми, який закріплений чинним Кримінальним процесуальним кодексом, покликаний бути гарантією захисту з одного боку прав та законних інтересів зазначених осіб а з іншого – правосуддя в цілому.

Серед усіх категорій осіб, чиї права і свободи зобов'язалася забезпечувати держава, слід виділити окрему групу – дітей, яким державні органи та службові особи повинні приділяти особливу увагу. Зважаючи на емоційно-психологічні, розумово-інтелектуальні та інші особливості неповнолітніх, вони належать до уразливих груп населення, правовий статус яких є показником рівня цивілізованості суспільства, у якому право, що розпочинало свою історію як право сильного, стає силою слабких.

Тенденція до уніфікації кримінальної процесуальної форми не виключає на сучасному етапі наявності її певної диференціації, викликаної насамперед необхідністю надання додаткових гарантій забезпечення прав та законних інтересів окремим категоріям. Як відомо, значна частина кіберзлочинів учиняється особами у віці до 18 років. Це обумовлено насамперед здатністю неповнолітніх до сприйняття усього нового у порівнянні з людьми старшого віку, недостатньою увагою з боку сім'ї, педагогічних колективів закладів освіти, обмеженої можливості цікаво і з користю проводити вільний час у поєднанні з притаманними підліткам максималізму, бажанням досягти чогось значного в очах однолітків, самореалізовуватися тощо.

Згідно зі ст. 492 КПК України до неповнолітнього з урахуванням його вікових та психологічних особливостей, роду занять може бути застосовано один із загальних запобіжних заходів. До загальних запобіжних заходів ст. 176 КПК відносить особисте зобов'язання, особисту поруку, заставу,

домашній арешт, тримання під вартою та затримання як тимчасовий запобіжний захід. Крім того ст. 493 КПК України дозволяє до неповнолітніх підозрюваних чи обвинувачених, крім загальних запобіжних заходів, застосовувати передання їх під нагляд батьків, опікунів чи піклувальників, а до неповнолітніх, які виховуються в дитячій установі, – передання їх під нагляд адміністрації цієї установи.

Згідно з п. 2, 3 ст. 178 КПК України при вирішенні питання про обрання запобіжного заходу, крім наявності ризиків, зазначених у ст. 177 цього Кодексу, слідчий суддя, суд на підставі наданих сторонами кримінального провадження матеріалів, зобов'язаний оцінити всі обставини, серед яких: тяжкість покарання, що загрожує відповідній особі у разі визнання підозрюваного, обвинуваченого винуватим у кримінальному правопорушенні, у вчиненні якого він підозрюється, обвинувачується; та вік підозрюваного, обвинуваченого. Аналізуючи положення ч. 3 ст. 176 КПК України, доходимо висновку про те, що до особи необхідно застосовувати найм'якіший із можливих запобіжних заходів.

При обранні кожного з запобіжних заходів є певні проблеми, що пов'язані з процедурою їх застосування, кваліфікацією кримінального правопорушення або особливостями самої особи підозрюваного.

Так застосування особистого зобов'язання, особистої поруки, застави, передання неповнолітніх під нагляд батьків, опікунів чи піклувальників або адміністрації дитячої установи безпосередньо пов'язане з бажанням або згодою самого підозрюваного чи обвинуваченого чи доброю волею осіб, які беруть на себе зобов'язання забезпечити належну поведінку неповнолітнього. Проблеми обрання запобіжного заходу у виді тримання під вартою та затримання неповнолітнього обумовлені взагалі неможливістю їх застосування при розслідуванні злочинів невеликої або середньої тяжкості Причому законодавча заборона на застосування зазначених запобіжних заходів щодо неповнолітніх є абсолютною і безальтернативною, у тому числі і у випадках продовження злочинної діяльності (якщо вчинювані злочини не є тяжкими або особливо тяжкими), переховування від органів досудового розслідування та суду, перешкоджання кримінальному провадженню іншим чином тощо.

Досить ефективним, на нашу думку, запобіжним заходом щодо неповнолітніх підозрюваних (обвинувачених) є домашній

арешт, що полягає в забороні підозрюваному, обвинуваченому залишати житло цілодобово або у певний період доби, враховуючи обов'язок осіб, що беруть участь у кримінальному судочинстві, здійснювати процесуальні дії в порядку, що найменше порушує звичайний уклад життя неповнолітнього та відповідає його віковим та психологічним особливостям, та вживати всіх інших заходів, спрямованих на уникнення негативного впливу на нього.

З огляду на викладене доходимо висновку, що *КПК України передбачена система запобіжних заходів, яка дозволяє у кожному конкретному випадку індивідуально обрати запобіжний захід, виходячи з конкретних обставин, встановлених у ході кримінального провадження, у тому числі до неповнолітніх підозрюваних (обвинувачених) у вчиненні кіберзлочинів.*

Разом з тим *правовий інститут запобіжних заходів і процесуальний механізм його реалізації у правозастосовній діяльності під час досудового розслідування і судового розгляду в кримінальних провадженнях щодо неповнолітніх потребує подальшої більш глибокої наукової розробки з метою напрацювання пропозицій для його удосконалення.*

Одержано 22.11.2013

УДК 343.133:004

Сергій Олександрович СИЧОВ,
старший викладач кафедри кримінального процесу факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

ПРОБЛЕМНІ ПИТАННЯ ПОВІДОМЛЕННЯ ОСОБІ ПРО ПІДОЗРУ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

У сфері нових суспільних відносин, зокрема, інформаційних – в останні десятиліття відбуваються найбільш істотні зміни. Суть переходу від індустріального суспільства до суспільства інформаційного полягає саме в сукупності процесів, пов'язаних з автоматизованою обробкою, пошуком, зберіганням і передачею зростаючого потоку інформації в усі сфери суспільного життя.

Цей фактор загострив потребу у необхідності правового регулювання відносин у сфері використання телекомунікаційних систем для прискорення процесів інформатизації

українського суспільства і подолання відставання від інших країн.

З розвитком глобальної інформаційної мережі Інтернет і формування нових економічних технологій (торгівля через «віртуальні» магазини, брокерські операції, кібербанки тощо) з'явилися нові види злочинів – «кіберзлочини» (cibercrime). Кіберзлочинність і її наслідки являють собою нову форму антигромадської поведінки, що лише нещодавно одержала визнання як явище, яке представляє собою загальну загрозу безпеці і нормальному функціонуванню суспільства.

Незважаючи на те, що в нашій державі сьогодні є безліч не менш нагальних проблем, які потрібно вирішувати невідкладно, проблема боротьби з кіберзлочинами не можна лишати поза увагою. Необхідно розробляти методологічні, теоретичні і практичні основи забезпечення захисту інформації в глобальній мережі Інтернет. Адже майже усі взаємовідносини між суб'єктами інформаційного суспільства ґрунтуватимуться на споживанні й обміні інформацією. А в цьому випадку питання інформаційної безпеки стає превалюючим. Розвиток правового регулювання використання мережі Інтернет у нашій країні має спрямовуватися як на врахування зарубіжного досвіду, так і національних інтересів України в інформаційній сфері. Особлива увага повинна приділятися виявленню та дослідженню недоліків з метою їх подальшого уникання в правотворчій та правозастосовній діяльності і запобігання негативних наслідків інформатизації. Це повинно здійснюватися шляхом ґрунтовного наукового забезпечення, залучення широкого кола вітчизняних фахівців, які володіють знаннями щодо юридичної теорії та практики України і зарубіжних країн, а також мають певну підготовку у галузі використання інформаційних технологій і захисту інформації [1].

З метою протидії вчиненню кіберзлочинів у системі МВС України були створені спеціальні відділи, діяльність яких спрямована на виявлення, запобігання, розслідування та профілактику злочинів у цій сфері. Але для успішного виконання поставлених на ці підрозділи завдань необхідно суворо дотримуватися чинного законодавства, яке не повинно створювати умов для неоднозначного тлумачення правових норм.

19 листопада 2013 року минув рік як кримінальне судочинство в Україні здійснюється згідного нового Кримінального

процесуального кодексу. За цей час при застосуванні кримінальних процесуальних норм, на ряду із позитивними нововведеннями, виявились чимало проблемних питань.

Так, статтею 276 Кримінального процесуального кодексу України (далі – КПК) передбачено повідомлення про підозру, яке здійснюється у випадках:

1) затримання особи на місці вчинення кримінального правопорушення чи безпосередньо після його вчинення;

2) обрання до особи одного з передбачених КПК запобіжних заходів;

3) наявності достатніх доказів для підозри особи у вчиненні кримінального правопорушення.

При цьому слідчий, прокурор або інша уповноважена службова особа (особа, якій законом надано право здійснювати затримання) зобов'язані невідкладно повідомити підозрюваному про його права, передбачені статтею 42 КПК. Після повідомлення про права слідчий, прокурор або інша уповноважена службова особа на прохання підозрюваного зобов'язані детально роз'яснити кожне із зазначених прав.

Порядок вручення письмового повідомлення про підозру передбачений статтею 278 КПК, згідно якої письмове повідомлення про підозру вручається в день його складення слідчим або прокурором, а у випадку неможливості такого вручення – у спосіб, передбачений КПК *для вручення повідомлень*. Письмове повідомлення про підозру затриманій особі вручається не пізніше двадцяти чотирьох годин з моменту її затримання. У разі якщо особі не вручено повідомлення про підозру після двадцяти чотирьох годин з моменту затримання, така особа підлягає негайному звільненню. Дата та час повідомлення про підозру, правова кваліфікація кримінального правопорушення, у вчиненні якого підозрюється особа, із зазначенням статті (частини статті) закону України про кримінальну відповідальність невідкладно вносяться слідчим, прокурором до Єдиного реєстру досудових розслідувань [2].

Але цей порядок вручення повідомлення про підозру не є чітко визначеним саме для цієї процесуальної дії, так як передбачений зовсім для інших процесуальних дій – виклику слідчим, прокурором, судового виклику і привода (глава 11 КПК). Така невизначеність положень чинного КПК України породжує незрозумілість практичними працівниками порядку

вручення повідомлення про підозру у випадках, коли особа ховається від правоохоронних органів, а тому не повністю забезпечує виконання завдань кримінального судочинства.

