6. Обмежити пересування підозрюваного на місці затримання.

7. Обмежити користування підозрюваного певною річчю (мобільним телефоном, персональним комп'ютером тощо).

8. Здійснити інші заходи з урахуванням конкретної ситуації.

Дотримання поліцейськими патрульної поліції вищевказаних криміналістичних рекомендацій, добросовісне виконання своїх обов'язків сприятиме своєчасному розкриттю та ефективному розслідуванню озброєного нападу на банківську установу.

Одержано 19.03.2019

УДК 343.85(477)

Марина Олександрівна КРАВЦОВА,
кандидат юридичних наук,
старший викладач кафедри кримінального права і кримінології факультету № 1
Харківського національного університету внутрішніх справ

«БЕЗПЕКОВІ» ФАКТОРИ ЛАТЕНТНОСТІ КІБЕРЗЛОЧИННОСТІ

У кримінологічній літературі під причинами виникнення та існування латентної злочинності прийнято розуміти сукупність обставин соціального, історичного, організаційного, кадрового, матеріального, правового, соціально-психологічного, технічного та іншого характеру, що заважають її виявленню та реєстрації, а також обліку злочинів, у тому числі забезпеченню повноти і всебічності їх розкриття.

Проблема латентної злочинності є однією з найбільш складних і актуальних для кримінології, її дослідженню присвячені роботи багатьох вчених, а саме: Р. М. Акутаєва, Є.М. Блажівського, Ю. Д. Блувштейна, К. К. Горяїнова, І. М. Даньшина, Г. І. Забрянського, А. Ф. Зелінського, О. Г. Кальмана, О. О. Ковалкіна, А. О. Конєва, О. М. Ларіна, Д. А. Лі, В. В. Лунєєва, В. В. Панкратова, В. М. Поповича, О. Г. Фролової, О. С. Шляпочнікова, Т. К. Щеглової та інших.

Що ж стосується безпосередньо кіберзлочинів, спеціальних досліджень рівня їх латентності як в Україні, так і за кордоном не проводилося. Кіберзлочинність – явище за своєю природою транскордонне, у зв'язку з чим, жоден комплексний кримінологічний аналіз не здатний дати повного уявлення про глобальні масштаби і тенденції кіберзлочинності.

Аналіз сукупності причин (факторів) латентності кіберзлочинів дозволяє виділити серед них такі, що безпосередньо залежать від користувача та базуються на недотриманні ним елементарних правил безпеки поводження в кіберпросторі. Це фактори, що обумовлюють природну латентність кіберзлочинів та фактори, пов'язані з негативною поведінкою жертви й очевидців злочину – нехтуванням необхідності звернення жертви та осіб, яким відомо про злочин, до правоохоронних органів та неповідомленням про факт вчинення злочину [3, с. 55].

Першу групу складають фактори, в силу яких про вчинений кіберзлочин відомо лише самому винному, і тому про небезпечність та поширеність злочину (злочинів) не стає відомо іншим. Це обумовлюється як складністю механізму вчинення кіберзлочинів, найрізноманітнішими можливостями (сферою та наслідками) їх вчинення, так і відповідною «комп'ютерною безграмотністю» більшості потенційних жертв кіберзлочинів. Так, наприклад, про несанкціоноване втручання в роботу ЕОМ (комп'ютерів), їх систем, комп'ютерної мережі чи мережі електрозв'язку або несанкціоновані дії з інформацією, яка оброблюється в ЕОМ (комп'ютерах), автоматизованій системі, комп'ютерній мережі або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, практично ніхто не дізнається внаслідок професійності вчинення таких злочинів з належним їх маскуванням під правомірні дії та приховуванням слідів, так і через неуважність чи безграмотність (прямий брак відповідних знань, навичок та досвіду – часто робить жертву нездатною усвідомлювати факт вчинення злочину) жертви злочину, або, як правило, через сполучення вказаних факторів.

Крім того, до даної групи факторів латентності кіберзлочинів слід віднести і безпосередні факти нехтування жертвою своєю безпекою. Користувачі комп'ютерних систем (від пересічного громадянина до серйозних державних органів та організацій) часто ігнорують заходи та засоби

комп'ютерної безпеки. Причиною цього є їх необачність або небажання витрачати «зайві кошти». Через відсутність необхідного обладнання, програмного забезпечення та відповідного персоналу (фахівців) часто більшість випадків несанкціонованого втручання в роботу ЕОМ (комп'ютерів), систем, комп'ютерної мережі, мережі електрозв'язку та вчинення інших кіберзлочинів залишається латентним.