Зазначені проблемні питання потребують ретельного наукового дослідження та негайного вирішення на законодавчому рівні.

Список використаних джерел:

1. Теоретико-правові проблеми боротьби з кіберзлочинами [Електронний ресурс]. – Режим доступу: http://www.br.com.ua/referats/Pravo/31004.htm.

2. Кримінальний процесуальний кодекс України : закон України від 13.04.2012 № 4651-VI [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17/page8.

Одержано 23.11.2013

УДК 343.98

Аліна Ігорівна АНАПОЛЬСЬКА,
кандидат юридичних наук,
старший викладач кафедри кримінально-правових дисциплін
Луганського державного університету внутрішніх справ
ім. Е. О. Дідоренка

ВЗАЄМОДІЯ ПРАВООХОРОННИХ ОРГАНІВ З БАНКІВСЬКИМИ УСТАНОВАМИ У РОЗСЛІДУВАННІ ШАХРАЙСТВ, ВЧИНЕНИХ У СФЕРІ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННИХ РОЗРАХУНКІВ

Банківська система, яка пов'язана з накопиченням, розподілом і використанням державних та приватних коштів, є однією з найбільш привабливих для окремих злочинців та організованих злочинних груп. У цій системі на сьогодні здійснюється велика кількість різноманітних афер, серед яких найпоширенішими є шахрайства, які вчиняються у сфері функціонування електронних розрахунків. Виявлення та розслідування таких злочинів є одним з пріоритетних завдань, що стоять перед правоохоронними органами. Не останнє місце у вирішенні зазначеного питання належить добре налагодженій взаємодії ОВС з банківськими установами.

Питанню взаємодії в окремих методиках розслідування злочинів у банківській сфері, присвячено чимало досліджень таких вчених, як О. П. Бущан, А. Ф. Волобуєв, В. А. Гамза, А. Л. Дудніков, В. П. Корж, В. Д. Ларічев, Г. А. Матусовський, В. М. Попович, Р. С. Сатуєв, Л. М. Стрельбицька, І. Б. Ткачук, С. С. Чернявський, Д. А. Шраєр, М. П. Яблоков,

П. С. Яні та ін. Між тим, в правоохоронній практиці залишаються проблемними питання спільної діяльності та сприяння з боку банківських установ розслідуванню кримінальних проваджень про шахрайства, вчинені у сфері функціонування електронних розрахунків, що пояснює низький рівень ефективності боротьби із зазначеними злочинами.

На сьогодні, банківські установи є відносно закритими для контролю з боку держави, у зв'язку із чим, у разі виявлення ознак злочинів, керівники банків звертаються за допомогою до правоохоронних органів лише в поодиноких випадках. Сукупність зазначених обставин стали об'єктивною умовою виконання завдань з виявлення та документування шахрайств, вчинених у сфері функціонування електронних розрахунків, співробітниками служб безпеки банків. Нормативні документи більшості банківських закладів України закріплюють такі обов'язки служб банківської безпеки як: виявлення ознак підготовлюваних і вчинених злочинів, вжиття заходів щодо їх попередження та припинення; готування матеріалів до правоохоронних органів для вирішення питання про початок кримінального провадження; участь у досудовому розслідуванні кримінальних правопорушень; направлення правоохоронним органам інформації, що має відношення до розслідування; вжиття у межах компетенції заходів щодо відшкодування завданих банку збитків. Між тим, відсутність у законодавстві прямих приписів з виконання вище перелічених обов'язків, призводить до того, що на практиці вони практично не виконуються.

Зазвичай, під час «внутрішніх» перевірок порушення порядку здійснення банківських операцій, співробітникам служб безпеки банків вдається виявити приблизно 10-15% шахрайств, які вчиняються уповноваженими працівниками банків. Між тим, як справедливо зазначає А. Ф. Волобуєв, діяльність банків, як структур ринкової економіки, в багатьох аспектах пов'язана зі збереженням комерційної (банківської) таємниці, тому різного роду майнові зловживання персоналу банку стають відомими правоохоронним органам тільки тоді, коли цього забажає керівництво банку [1, с. 253]. Між тим, як показало проведене нами дослідження, внутрішніми користувачами (якими є співробітники банків) скоюється близько 79 % злочинів, тоді як зовнішніми користувачами тільки 21 %. Отримані нами дані кореспондуються з результатами

досліджень П. Д. Біленчука, О. П. Дубового, М. В. Салтевського та П. Ю. Тимошенка, які зазначають, що основна небезпека в процесі вчинення зазначеного різновиду злочинів виходить від внутрішніх користувачів, ними вчинюється 94 % злочинів, тоді як зовнішніми користувачами – лише 6 %, при цьому 76 % з числа зовнішніх користувачів – це клієнти-користувачі комп'ютерної системи, а 24% – обслуговуючий персонал [2, с. 374–375]. Результати виявлення вчинених ними шахрайств уповноваженими працівниками приватної охоронної структури, керівники банків також намагаються віднести до охоронюваної законом банківської таємниці, не давши їй офіційного ходу. Проте, інститут банківської таємниці в законодавстві України існує не для ухилення від надання відповідної інформації, а для забезпечення захисту законних прав та інтересів учасників правовідносин у кредитно-фінансовій сфері.

У разі ж подання заяви до органу внутрішніх справ, представники банківської установи, зазвичай, обмежують процес ознайомлення правоохоронців з результатами власних розслідувань, що надалі ускладнює процес доказування та судового розгляду кримінальних проваджень про шахрайства, вчинені у сфері функціонування електронних розрахунків. У свою чергу працівники правоохоронних органів, не маючи прямого доступу до операцій та документів банку, не рідко змушені обмежуватися лише поверхневим дослідженням наявних доказів, не використовуючи більшість процесуальних та оперативно-розшукових засобів їх отримання.

Прийняття нового КПК України також сприяло зменшенню активності у виявленні таких злочинів, що, перш за все, пов'язано із розширенням у ньому переліку кримінальних правопорушень, за якими кримінальне провадження розпочинається лише на підставі заяви потерпілого (зокрема, це стосується й ч. 3 ст. 190 КК України).

Результати опитування працівників банківської безпеки та слідчих органів внутрішніх справ, проведені В.О. Фінагеєвим, показали, що спільна діяльність банків та органів досудового розслідування може бути доволі ефективною у випадках: надання службами безпеки правоохоронним органам матеріалів для вирішення питання про початок кримінального провадження (88 %; 92 %), доступу до технічних засобів банку, приміщень і документів, необхідних для проведення

слідчих (розшукових) та негласних слідчих (розшукових) дій, і допомоги в їх застосуванні (51 %; 76 %); налагодження зв'язків і одержання інформації від інших банків, звідки або куди перераховувались кошти в ході реалізації злочинної діяльності (42 %; 68 %); збирання та надання доказів, що мають відношення до розслідування (74 %; 92 %); участь у розшуку осіб, які вчинили посягання на інтереси банку або підозрюваних у їх вчиненні, а також вжиття у межах компетенції заходів щодо відшкодування завданих банку збитків (35 %; 44 %) [3, с. 268–269]. Все це свідчить про розуміння практичними працівниками як банківських установ, так і правоохоронних органів, необхідності закріплення означених нами питань взаємодії на законодавчому рівні.

Таким чином, визначення принципів і форм взаємодії правоохоронних органів зі службами безпеки банків, розроблення відповідних методик документування і викриття злочинів, а також проведення спільних семінарів і тренінгів для працівників практичних підрозділів за участю фахівців з банківської сфери та спеціалістів у галузі комп'ютерних технологій дозволять належним чином організувати боротьбу з шахрайствами, вчиненими у сфері функціонування електронних розрахунків.

Список використаних джерел:

1. Волобуєв А. Ф. Проблеми методики розслідування розкрадань майна в сфері підприємництва / А. Ф. Волобуєв. – Х. : Вид-во Ун-ту внутр. справ, 2000. – 336 с.

2. Криміналістика : підруч. для слухачів, ад'юнктів, викладачів вузів системи МВС України / П. Д. Біленчук, О. П. Дубовий, М. В. Салтевський, П. Ю. Тимошенко. – К. : Атіка., 1998. – 416 с.

3. Фінагеєв В. О. Проблеми взаємодії правоохоронних органів та підрозділів безпеки банків у виявленні та розслідуванні злочинів / В. О. Фінагеєв // Митна справа. – 2013. – № 2 (86). – Ч. 2, кн. 1. – С. 264–270.

Одержано 23.11.2013

УДК 343.1

Наталія Миколаївна АХТИРСЬКА,
кандидат юридичних наук, доцент,
доцент кафедри правосуддя Київського національного університету імені Тараса Шевченка

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ФАКТОР ФОРМУВАННЯ СПРАВЕДЛИВОГО ТА ДОСТУПНОГО СУДОЧИНСТВА

Як влучно зазначав Джон Брокман, ретроспективна подорож в суспільне життя є інтелектуальною пригодою, яка підтверджує, що наука, новітні технології стали новою суспільною силою, яка створила нову суспільну культуру міжособистісну та ділову [1, с. 10]. Інформаційні технології у своєму динамічному розвитку послідовно та впевнено проникають у суміжні галузі, перетворюючи класичні уяви про сталість окремих процесів, можливостей та наслідків. Потреба удосконалення судочинства викликала необхідність поєднання римських принципів судової поміркованості з європейською елегантністю тлумачення та інформаційно-технічною революційністю.

Судочинство тривалий час не зазнавало власної трансформації у процесуальному розумінні від впливу комп'ютерних технологій. Статистичні дані провадженні у судах лише фіксували наявність нової загрози. Так, у 2012 р. за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (ст. 361–363-1 КК України) судами України було засуджено 80 осіб, з яких 4 іноземці, 76 громадян України, 1 жінка; 12 осіб вчинили злочин у складі групи, 3 – у складі організованої групи. Вік засуджених має вражаючу амплітуду – від 18 до 65 років (12 осіб у віці від 18 до 25 років; 24 особи – від 25 до 30 років; 40 осіб –від 30 до 50 років; 4 особи – від 50 до 65 років). Рід занять засуджених: 9 – робітники, 5 – державні службовці, 10 – інші службові особи, 7 – приватні підприємці, 4 – працівники господарських товариств тощо.

В методології кримінального судочинства вагомого значення набуває питання ролі системного підходу до вирішення проблем. Системність виявляється у всіх формах та на будь-яких рівнях об'єктивного світу. Основним змістом пізнання стають не стільки предмети або системи самі по собі, скільки їх взаємодія, баланс сил, факторів, процесів. Варто при цьому зазначити, що кожна методологічна настанова

передбачає характер знання, яке необхідно одержати та спосіб його здобуття.

Першою проблемою, яка постала в реформуванні судочинства – дотримання розумних строків провадження. Своєчасність виклику учасника процесу забезпечувалась надсиланням судових повісток. Однак,як свідчить статистика, у 2012 р. зафіксовано значну кількість фактів відкладення розгляду справ у зв'язку неявкою учасників процесу, зокрема 55 500 фактів неявки свідків та потерпілих, значна частина яких скаржилась на відсутність належного повідомлення. Використання телекомунікаційних мереж дозволило надсилати повідомлення у вигляді SMS-повідомлень. Так, наказом Державної судової адміністрації України від 01.06.2013 затверджено Порядок надсилання учасникам судового процесу (кримінального провадження) текстів судових повісток у вигляді SMS-повідомлень. Вимоги до змісту судової повістки у вигляді SMS-повідомлення визначаються ст. 137 Кримінального процесуального кодексу України.

Текст судової повістки може бути надісланий судом Учаснику SMS-повідомленням лише після подання ним до суду заявки про намір отримання судової повістки в електронному вигляді за допомогою SMS-повідомлення. Така заявка оформляється безпосередньо в суді або шляхом роздрукування та заповнення форми, яка розміщена на офіційному вебпорталі судової влади України. Формування тексту судової повістки, облік та її відправка у вигляді SMS-повідомлення здійснюється в автоматизованій системі документообігу суду. Судова повістка додається до електронної обліково-статистичної картки справи як документ по справі, після чого автоматично доставляється у вигляді SMS-повідомлень на номер мобільного телефону. Результат доставки SMS-повідомлення на номер мобільного телефону учасника процесу (дата та час доставки або причина недоставки) автоматично розміщується у відповідному електронному реєстрі автоматизованої системи документообігу. Відповідальний працівник апарату суду роздруковує таке повідомлення та долучає його до матеріалів справи.

Другим кроком у використанні новітніх технологій стало впровадження відеоконференції у кримінальному провадженні. Однак, як свідчать рішення Європейського суду з прав людини, сумнівними є канали передачі інформації,

оскільки у таких випадках держава має створити спеціальні конфіденційні канали зв'язку. Так, у рішенні «Сахновський проти Росії» було зазначено, що у випадку дистанційного спілкування з учасниками процесу «держава має створити та забезпечити систему зв'язку, яка належить та обслуговується державою» [2].

Несподіваним об'єктом дослідження спеціалістів з комп'ютерних технологій стають електронні записи судового провадження на предмет внесення до них змін (зокрема – вилучення, монтажу тощо).

Отже, інформаційні технології, які використовуються судами України, безумовно сприяють вирішенню організаційних та правових питань. Водночас фахівцями доцільно прогнозувати нові ризики та загрози, які можуть призвести до ускладнень, та запропонувати запобіжні механізми.

Список використаних джерел:

1. Будущее науки в XXI веке. Следующие пятьдесят лет / под ред. Джона Брокмана ; пер. с анг. Ю. В. Букановой. – М. : АСТ ; Астрель ; Владимир : ВКТ, 2011. – 256 с.

2. Дело Сахновский против России : [постановление Европейского суда по правам человека от 02.11.2010] : жалоба № 21272/03 [Електронний ресурс]. – Режим доступу: http://hr-lawyers.org/files/docs/1291296455.pdf.

Одержано 23.11.2013

РОЗДІЛ 3
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ТЕХНІЧНИХ ЗАСОБІВ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

УДК 65.012.8+004

В'ячеслав Валерійович МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців
для підрозділів боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ АВТОМАТИЗОВАНОГО БАНКУ ДАНИХ «НЕВІД» У ПРАКТИЧНОМУ НАВЧАННІ КУРСАНТІВ

Український досвід засвідчує, для того щоб ефективно протистояти кіберзлочинності, потрібно постійно вчитися – вчитися новим технологіям та вміти застосовувати ці знання на практиці в рамках діючого законодавства. Звичайно, що для ефективної роботи з протидії високотехнологічній злочинності правоохоронне відомство потребує постійного поповнення як матеріально-технічним забезпеченням, так і кваліфікованими кадрами.

Як і в інших сферах правоохоронної діяльності якісно підготовлений «кіберкоп» з перших днів закінчення вишу повинен ефективно застосовувати набуті знання на практиці. Ось чому важливою є практична складова підготовки таких фахівців. Звичайно сюди входить і моделювання практичних ситуацій, і відпрацювання навичок на спеціальних навчально-тренувальних полігонах, і розробка власного програмного забезпечення. Проте це не все. Потрібно залучити курсанта протягом навчання у взаємодії з територіальними підрозділами до виконання реальних завдань боротьби з кіберзлочинністю. Досвід Харківського національного університету внутрішніх справ засвідчує ефективність такої методики, яка реалізована у декількох проектах.

Одним з таких проектів є автоматизований банк даних «Невід», призначений для накопичення інформації про розміщення протиправного контенту в мережі Інтернет (інформаційна система «Правопорушення») і розшуку осіб (інформаційна система «Розшук») та відповідних заходів щодо цього з боку органів внутрішніх справ.

Вперше його було презентовано 23 квітня 2013 року в рамках конференції «Протидія кіберзлочинності в фінансово-банківській сфері» за участю заступника Міністра внутрішніх справ України – керівника апарату С. І. Лекаря.

На сьогодні роботу системи забезпечують 17 курсантів, частина з яких програмує відповідні модулі, решта здійснює пошук інформації за пріоритетними напрямами, визначеними МВС. За домовленістю з керівництвом Управління боротьби з кіберзлочинністю МВС України «Невід» після доопрацювання буде інтегровано як окремий модуль до розроблюваного автоматизованого робочого місця працівника УБК, після чого до його наповнення будуть залучені курсанти решти вишів системи МВС.

На теперішній час за результатами опрацювання віднайденої курсантами в мережі інформації регулярно відкриваються кримінальні провадження та попереджаються правопорушення. Зокрема, за час функціонування інформаційної системи «Правопорушення» виявлено та надіслано інформацію про 58 правопорушень, з яких ст. 115 КК (умисне вбивство) – 1, ст. 301 КК (ввезення, виготовлення, збут і розповсюдження порнографічних предметів) – 33, ст. 307 КК (незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів) – 15, ст. 358 КК (підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів) – 6, ст. 263 КК (незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами) – 3.

У рамках функціонування автоматизованого банку даних «Невід» діє також новоутворена інформаційна система «Розшук» на підставі трьохсторонньої угоди, укладеної між Управлінням боротьби з кіберзлочинністю МВС України, Управлінням кримінальної міліції у справах дітей МВС України та Харківським національним університетом внутрішніх справ.

Наповнення системи здійснюють курсанти за результатами вжитих заходів щодо пошуку безвісти зниклих дітей з використанням комп'ютерних технологій.

Одним з прикладів успішного проведення таких заходів став випадок із 14 річною безвісти зниклою громадянкою П. За словами матері дівчина вийшла з секції малювання та

в назначений час не прибула до дому. При цьому її мобільний телефон був вимкнений. Після написання громадянкою П. заяви до Київського районного відділу міліції ГУМВС України в Харківській області, вона того ж дня звернулась з проханням про допомогу до Харківського національного університету внутрішніх справ.

Курсанти – учасники проекту «Невід», з дозволу батьків зниклої дівчини, виїхали до квартири, де вона мешкає, та оглянули вміст її персонального комп'ютера на предмет даних, які можуть допомогти в її пошуку. Під час перегляду інформації, що знаходилась на комп'ютері, було виявлено електронну поштову скриньку та сторінку в соціальній мережі «ВКонтакті», якими користувалась зникла дівчина. Шляхом аналізу знайденої інформації було встановлено коло осіб, з якими вона активно спілкувалася та відповідно у яких вона могла знаходитись.

Одержану інформацію було передано оперативним працівникам ГУМВС України в Харківській області, які встановили місце проживання зазначених осіб, та шляхом їхнього опитування виявили особу, у якої переховувалась зникла дівчина.

Таким чином, у рамках підготовки фахівців для підрозділів, задіяних у боротьбі з кіберзлочинністю, в університеті постійно використовуються нові ідеї та підходи. А інновації, як відомо, – це запорука розвитку правоохоронного відомства, інструмент, який стає реальною зброєю у боротьбі зі злочинністю. Саме тому на важливості використання інновацій у роботі міліції постійно наголошує керівництво Міністерства внутрішніх справ, особливо у контексті реформування правоохоронної системи України.

Одержано 06.11.2013

УДК 343.346.8

Володимир Михайлович СТРУКОВ,
кандидат технічних наук, доцент,
завідувач кафедри інформаційних технологій та захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ,
Володимир Володимирович ТОРЯНИК,
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційних технологій та захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ТЕХНОЛОГІЇ ПРОТИДІЇ РОЗСЛІДУВАННЮ МЕРЕЖЕВИХ КІБЕРЗЛОЧИНІВ

В сучасних умовах стрімкого поширення інформаційних технологій нагальною стає проблема координації діяльності правоохоронних структур та правового унормування зон відповідальності відомств, процедур взаємодії та засобів комплексного реагування на кіберзлочини, а також попередження таких злочинів [1]. В Україні органом, на який покладаються повноваження щодо розслідування злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України» [2]. У доктрині інформаційної безпеки України [3] окремою загрозою визначено лише прояви комп'ютерної злочинності та тероризму, що загрожують функціонуванню національних інформаційно-телекомунікаційних систем. Але в сучасних реаліях активізації кіберзлочинності комп'ютерні злочини є складовою всіх загроз негативного інформаційного впливу.