Природну латентність кіберзлочинів може обумовлювати також і те, що факт вчинення злочину залишається взагалі нікому невідомий (навіть самому злочинцю, який не усвідомлює протиправність своїх дій). Як вказує А. І. Журба, деяких комп'ютерних фанатів відрізняє відсутність у них чітко вираженого відчуття протиправності своїх намірів. Практика свідчить, що всі дії здійснюються ними для реалізації своїх, нерідко побудованих на егоїстичних рисах, інтелектуальних і професійних здібностей. При цьому, інтереси інших осіб, зокрема потерпілих, повністю ігноруються [1, с. 100]. Вчені пов'язують це з недостатністю юридичних знань в осіб, які мають технічну освіту. Серед професіоналів досліджуваного виду злочинності такого недоліку не спостерігалося [2, с. 126].

Що стосується другої групи – факторів, пов'язаних з негативною поведінкою жертви (очевидців) злочину, то причини цього можуть бути різні. Найбільш поширеною причиною, через яку про факт вчинення кіберзлочину жертва не інформує правоохоронні органи, є її небажання привертати до себе їх увагу або громадськості взагалі. Як правило, це відбувається через те, що жертва злочину сама має відношення до протиправної діяльності. Звідси – бажання приховати свою злочинну чи незаконну діяльність, фінансові махінації або незаконне збагачення, ухилення від сплати податків, користування неліцензійним програмним забезпеченням тощо. Також це може відбуватися через небажання розкриття (розповсюдження) інформації особистого характеру – від елементарних інтимних моментів особистого життя до користування продукцією порноіндустрії тощо. При цьому, ситуація, коли жертва змушена «захищати» себе від розповсюдження відповідної «інформації» може створюватися (провокуватися) самими злочинцями. Так, наприклад, дуже поширеним залишається вимагання сплати «штраф» через розповсюдження вірусу, що блокує операційну систему, нібито у зв'язку з користуванням жертвою порноресурсами. Окремо слід зазначити проблему захисту бізнес-інтересів (інформації, іміджу фірми тощо), коли жертва злочину навіть попри заподіяну їй шкоду, намагається приховати (не розголошувати) факт вчинення злочину, побоюючись використання цього факту (інформації з ним пов'язаної) конкурентами чи іншими зацікавленими особами.

Причиною неповідомлення про вчинений кіберзлочин у правоохоронні органи може бути відповідне емоційне відношення до цього факту з боку жертви або очевидців. Якщо жертва злочину оцінює шкоду (матеріальну та моральну) заподіяну їй такими діями як незначну, то вона вважає, що немає й необхідності звертатися до правоохоронних органів. Очевидці ж злочину можуть не повідомляти про відповідні випадки як через елементарну байдужість, так і через заздрість (наприклад, до матеріального становища жертви), помсту конкретній особі чи фірмі-роботодавцю, начальнику тощо.

Причиною неповідомлення про вчинений кіберзлочин до правоохоронних органів може бути бажання отримання від цього вигоди. Навіть при негативному моральному відношенні до винного та вчиненого ним діяння, отримання прямої матеріальної чи іншої вигоди (особливо тих очевидців, яким безпосередньо шкода злочинними діями не спричиняється) може стати вирішальним фактором щодо повідомлення чи неповідомлення про злочин правоохоронним органам. Особливо це стосується випадків, коли жертва злочину володіє необхідними знаннями комп'ютерних технологій, навичками та, відповідно, усвідомлює всю тяжкість розслідування таких злочинів й доведення вини злочинця. Також, вказане вкрай актуальне у випадках, коли факт злочину був виявлений працівниками (фахівцями) спеціальних служб безпеки установ чи організацій, або коли у справі в якості винного фігурують працівники установи чи організації. В останньому випадку жертві (в особі роботодавця) вигідніше не лише приховати відповідний факт, але й компенсувати (можливо з надлишками) спричинену шкоду, особливо якщо це збігається з бажанням жертви не привертати до себе увагу правоохоронних органів.