Середовищем, що сприяє розвитку кіберзлочинності є комп'ютерні мережі, технічні особливості котрих утруднюють процедури документування злочину та пошуку злочинця. Існує низка мережевих технологій здійснення негативного впливу на інформаційну сферу життєдіяльності суспільства, які можуть застосовуватись терористичними та екстремістськими організаціями та кримінальними структурами, сприяючи збереженню їх анонімності [4, с. 119].

Проаналізуємо деякі актуальні мережеві технології анонімного використання комп'ютерної мережі з точки зору складності та ефективності процедур документування кіберзлочинів та ідентифікації зловмисників.

1. Відкритий проксі-сервер – сервер, що обробляє запити від будь-яких IP-адрес в Інтернеті, на відміну від звичайних проксі-серверів, якими користується обмежена кількість довірених осіб зазвичай в зоні відповідальності власника проксі-сервера – наприклад, в локальній мережі. Відкритий проксі-сервер дозволяє практично будь-якому вузлу мережі звертатися через себе до інших вузлів мережі. При цьому, коли говорять про відкриті проксі-сервери, то часто мають на увазі анонімні відкриті проксі-сервери, які приховують реальні IP-адреси клієнтів і тим самим надають можливість анонімно користуватися послугами мережі Інтернет (відвідувати сайти, брати участь у форумах). Це представляє певну проблему, оскільки подібна анонімність може дозволити безкарно порушувати закон і умови надання послуг в мережі [5].

2. VPN (англ. – Virtual Private Network) – узагальнена назва технологій, що дозволяють забезпечити кілька мережевих з'єднань (логічну мережу) поверх іншої мережі (наприклад, інтернет). Незважаючи на те, що комунікації здійснюються по мережах з меншим або невідомим рівнем довіри (наприклад, по публічних мережах), рівень довіри до побудованої логічної мережі не залежить від рівня довіри до базових мереж завдяки використанню засобів криптографії (шифрування, аутентифікації, інфраструктури відкритих ключів, та ін.) [6].

3. Tor (англ. – The Onion Router) - система, що дозволяє встановлювати анонімне мережеве з'єднання, захищене від прослуховування. Розглядається як анонімна мережа, що надає передачу даних в зашифрованому вигляді. За допомогою Tor користувачі можуть зберігати анонімність при відвідуванні веб-сайтів, публікації матеріалів, відправці повідомлень і при роботі з іншими додатками, що використовують протокол TCP. Безпека трафіку забезпечується за рахунок використання розподіленої мережі серверів (нод-«вузлів»), званих «багатошаровими маршрутизаторами» (onion routers). Технологія Tor також забезпечує захист від механізмів аналізу трафіку, які ставлять під загрозу не тільки анонімність користувача, але також конфіденційність бізнес-даних, ділових контактів тощо. Tor оперує мережевими рівнями onion-

маршрутизаторів, дозволяючи забезпечувати анонімні вихідні з'єднання і анонімні приховані служби [7].

Очевидно, розглянуті технологій анонімності в мережі можуть бути істотним інструментом зловмисної протидії документуванню та розслідуванню кіберзлочинів. Цю обставину необхідно враховувати при розробці стратегії розслідування кіберзлочинів, принаймні, у двох аспектах. По-перше, у технічному аспекті, залучати експертів для фіксації помилок та недосконалостей використовуваних зловмисниками технологій анонімності. По-друге, у законодавчому аспекті, проводити системну законодавчу роботу щодо правого механізму вибіркового блокування анонімного сегменту Інтернету.

Список використаних джерел:

1. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : аналіт. записка [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/454.

2. Про внесення зміни до Закону України «Про ратифікацію Конвенції про кіберзлочинність» : закон України [Електронний ресурс]. – Режим доступу: http://zakon. rada.gov.ua/laws/ show/2532-17.

3. Про Доктрину інформаційної безпеки України : указ Президента України від 8 лип. 2009 р. № 514/2009 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/514/2009.

4. Федотов Н. Н. Форензика – компьютерная криминалистика / Н. Н. Федотов. – М. : Юрид. Мир, 2007. – 432 с.

5. Открытый прокси-сервер [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/Открытый_прокси.

6. VPN [Електронний ресурс]. – Режим доступу: http://wikipedia.org/wiki/VPN.

7. Tor [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/Tor.

8. Борьба с анонимностью в интернете [Електронний ресурс]. – Режим доступу: http://www.itar-tass.com/politika/661406.

Одержано 19.11.2013

УДК 343.983.25,004.9

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент,
професор кафедри захисту інформації
факультету підготовки фахівців для підрозділів
боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ЗАРУБІЖНИХ ПРОГРАМ ПІДТРИМКИ КОМП'ЮТЕРНО-ТЕХНІЧНИХ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ

При проведенні експертних досліджень у процесі розслідування кіберзлочинів, приймаючі до уваги швидкий розвиток інформаційних технологій, потрібно вирішувати цілий ряд складних питань відносно інструментарію дослідження, а саме:

– вибір відповідного наявного інструментарію проведення конкретних експертних досліджень;

– розуміння принципів функціонування та довіра до коректності роботи інструментарію, наприклад у вигляді доступних результатів незалежних випробувань;

– наявність методики експертного дослідження для конкретних обставин розслідування та ін.

Підтримка у вирішенні зазначених питань можлива при наявності постійно діючих, відкритих для усіх зацікавлених сторін, програм моніторингу, аналізу, упорядкуванню і випробуванню інструментарію експертного дослідження при розслідуванні кіберзлочинів.

Подібна сукупність програм започаткована і функціонує під егідою Лабораторії Інформаційних Технологій (Information Technology Laboratory, ITL) Національного Інституту Стандартів і Технологій (National Institute of Standards and Technology, NIST) Департаменту торгівлі США (U.S. Department of Commerce). Серед цілої сукупності програм можна виділити такі:

– The National Software Reference Library (NSRL) – Національна довідкова бібліотека програмного забезпечення для правоохоронних органів і інших організацій, які проводять комп'ютерні експертні дослідження (computer forensics investigations) (http://www.nsrl.nist.gov);

– Computer Forensic Reference Data Sets (CFReDS) – база довідкових даних для комп'ютерних експертних досліджень, яка може використовуватися при перевірці коректності інструментарію експертних досліджень, навчанні і атестації

експертів, порівнянні отриманих результатів із зразковими та ін. (http://www.cfreds.nist.gov);

– Computer Forensics Tool Catalog (CFTT) – каталог інструментарію комп'ютерного експертного дослідження, який є результатом програми по розробці процедур і критеріїв випробувань методик та інструментарію експертних досліджень, власне випробувань інструментарію, каталогізації результатів випробувань (http://www.cftt.nist.gov/tool_catalog/index.php).

CFTT має три основних розділи: пошук інструментарію за функціональними можливостями; класифікація (таксономія) функцій і технічних параметрів інструментарію; сервіс для постачальників і розробників інструментарію щодо постійного оновлення каталогу. Інструментарій каталогізовано за такими областями експертних досліджень: Cloud Services, Deleted File Recovery, Disk Imaging, Email Parsing, File Carving, Forensics Boot Environment, Forensic Tool Suite (Mac Investigations), Forensic Tool Suite (Windows Investigations), Hardware Write Block, Hash Analysis, Instant Messenger, Media Sanitization/Drive Re-use, Memory Capture and Analysis, Mobile Device Acquisition and Analysis, P2P Analysis, Remote Capabilities/Remote Forensics, Social Media, Software Write Block, Steganalysis, String Search, Web Browser Forensics, Windows Registry Analysis.

Використання можливостей NSRL, CFReDS, CFTT при навчанні і атестації експертів, і власне при проведенні експертних досліджень дозволить якісно підвищити ефективність розслідування кіберзлочинів правоохоронними

Одержано 07.11.2013

УДК 343.1

Юрій Валерійович ЛИСЮК,
кандидат юридичних наук, доцент,
начальник відділення юридичного забезпечення
Одеського державного університету внутрішніх справ

СУЧАСНІ ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ СИСТЕМИ: ПРИВІД ДО ВЧИНЕННЯ ЗЛОЧИНІВ

Права і свободи людини в будь-якій галузі права на кожному етапі становлення людства залишаються постійним об'єктом щодо здійснення правопорушень та посягань з боку

різного роду осіб. Незважаючи на те, що дана проблематика обговорюється та досліджується багато років, все ще залишаються невирішеними суттєва кількість питань, більше того з впровадженням в дію нових нормативно-правових актів з'являються нові аспекти, які інколи потребують набагато більше часу для їх вивчення та дослідження. Отже, на нашу думку, проблематика дотримання прав і свобод людини ніколи не буде вичерпана, а навпаки тільки сильніше буде привертати увагу багатьох науковців і практиків в різних галузях права, аспектах та проявах.

Одним із таких сучасних проявів порушень прав людини є стрімке зростання різного роду правопорушень та злочинів у сфері інформаційних та комп'ютерних мереж. На сьогодні, жодна людина не визначить, що цей розвиток сучасних інформаційних технологій не був виправданим, оскільки на сьогодні не тільки не вбачається, але й не можна собі уявити життя без сучасних інформаційних, комп'ютерних, технічних систем, які суттєво допомагають існувати в цей непростий час.

Сучасний розвиток сучасних інформаційних технологій став приводом для здійснення правопорушень у цій сфері та в багатьох випадках має ознаки злочинів, які свідомо та навмисно порушують права людини, в більшості з корисливих спонукань та мотивів. Отже, можемо констатувати, що розвиток сучасних інформаційних технологій несе з собою, як позитивні, так і негативні тенденції. Якщо аналізувати статистику, то треба зазначити, що все більша кількість людей користується всіма можливими електронними засобами, це стосується всіх без виключення сфер життєдіяльності людини, будь-то спілкування, торгівля, сплата рахунків, отримання заробітної плати та інші. Так, безумовно, багато в чому ці електронні системи спростили життя населення але поступово спричинили підвищений інтерес з боку інших кримінально налаштованих осіб, метою яких стало порушення прав людини та заволодіння складовими цих електронних засобів, спричинення майнової шкоди, що врешті-решт викликало появу нового виду злочинів – кіберзлочинність.

Права людини в будь-якій державі світу – це фундаментальні основи від яких прямо залежить розвиток держави, їх правовий, економічний та соціальний статус. В цьому сенсі, дотримання, реалізація та захист прав людини в державі виступають ключовим гарантом діяльності всієї держави. На

жаль, порушення прав людини у сфері кіберзлочинності не оминули і нашу державу, де останнім часом спостерігається посилення цієї проблематики, але поряд з цим наша держава докладає значних зусиль для того, що протистояти цій всезагальної системної проблеми.

Як вбачається з чинного законодавства України Конституція України є основним законом держави, який регулює суспільні відносини, що складаються в процесі здійснення фундаментальних засад організації суспільства й держави, де ключовою точкою між суспільством та державою є сама людина, його головна цінність, її права та свободи.

Отже, Конституція України закріплює, що людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнаються найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави. Відповідно до ст. 21 Конституції усі люди є вільними і рівними у своїй гідності та правах. Права і свободи людини є невідчутними та непорушними [1].

В цьому розрізі необхідно зазначити, що незважаючи на те, що Конституцією України прямо визначено про непорушність прав людини, вона все ж таки відчуває окремі порушення її прав, особливо це знаходить своє відображення у сфері кримінального провадження, основним завданням якого є захист прав людини від протиправних посягань, в тому числі від кіберзлочинності або злочинів які вчиняються з використанням комп'ютерних систем та мереж електрозв'язку.

Так, згідно із ст. 2 нового Кримінального процесуального кодексу України основним із завдань кримінального провадження є захист особи від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також те, що жодна особа не може бути піддана необґрунтованому процесуальному примусу і до кожного учасника кримінального провадження повинна бути застосована належна правова процедура, що в повній мірі відноситься й до проваджень відносно кіберзлочинів.

Враховуючи те, що більшість випадків, в яких здійснюються порушення прав людини з використанням комп'ютерних систем та мереж електрозв'язку мають ознаки злочинів, то вони підпадають під дію ст. 215 КПК України, яка

чітко передбачає, що порядок проведення досудового розслідування таких злочинів здійснюється у формі досудового слідства. Відповідно до ст. 214 цього ж Кодексу, досудове розслідування починається з моменту реєстрації повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення обставин, що можуть свідчити про вчинення кримінального правопорушення та внесення відомостей до Єдиного реєстру досудових розслідувань. Керівник органу досудового розслідування самостійно вирішує питання щодо особи, яка буде його проводити [2].

Повертаючись до питання злочинів, що вчиняються з використанням комп'ютерних систем та мереж електрозв'язку, треба зазначити, що порядок єдиний та чітко встановлений нормами зазначеного Кодексу. Отже, термін кіберзлочинності в офіційних нормативно-правових актах не визначений але поряд з цим він існує та закріпився в термінології правоохоронних органів, зокрема в міжнародних правових актах та конвенціях. Кіберзлочинність вважається досить новим видом злочинів, проте на відміну від традиційних крадіжок і шахрайства, вона постійно удосконалюється нарівні з новими технологіями, що у свою чергу ускладнює виявлення та протидію таким злочинам [3].

Так, кіберзлочинність включає в себе злочинність у сфері комп'ютерної інформації і телекомунікацій, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для електронних систем, а також інші види злочинності [3]. Одним із найпоширеніших злочинів у цій сфері, на наш погляд, слід вважати злочини, які стосуються розголошення конфіденційної інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційну інформацію, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства й держави, за допомогою різного роду сучасних інформаційних систем та технологій. Як вже наголошувалося, у світі останнім часом розробляється багато нових та вдосконалюються вже існуючі електронні інформаційні системи, що постійно стають об'єктами вчинення злочинів.

Так, найбільш розповсюдженими злочинами у сфері інформаційних систем є злочини, що відносяться до фінансового сектору економіки, а саме банківська сфера. Банківська сфера, на сьогодні, становить досить криміногенну сферу, в

якій з одного боку зосереджується питома вага цінностей людей, а з іншого використовуються найсучасніші технічні засоби для вчинення шахрайства з платіжними картками [4]. Однак, треба підкреслити, що не все залежить від самих злочинців, їх сучасного обладнання, оскільки велика частина залежить й віктимологічних дій самих людей, тому що вони часто діють необачно, а в деяких випадках надмірно довіряють іншим громадянам.

Більше того, стан законодавчої і нормативної бази у сфері кібернетичної злочинності в цілому можна охарактеризувати як недосконалий через наявну безсистемність і відсутність термінологічної визначеності в базових поняттях, що найчастіше призводить до порушення прав людини та неможливості притягнення винної особи до юридичної відповідальності.

Таким чином, можна зробити висновок про те, що нинішній стан забезпечення прав і свобод людини під час здійснення кримінального провадження, зокрема у сфері кіберзлочинності, знаходиться на досить проблематичному рівні та потребує більш рішучих заходів зі сторони правоохоронних органів, а також вдосконалення існуючої законодавчої і нормативно-правової бази для більш ефективної протидії кіберзлочинності.

Однак, для повного, об'єктивного та неупередженого забезпечення кримінального провадження, необхідно правильно та чітко діяти відповідно до законів та норм права, розуміти та вимагати від суб'єктів кримінального провадження дій, що передбачені законом і лише тоді можна буде розраховувати на позитивний результат та вести розмову про ефективність протидії кіберзлочинності. Крім цього, в розрізі запобігання цим видам злочинів вагома частина буде залежати від самої людини, їх обережності, особливо в частині збереження своєї конфіденційної інформації та персональних даних для захисту своїх прав та інтересів. Втім вказані питання підлягають подальшому дослідженню.

Список використаних джерел:

1. Конституція України : прийн. на 5-й сесії Верховної Ради України 28 черв. 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Кримінальний процесуальний кодекс України : закон України від 13 квіт. 2012 р. № 4651-VI // Голос України. – 2012. – 19 трав. – № 90–91.

3. Кіберзлочинність в Україні [Електронний ресурс]. – Режим доступу: http://www.science-community.org/ru/node/16132.

4. Кіберзлочинність: зміст та методи боротьби [Електронний ресурс]. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/tppe/2009_19/Zb19_48.pdf.

Одержано 18.11.2013

УДК 65.012.8+004

Олександр Володимирович МАНЖАЙ,
кандидат юридичних наук, доцент,
доцент кафедри захисту інформації
факультету підготовки фахівців
для підрозділів боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ,
Ірина Анатоліївна ОСЯТИНСЬКА,
вчитель інформатики
Харківської спеціалізованої школи з поглибленим вивченням
окремих предметів № 133 «Ліцей мистецтв»

ВСТАНОВЛЕННЯ ТА ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ ОСОБИ ЗА ЇЇ МЕРЕЖНИМИ ІДЕНТИФІКАТОРАМИ

У сучасній методиці боротьби з кіберзлочинністю одним з проблемних питань залишається встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами, тобто за тими обліковими даними, які особа залишила по собі в мережі. Як правило, такими ідентифікаторами виступають адреса електронної поштової скриньки, нікнейм у форумі, профіль соціальної мережі тощо. Вказана проблема нерідко обумовлена підвищеним рівнем анонімності, що реалізується за допомогою різного роду розподілених ресурсів (проксі-сервери, шели) та використанням спеціалізованих захищених мереж (TOR, I2P).

Враховуючи наведене, можна окреслити декілька напрямів щодо визначення місцезнаходження особи за її мережними ідентифікаторами.

По-перше, це встановлення особи за допомогою офіційного запиту до власника ресурсу або провайдера (оператора) телекомунікацій. У зв'язку з тим, що значна кількість розподілених ресурсів розташована за межами національної юрисдикції, такий спосіб часто не дає бажаного результату (складний процес, зволікання або взагалі відсутність відповіді).

Другим способом встановлення особи може виступати пошук інформації за певним ідентифікатором за допомогою різного роду сервісів та ресурсів. Для цього, перш за все,

необхідно скористатися можливостями Інтегрованої інформаційно-пошукової системи органів внутрішніх справ. У рамках використання даного способу також можуть бути застосовані пошукові системи Google, Rambler, Yandex, Yahoo тощо. Пошук доцільно продовжити в соціальних мережах, таких як www.odnoklassniki.ru, www.vkontakte.ru, www.facebook.com тощо. Також можна спробувати здійснити пошук особи серед зображень облич (www.facesaerch.com) та з використанням сайту www.radaris.com. В разі якщо отриманих відомостей не вистачає, необхідно скористатися іншими інформаційними ресурсами (наприклад, www.nomer.org, lookup.com), зокрема, приватними базами, які надають інформацію для маркетингових досліджень. Якщо у наявності є електронне поштове відправлення шуканої особи, слід ретельно проаналізувати його заголовок та вибудувати маршрут руху листа для планування подальших дій.

Одним із способів встановлення особи за мережним ідентифікатором є використання систем відновлення паролів різних ресурсів. Зокрема, таким чином можна встановити номери телефонів [1], віднайти профіль особи у соціальних мережах тощо. У подальшому, аналізуючи зміст та геопозначки відповідних фотографій можна встановити місця перебування особи у певний проміжок часу. Знаючи місця пересування особи, можна у 95 % випадків однозначно її ототожнити, що на практиці було доведено дослідниками з Масачусетського технологічного інституту (MIT) і Католицького університету в Левені [2].

Крім зазначених способів встановити особу та ототожнити її можливо також оперативним шляхом через здійснення низки заходів.

Слід відмітити, що наведені способи не є вичерпними. Багато в чому конкретна методика встановлення особи залежить від наявної ситуації, тому оперативному працівнику та слідчому для ефективної реалізації описаного у даній роботі завдання слід бути не лише юридично, але й технічно обізнаним працівником та постійно підвищувати свій професійний рівень, відслідковуючи новітні методики та розробки, які зможуть допомогти у вирішенні завдань боротьби зі злочинністю.