Висновок. Безпека кожного користувача ЕОМ (комп'ютеру), автоматизованої системи, комп'ютерної мережі перш за все залежить від його обізнаності у існуючих загрозах. Будь-яка діяльність, навіть найбільш підготовлених підрозділів Національної поліції України, а також правоохоронних органів в цілому буде самоціллю, доки сам користувач віртуальної мережі не

буде опікуватися своєю безпекою. Доки в суспільстві не буде стану нульової толерантності до будь-яких злочинних проявів, будуть існувати латентні форми злочинності яким, нажаль, не здатна протидіяти навіть ідеальна правоохоронна система.

Список бібліографічних посилань

1. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. … канд. юрид. наук : 12.00.09. Донецьк, 2007. 230 с.

2. Комп'ютерна злочинність : навч. посіб. / П. Д. Біленчук, Б. В. Романюк. В. С. Цимбалюк та ін. Київ : Атіка, 2002. 240 с.

3. Кравцова М. О. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с.

Одержано 10.03.2019

УДК 343.341(477)

Григорій Сергійович КРАЙНИК,
кандидат юридичних наук,
асистент кафедри кримінального права № 1
Національного юридичного університету імені Ярослава Мудрого (м. Харків)

ЩОДО ВИЗНАЧЕННЯ ВИНИ В НЕОБЕРЕЖНИХ ЗЛОЧИНАХ ПРОТИ ГРОМАДСЬКОЇ БЕЗПЕКИ, ЩО ЗАПОДІЮЮТЬ ШКОДУ ЖИТТЮ АБО ЗДОРОВ'Ю ЛЮДИНИ (Ч. 3 СТ. 265 ТА Ч. 2 СТ. 267 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ)

У ч. 1 ст. 265 Кримінального кодексу України (далі – КК України) «Незаконне поводження з радіоактивними матеріалами» передбачається відповідальність за «придбання, носіння, зберігання, використання, передача, видозмінення, знищення, розпилення або руйнування радіоактивних матеріалів (джерел іонізуючого випромінювання, радіоактивних речовин або ядерних матеріалів, що перебувають у будь-якому фізичному стані в установці або виробі чи в іншому вигляді) без передбаченого законом дозволу». Ч. 3 ст. 265 КК України визначає «Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони *спричинили загибель людей*, майнову шкоду у великому розмірі, *значне забруднення довкілля чи інші тяжкі наслідки*, карається…». У ч. 1 ст. 267 КК України «Порушення правил поводження з вибуховими, легкозаймистими та їдкими речовинами або радіоактивними матеріалами» зазначено: «Порушення правил зберігання, використання, обліку, перевезення вибухових речовин чи радіоактивних матеріалів або інших правил поводження з ними, а також незаконне пересилання цих речовин чи матеріалів поштою або вантажем, якщо це порушення створило небезпеку загибелі людей або настання інших тяжких наслідків, – карається…». Ч. 3 ст. 267 КК України: «Ті самі діяння, а також незаконне пересилання поштою або багажем легкозаймистих або їдких речовин, якщо вони *спричинили загибель людей* або *інші тяжкі наслідки*, карається…» [1].

З погляду В. П. Тихого, суб'єктивна сторона складу злочину, передбаченого ст. 265 КК, характеризується прямим умислом [2, с. 508]. Із суб'єктивної сторони склад злочину, передбаченого ст. 267 КК, може бути вчинений як умисно, так і з необережності [3, с. 760]. Складність визначення вини у цих складах злочинів пов'язана з тим, що слід встановити психічне ставлення не лише до суспільно небезпечного діяння, але й до суспільно небезпечних наслідків.

Обов'язковою ознакою об'єктивної сторони злочину є незаконність поводження з радіоактивними матеріалами, тобто поводження без передбаченого законом дозволу. Надання дозволу на поводження з радіоактивними матеріалами у контексті відповідальності за ст. 265 КК передбачено в нормативно-правових актах та міжнародних договорах України. Це: а) Закон «Про дозвільну діяльність у сфері використання ядерної енергії та радіаційної безпеки» від 11 січня 2000 р. № 39/95-ВР; б) Конвенція про фізичний захист ядерного матеріалу від 3 березня 1980 р.; в) Постанова КМУ «Про затвердження Порядку ліцензування окремих видів діяльності у сфері використання ядерної енергії» від 6 грудня 2000 р. № 1782 тощо.