Список використаних джерел:

1. Соцсети позволяют легко найти номера мобильных телефонов многих пользователей [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/440882.php.

2. Unique in the Crowd: The privacy bounds of human mobility [Електронний ресурс] / Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, Vincent D. Blondel. – Режим доступу: http://www.securitylab.ru/news/440882.php.

Одержано 13.11.2013

УДК 65.012.8+004

Олександр Володимирович МАНЖАЙ,
кандидат юридичних наук, доцент,
доцент кафедри захисту інформації
факультету підготовки фахівців
для підрозділів боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ,
Микола Миколайович ПЕРЕПЕЛИЦЯ,
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ

УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ НА БАЗІ ПРОГНОСТИЧНОГО АНАЛІЗУ

Зростання рівня кіберзлочинності з кожним роком невпинно пришвидшується. Цей процес потребує своєчасного та адекватного реагування державних органів. Одним з елементів такого реагування виступає якісна організація протидії високотехнологічним злочинам, яка має базуватися на прогностичній основі.

Експерти Європолу вважають, що до 2020 року межа між кібератакою та фізичним нападом на людину у багатьох випадках буде стерта. Найбільш поширеними комп'ютерними атаками стануть:

1. Розвиток ринку скремблерів розпізнавання настрою користувачів, симуляції дистанційної присутності, технології Near Field Communication.

2. Розподілені DoS-атаки через хмарні сервіси.

3. Використання хмарних ботнетів і розподілених обчислювальних ресурсів.

4. Сталий ринок викрадених та підроблених віртуальних елементів.

5. Розподілені захищені кримінальні обчислення.

6. Фізичні атаки на дата-центри і точки обміну трафіком.

7. Електронні атаки на критичну інфраструктуру, включаючи джерела енергії, транспорт й інформаційні служби.

8. Мікрозлочинність, включаючи крадіжку і генерацію фальшивих мікроплатежів.

9. Біозломи елементів багатофакторної автентифікації.

10. Насильство проти людей з використанням комп'ютерів, поява шкідливих програм для людей.

11. Війни киберугруповань.

12. Кваліфікована кримінальна розвідка, включаючи дата-майнінг великих об'ємів даних.

13. Збільшення атак імперсонації.

14. Складні маніпуляції з репутацією.

15. Підміна реальних даних та шахрайства з використанням соціального інженірінгу.

16. Використання безпілотних апаратів і роботів в злочинних цілях.

17. Хакреські атаки проти сполучних пристроїв з безпосереднім доступом (міжмашинні комунікації, індикатори відображення важливої інформації – Heads-Up Display тощо) [1]

Враховуючи наведені тенденції потребує якісного переосмислення й організаційна структура боротьби з кіберзлочинністю в Україні. Відповідну модернізацію слід проводити, враховуючи ефективність, яку показала та або інша організаційна структура за час свого існування в інших країнах.

Для проведення відповідного аналізу слід брати не лише емпіричну базу розвинених країн, але й таких, що розвиваються, оскільки не можна відкидати цінні ідеї, базуючись лише на усталених авторитетах.

Структурні елементи світової організації боротьби з кіберзлочинністю можна умовно поділити на міжнародні та національні. До міжнародних слід віднести такі органи як Інтерпол, Європол та інші міжнаціональні правоохоронні органи. Окремі елементи національної структури боротьби з кіберзлочинністю наведено на рис. 1.

Базуючись на аналізі ефективності, яку показав орган протидії кіберзлочинності у тій або іншій країні, можна адоптувати відповідні позитивні новели в українських державних органах, що виконують аналогічні завдання, шляхом впровадження відповідних норм до діючого законодавства.

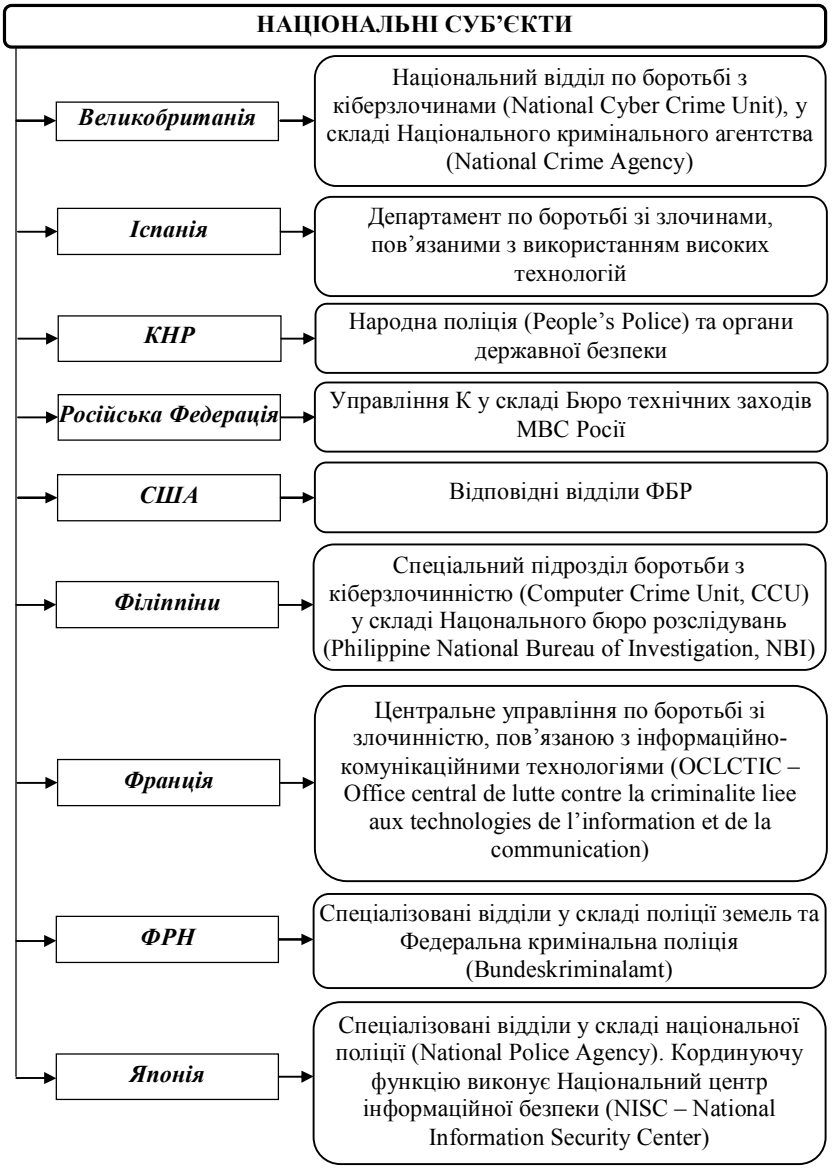

Рис. 1. Національні державні органи протидії кіберзлочинності

Список використаних джерел:

1. Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers [Електронний ресурс] / Европейский центр по борьбе с киберпреступностью при Европоле. – 25 р. – Режим доступу: https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf.

Одержано 20.11.2013

УДК 343.98

Андрій Михайлович ЩЕРБАКОВСЬКИЙ,
здобувач
Харківського національного університету внутрішніх справ

ОТРИМАННЯ ІНФОРМАЦІЇ ПРО ОЗНАКИ КІБЕРЗЛОЧИНІВ ЕКОНОМІЧНОЇ СПРЯМОВАНОСТІ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Згідно зі ст. 214 КПК України досудове розслідування починається після подання заяви, повідомлення про вчинене кримінальне правопорушення і внесення відповідних відомостей до Єдиного реєстру досудових розслідувань. При вчинені в сфері економіки злочинів з використанням комп'ютерних технологій (засобів та програмного забезпечення) в таких заявах, повідомленнях повинна міститься інформація, яка б відбивала ознаки злочинних посягань. Такі ознаки можуть бути в певних випадках встановлені володільцями електронних інформаційних систем.

Виявлення ознак кіберзлочинів економічної спрямованості полягає в цілеспрямованому процесі виявлення в електронних інформаційних системах або локальних обчислюваних мережах (далі - мережах) порушень, пов'язаних з несанкціонованим доступом до інформації, використанням і поширенням шкідливих програм і порушенням правил експлуатації, що призвело до знищення, блокування й модифікації конфіденційної інформації.

Порушення в роботі мережі, які надалі трактуються як ознаки кіберзлочинів, можуть бути обумовлені проявом наступних погроз інформаційної безпеки: несанкціонованого доступу до інформації; атакою комп'ютерних вірусів; спеціальним програмно-технічним впливом; внесенням й ініціалізацією недекларованих можливостей (закладок); порушенням надійності функціонування компонентів мережі і т. д.

У відповідності до ст. 361, 361-1, 362 КК України, реалізація першої погрози інформаційної безпеки відноситься до несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж; встановлення другій-четвертої погроз слід розглядати як створення, використання й розповсюдження шкідливих програм. Поява п'ятої погрози пов'язана із злочинним діянням або халатним відношення до службових обов'язків особи, яка має право доступу до мережі.

Виявлення ознак кіберзлочинів, особливо тих, що вчиняються із використанням засобів дистанційного доступу, здійснюється на основі систематичного контролю порядку експлуатації мережі. Об'єктами посягання при вчинені кіберзлочинів є, насамперед, інформація економічного характеру. Тому, методи й інструментальні засоби виявлення ознак кіберзлочинів повинні забезпечувати виконання наступних основних завдань:

1) встановлення факту яких-небудь порушень у роботі програм або неправомірного доступу до конфіденційної інформації економічного характеру;

2) визначення факту порушення експлуатаційної безпеки мережі в цілому, що призвело до невиконання (викривленню процесу виконання) функціональних завдань або розкраданню інформації з використанням електронних засобів доступу;

3) формування вихідних даних для попередньої оцінки нанесеної шкоди, обсяг якій обумовлює необхідність проведення досудового розслідування.

Доцільно методи й інструментальні засоби виявлення ознак кіберзлочинів у мережах, вчинених з дистанційним доступом, об'єднати в єдину систему комплексного адміністрування інформаційної безпеки. Застосування системи адміністрування дозволяє з високим ступенем імовірності виявляти ознаки кіберзлочинів.

Технологія виявлення ознак кіберзлочинів включає основні дії адміністратора інформаційної безпеки в процесі виконання своїх обов'язків, організаційно-технічні заходи і інструментальні засоби, і складається з наступних компонентів:

а) функції адміністратора, що передбачають діагностику стану й порушень у роботі мережі;

б) процеси спостереження за суб'єктами й об'єктами адміністрування й здійснення практичних дій адміністратором;

в) інструментальні засоби адміністрування, що включають засоби захисту, вбудовані в загальне програмне забезпечення, засоби безпеки локальних обчислювальних мереж і телекомунікаційних систем, тестове програмне забезпечення, засоби моніторингу технічного устаткування й спеціальні засоби інформаційної безпеки.

Технологія виявлення ознак кіберзлочинів економічної спрямованості включає наступні взаємозалежні процедури:

1) адміністрування інформаційної безпеки програмного забезпечення;

2) сканування інформаційних і обчислювальних ресурсів мережі;

3) контроль забезпечення надійності функціонування мережі на основі перевірки дотримання правил експлуатації;

4) аналіз діагностичних повідомлень у системних журналах і оцінка проявів впливів;

5) виявлення джерел порушень і впливів на рівні структур даних, програмного забезпечення, окремого автоматизованого робочого місця, мережі, засобів дистанційного доступу й суб'єктів доступу;

6) локалізація порушень і деструктивних впливів у структурі мережі;

7) попередня оцінка шкоди.

Суб'єктами адміністрування є оператори мережі, обслуговуючий персонал і будь-які особи, що перебувають на об'єкті інформатизації державного підприємства або комерційної організації. Виконання робіт з адміністрування інформаційної безпеки може здійснюватися як на основі застосування тільки організаційно-технічних заходів, застосування окремих інструментальних засобів, так і шляхом застосування автоматизованих засобів комплексного адміністрування інформаційної безпеки й супроводу програмного забезпечення мережі.

Організаційно-технічні заходи дозволяють виявити порушення в системі доступу, оснастити об'єкт інформатизації відповідним технічним устаткуванням, сформувати паперові й електронні засоби фіксації подій і порушень у мережі. Вказані заходи включають наступне: розміщення технічних засобів охорони для виявлення зовнішніх потенційних порушників; здійснення контролю доступу суб'єктів у службові приміщення; створення спеціальної служби інформаційної

безпеки, призначення адміністратора інформаційної безпеки й визначень повноважень і прав по доступу до інформації; планування заходів щодо інформаційної безпеки; ведення експлуатаційної документації; проведення профілактичних і регламентних робіт; експертизу експлуатаційної документації й протоколювання позаштатних ситуацій; атестацію співробітників по знанню вимог інформаційної безпеки. Усі зроблені адміністратором інформаційної безпеки дії й події, що відбуваються в мережі, повинні в обов'язковому порядку документуватися в електронному виді в системних журналах і на паперовому носії в журналі контролю експлуатаційної безпеки програмного забезпечення.

Таким чином, приведення технологія дозволяє забезпечити встановлення ознак кіберзлочинів у мережі на основі комплексного адміністрування інформаційної безпеки програмного забезпечення й обчислювальних ресурсів і застосування інструментальних засобів. Інформація, що містить ознаки кіберзлочинів. Слугує підставою для обґрунтованого початку кримінального провадження.

Одержано 20.11.2013

УДК 343.1

Даліант Олександрович МАКСИМУС,
старший слідчий СВ Красногвардійського РВ
ДМУ ГУМВС України в Дніпропетровській обл.

ДЕЯКІ АСПЕКТИ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ ПРАЦІВНИКАМИ ОВС СОЦІАЛЬНИХ МЕРЕЖ ІНТЕРНЕТУ ДЛЯ РОЗПОВСЮДЖЕННЯ АУДІО-, ВІДЕО- ЧИ ТЕКСТОВОЇ ІНФОРМАЦІЇ

На даний момент, на теренах безкрайнього простору мережі Інтернет, існує великий різновид сайтів. Це можуть бути і інтернет-форуми, дошки оголошень, електронні бібліотеки, мультимедіа чи розважальні портали, тощо. Але найбільшою популярністю та значимістю для спілкування та розміщення приватних відео чи графічних матеріалів користувачами мережі Інтернет, мають так звані сайти – соціальні мережі.

Соціальні мережі Інтернету в країнах СНД набули популярності з другої половини 2000-х років. В соціальних мережах Інтернету користувач може створити сторінку для себе

як під своїм, так і під чужим ім'ям, може добавляти свої фотографії, писати свої думки, ділитись з іншими користувачами соціальної мережі аудіо чи відеозаписами. Іншими словами, якщо протоколи та сервіси електронного листування прискорили звичайне листування до швидкості світла, то соціальні мережі повністю змінили наше уявлення про можливості комунікації між людьми. За допомогою соціальних мереж можливо вести одночасне листування, перегляд відеоматеріалів та прослуховування тих чи інших звукових файлів одразу з сотнею, тисячею чи навіть десятьма тисячами користувачів у різних кутках світу. Іншими словами багато в чому такий вид комунікації є новацією та революцією, яка змінює сучасний світ. Вже не один рік продаж та реклама товарів через соціальні мережі Інтернету приносять міль'ярди доларів США, а телеканали та радіостанції мають в соціальних мережах свої персональні сторінки та постійно поновлюють їх новою інформацією.

Таким чином необхідно погодитись, що соціальні мережі надають користувачам дуже великі можливості по розповсюдженню інформації в текстовому, графічному та аудіо форматах між профілями інших користувачів соціальної мережі, а отже це може бути доцільним і для працівників органів внутрішніх справ. Інформація, яку може бути доцільно розповсюджувати через соціальні мережі, має наступні ключові особливості:

1) моментальність розміщення – адже печать оголошення в газеті, трансляція телепередачі, випуск новини в радіоефірі займає суттєвий проміжок часу, а публікація інформації в соціальній мережі є миттєвою;

2) безкоштовність – на відміну від газет та телерадіокомпаній, користування соціальними мережами майже без виключень є безкоштовним;

3) цільова аудиторія – користувач може сам обирати коло інших користувачів за віком, місцем проживання, статтю, місцем навчання, тощо, на відміну від інших засобів масової інформації;

4) динамічність – можливість редагувати, видаляти та доповнювати новими частинами опубліковану інформацію із плином часу та зміною навколишньої дійсності, що неможливо при використанні звичайних засобів масової інформації.

Стосовно використання соціальних мереж Інтернету працівниками ОВС, необхідно зазначити, що доцільно використовувати не одну, а хоча б три з чотирьох самих популярних на території СНД соціальних мереж: «ВКонтакте» (http://www.vk.com), «Facebook» (http://www.facebook.com), «Мой Мир» (http://www.my.mail.ru) та «Одноклассники» (http://www.odnoklassniki.ru), в яких би дублювалась уся інформація, яку необхідно розповсюдити в мережі Інтернет. Це може бути інформація наступного різнопрофільного характеру:

1) інформація про осіб, яких було об'явлено в розшук;

2) інформація та дезінформація для осіб, яких було об'явлено в розшук, чи для осіб, які підозрюються у вчиненні злочину;

3) новини чи повідомлення для громадян, стосовно правоохоронної діяльності ОВС України;

4) контактні дані конкретного підрозділу ОВС, необхідні для надіслання звернення у письмовій формі;

5) звернення громадян до конкретного підрозділу ОВС у електронній формі.

Слід зазначити, що створення персональної сторінки конкретного підрозділу ОВС України у соціальній мережі Інтернету необхідно узгоджувати з керівництвом ГУМВС України в конкретній області, а розміщена в подальшому на такій сторінці інформація – повинна суворо відповідати дійсності. Таким чином доцільним є створення як офіційних, так і легендованих персональних сторінок в соціальних мережах Інтернету. Офіційних – для певних підрозділів ОВС, а легендованих – для вигаданих і реально не існуючих осіб. Крім вищесказаного, враховуючи те, що в руках у кожного працівника, який займається створенням персональної сторінки в соціальній мережі Інтернету є можливість вибирати майже будь-яке ім'я, фотографію обличчя та фотографії дозвілля, контактні дані та багато інших вподобань чи поглядів на життя певної особи – використовуючи чужі фотографії (з дозволи чи без такого особи, яка зображена на фотографіях, вирішується на страх та ризик працівника оперативного підрозділу ОВС, і в цьому питанні важко щось порадити) можна створити персональну сторінку особи, яка виглядає, як кримінальний елемент, культурист, спортсмен, бізнесмен, дівчина – модель, особа, яка займається проституцією тощо.

Після створення будь-якої персональної сторінки в соціальній мережі, перш за все необхідно створити велике коло «друзів» в соціальній мережі. Статус «друзі» в соціальній мережі здебільшого надає такі можливості: 1) листуватись та надсилати крім текстових, також графічні, аудіо та відео файли; 2) дивитись особисті дані та фотографії своїх «друзів»; 3) надсилати своїм «друзям» оголошення та запрошення на ті чи інші заходи. Таким чином, та враховуючи те, що у всіх соціальних мережах Інтернету передбачений ліміт запрошень інших користувачів соціальних мереж у «друзі» 20–40 осіб на день, створення дійсно якісної та ефективно діючої в сенсі розповсюдження інформації сторінки – є процесом доволі тривалим, але реально можливим і для однієї людини, яка приділяє цьому процесу 10–15 хвилин на день, але кожен день на протязі декількох місяців. Також було виявлено просту закономірність при створенні достатньо великого кола «друзів» у соціальних мережах Інтернету: отримання позитивної відповіді від особи на запрошення до кола «друзів» тим простіше, чим більше вже існуюче коло «друзів». Тобто створення кола друзів з «нуля» до 50 осіб зайняло в середньому 16 днів, з 50 осіб до 100 осіб – ще 12 днів, зі 100 осіб до 200 осіб – ще 15 днів, від 200 осіб до 400 осіб – ще 25 днів.

Одержано 19.11.2013

УДК 65.012.8+004

Андрій Петрович КОСМИНЯ,
курсант
Харківського національного університету внутрішніх справ,
Кирил Олександрович ШЕПЕЛЬ,
курсант
Харківського національного університету внутрішніх справ

РОЗВИТОК МОБІЛЬНИХ ВІРУСІВ ДЛЯ ОПЕРАЦІЙНОЇ СИСТЕМИ «ANDROID»

З кожним днем збільшується кількість фінансових операцій за допомогою смартфонів. Їх використання є досить зручним та дозволяє швидко, незалежно від місця та часу, здійснювати операції у сфері електронної комерції.

Популяризація використання смартфонів, а саме їх можливості у сфері грошових операцій не залишили без уваги і кіберзлочинців, які, як відомо, оперативно відслідковують

сфери фінансових потоків. Для реалізації своєї злочинної мети вони шукають вразливості в операційних системах, розробляють шкідливе програмне забезпечення – мобільні віруси.

За даними дослідження ФБР найбільш вразливими для таких вірусів є мобільні пристрої на базі операційної системи «Android». На дану операційну систему була здійснена найбільша кількість хакерських атак, близько 79 %, слідом за нею «Symbian» –19 %, «WindowsMobile» і «BlackBerry» – по 0,3 % відповідно, «IOS» – 0,7 %, на інші операційні системи припало 0,7 % [1].

З метою поширення шкідливого програмного забезпечення кіберзлочинці використовують різні методи. Наприклад, метод соціальної інженерії, де під виглядом завантаження антивірусного програмного забезпечення встановлюється троянська програма – Android.Sms.Send, або під виглядом окремого інсталяційного пакета для безкоштовного програмного забезпечення.

Існують такі модифікації троянської програми «Android.Sms.Send»:

– 412 (поширюється у вигляді браузера);

– 468 (клієнтська програма соціальної мережі «Одноклассники»);

– 764 (медіаплеєр) [2].

Дана троянська програма призначена для відправки повідомлень на короткі номери, де проходить висока тарифікація дзвінка, для крадіжки особистих даних користувача, а також для оформлення платних підписок.

Переважна кількість даних троянських програм поширюється у вигляді окремих інсталяційних пакетів, що мають розширення «.apk», у вигляді окремого інсталяційного пакета для безкоштовного програмного забезпечення, чи у вигляді рекламного рекомендованого сповіщення для інстальованого програмного забезпечення (під виглядом пропозиції оновлення).

Також дослідницькою групою BlueboxLabs була виявлена вразливість в операційній системі «Android», що дозволяє змінити код «.apk», при цьому не пошкоджуючи криптографічний підпис застосування. Дана вразливість дає можливість перетворити будь-яке підписане застосування у троянську програму [3].

Також відома нова схема, яку часто використовують кіберзлочинці. Вони розсилають власникам мобільних телефонів СМС-повідомлення з гіперпосиланнями, перейшовши

за якими, користувач завантажує шкідливе програмне забезпечення, що дозволяє без його участі здійснювати можливі банківські операції.

Останнім часом у мережі все більше з'являється вебсайтів, подібних за оформленням до GooglePlay, де пропонують відвідувачам під виглядом ліцензійного шкідливе програмне забезпечення.

За результатами опитування компанії «B2BInternational» і «Лабораторії Касперського», станом на червень 2013 року, 38 % користувачів смартфонів на операційній системі «Android» не використовують антивірусне програмне забезпечення [4].

Тому, якщо виявлено що смартфон заражений вірусом необхідно:

– вийняти SIM-карту, щоб уберегтись від відправки неконтрольованих SMS-повідомлень;

– ізолювати смартфон від доступу до мережі Internet, щоб уникнути витоку інформації;

– встановити антивірусне програмне забезпечення та просканувати телефон.

Список використаних джерел:

1. ФБР предупредило об опасностях фрагментированной Android [Електронний ресурс]. – Режим доступу: http://tech.onliner.by/2013/08/28/android-9.

2. Обнаружена крупнейшая в мире бот-сеть на базе Android [Електронний ресурс]. – Режим доступу: http://www.ferra.ru/ru/soft/news/2013/09/20/drweb-200000-Android/.

3. 99 % Android-устройств подвержены уязвимости APK-файлов [Електронний ресурс]. – Режим доступу: http://www.comss.info/page.php?al=Android_APK_vulnerability.

4. Как спастись от мобильных вирусов [Електронний ресурс]. – Режим доступу: http://www.utro.ru/articles/2013/10/29/1153228.shtml.

Одержано 12.11.2013

УДК 343.451

Руслан Юрійович СЕНЬ,
курсант
Харківського національного університету внутрішніх справ,
Ярослав Олегович БАГЛАЙ,
курсант
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ DHCP-ПРОТОКОЛІВ У РОЗСЛІДУВАННЯХ КІБЕРЗЛОЧИНІВ

Сьогодні, у XXI столітті – столітті інновацій та розробок все більшу роль у житті людства відіграють комп'ютерні технології. Невпинно зростає кількість комп'ютерів – і як наслідок розширюються мережі. Для автоматизації їх роботи розроблено чимало протоколів.

DHCP (Dynamic Host Configuration Protocol) – один з найважливіших протоколів у стеку TCP/IP. Він призначає хостам різні параметри необхідні для роботи в мережі, зокрема, їх IP-адрес, адреси шлюзу, IP-адрес DNS-серверів і багато інших. DHCP значно полегшує налаштування мережі з великою кількістю хостів. Однак його недолік в тому, що він розроблявся без урахування критеріїв безпеки.

Проаналізувавши процедуру отримання мережних налаштувань, можна побачити, що ні сервер, ні клієнт ніяк себе не ідентифікують – інакше кажучи, в протоколі DHCP відсутній механізм автентифікації (як клієнта так і сервера). Клієнт не може бути впевнений що він отримав мережні налаштування з потрібного джерела, так само як і сервер не може перевірити клієнта. У цьому і полягає основна проблема протоколу DHCP і саме такий механізм роботи привів до появи різних методів атак. Найбільш поширені з них:

– прослуховування трафіку DHCP;
– DHCP starvation («голодування»);
– хибний DHCP-сервер у мережі.

Розглянемо в чому саме проявляється небезпека перерахованих вище атак.

Прослуховування трафіку DHCP

Завдяки прослуховуванню трафіку DHCP можливо отримати повну інформацію про адреси в мережі, адреси DNS серверів і т. д. Як наслідок – злочинцю легше вибрати свою «жертву» і не потрібно буде витрачати зайвий час на збирання інформації про мережу.

Помилкові DHCP-клієнти або виснаження пулу DHCP (DHCP starvation)

Дана атака полягає в передачі великої кількості запитів DHCP з підроблених MAC-адрес одночасно. Внаслідок цього зловмисник може повністю вичерпати адресний простір DHCP-серверу, й він не зможе обслуговувати нових клієнтів. Таким чином DHCP starvation можна класифікувати як DOS (Denial of service – відмова в обслуговуванні).

Хибний DHCP-сервер в мережі

У даній атаці зловмисник підставляє свій DHCP-сервер і видає свої налаштування користувачам мережі. Внаслідок чого він зможе прослуховувати мережу та скоювати інші несанкціоновані дії. Звичайно, можлива наявність інших DHCP-серверів, які також будуть відповідати на запити клієнтів. Але цю проблему дуже легко вирішити, попередньо скориставшись вищенаведеною атакою DHCP starvation, яка виведе зі строю працездатні DHCP-сервери.

На теперішній час основним методом боротьби з даними атаками є використання функції комутатора DHCP snooping. Ця функція дозволяє захистити клієнтів у мережі від атаки типу DHCP starvation шляхом порівняння MAC-адреси вказаного в DHCP-запиті і MAC-адреси, яка була прописана на порту комутатора. Якщо адреси однакові, то комутатор відправляє пакет далі. Якщо адреси не збігаються, то комутатор відкидає пакет. Також DHCP snooping захищає від неавторизованих DHCP-серверів у мережі, регулюючи потік повідомлень по портам, поділяючи їх на довірені (DHCP-відповіді, які проходять через ці порти не відкидаються) і не довірені (DHCP-відповіді, які проходять через ці порти відкидаються).

На думку деяких експертів, на теперішній час DHCP недостатньо відмовостійкий. Протоколу явно бракує механізму активного повідомлення клієнтів про екстремальні ситуації (наприклад, про нестачу адрес) та серверного підтвердження про звільнення адрес.

Отже, використовуючи протокол DHCP ми не тільки автоматизуємо та прискорюємо роботу мережі, але й допускаємо можливість виникнення проблем принципового характеру (несанкціоноване втручання й т. п.). Тобто, перед використанням протоколу потрібно оцінити можливі ризики внаслідок його використання.

Одержано 21.11.2013

А43 **Актуальні** питання розслідування кіберзлочинів : матеріали Міжнар. наук.-практ. конф., м. Харків, 10 груд. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2013. – 272 с.

У збірнику висвітлено погляди науковців та практиків щодо проблем правового, організаційного та кадрового забезпечення протидії кіберзлочинності, кримінально-процесуальних та криміналістичних проблем розслідування кіберзлочинів в Україні та використання інформаційних технологій і технічних засобів під час їх розслідування.

УДК 343.98:[343.3/.7:004](477)(063)
ББК 67.9(4УКР)623.19я431

Наукове видання

АКТУАЛЬНІ ПИТАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Матеріали
Міжнародної науково-практичної конференції

м. Харків, 10 грудня 2013 р.

Комп'ютерне верстання *Білоуса П. О., Зозулі А. О.*

Формат 60х84/16. Ум.-друк. арк. 15,87. Обл.-вид. арк. 13,72.
Тираж 200 пр. Зам. № 2013-24.

Видавець –
Харківський національний університет внутрішніх справ,
просп. 50-річчя СРСР, 27, м. Харків, 61080.
Свідоцтво суб'єкта видавничої справи ДК № 3087 від 22.01.2008.

Надруковано в ТОВ «Компанія "ВАІТЕ"»,
вул. Саперне поле, 26, кв. 27, м. Київ, 01042,
тел. (044) 531-14-32