Але, крім заміни назви з «підмовника» на «підбурювача», дещо змінився і опис способів схиляння іншого співучасника до вчинення злочину.

Зокрема, в КК 1960 р. як способи підбурювання визначались умовляння, обіцянка, погроза і підкуп. У КК 2001 р. – умовляння, підкуп, погроза і примус.

Отже, у КК 2001 р. схиляння шляхом обіцянок не виділяється як окремий спосіб підбурювання. Його замінив такий спосіб як примус, тобто вимога від іншої особи вчинити злочин шляхом заподіяння тілесних ушкоджень або застосування іншого насильства. Це можна пояснити тим, що обіцянка у КК 2001 р. включена, певною мірою, до підкупу і тому не потребує самостійного виділення.

Таким чином, проаналізувавши КК 1960 та 2001 рр., можна зазначити, що у КК 2001 р. поняття співучасті розширене за рахунок вказівки на умисну форму вини злочину, вчиненого у співучасті. Також деталізовано та конкретизовано види учасників співучасті, тобто це ті особи, які наділені ознаками суб'єктів співучасті.

Відбулась заміна термінів з підмовника на підбурювача. Дещо розширилось поняття пособника, зокрема його дії доповнились тим, що пособником також визнається особа, яка заздалегідь обіцяла переховати злочинця, знаряддя чи засоби вчинення злочину, сліди злочину чи предмети, здобуті злочинним шляхом.

1. Кримінальний кодекс України 1960 р. // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/2001-05 (дата звернення: 24.10.2018).

2. Кримінальний кодекс України 2001 р. // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 24.10.2018).

Сидорова Е.О.
к.ю.н., викладач кафедри цивільно-правових
дисциплін ДДУВС

АКТУАЛЬНІ ЗЛОЧИНИ У СФЕРІ ПЛАТІЖНИХ СИСТЕМ В УКРАЇНІ

На сучасному етапі розвитку суспільства і технологій поняття кіберзлочинність зайняло значне місце серед можливих видів суспільно-небезпечних явищ. Темпи зростання злочинності у «віртуальному просторі» набуває поширення в залежності від стрімкого розвитку сфери застосування комп'ютерних технологій у повсякденному житті.

Проблематикою боротьби та подолання кіберзлочинності виступає об'єктом дослідження таких вчених, як: Н. Андерсон, В. Бурячок, А. Козловскі, Е. Старостіна, А. Щетилов та ін. [1].

У загальному понятті під кіберзлочинністю слід розуміти сукупність злочинів пов`язаних із використанням комп`ютерів, так і з використанням інформаційних технологій і глобальних мереж що вчинюються у віртуальному просторі [2].

Так, щоденна робота фінансових структур, банківського, державного та приватного сектору неможлива без надійної роботи комп'ютерної техніки та засобів комунікацій. Банківська і фінансові системи України являють собою сфери, де найбільш широко та активно використовуються сучасні можливості інформаційних технологій та мережі Інтернет. А враховуючи, що зазначені технології використовуються для грошових переказів та розрахунків, зазначена сфера привертає все більшу увагу осіб із злочинними намірами [3].

За перше півріччя 2018 року працівниками Департаменту кіберполіції супроводжувались 1336 кримінальних правопорушень вчинених у сфері платіжних систем. Слід зазначити, що питому вагу у структурі кіберзлочинності займають саме злочини вчинені у сфері платіжних систем, що становить 40% від загального обсягу вчинених злочинів. Порівняно з 2017 роком виявлено в 1,4 рази більше фактів у цьому напрямку [4].

З огляду на зазначене метою написання статті є висвітлення найбільш розповсюджених видів злочинів у сфері платіжних систем, а також виокремлення та аналіз певних способів учинення таких злочинів.

Так, слід висвітити механізм вчинення злочину, сутність якого полягає у несанкціонованому доступі до облікового запису клієнта банку у системі дистанційного банківського обслуговування (далі – ДБО). Сутність механізму вчинення зазначеного злочину полягає у тому, що зловмисники, використовуючи спрощений порядок перевипуску SIM-карток операторів мобільного зв'язку, отримують від авторизованих сервісно-торгівельних мереж дублікати SIM-карток потенційної жертви шахрайства. В подальшому зловмисник здійснює реєстрацію облікового запису клієнта в системі, таким чином отримуючи повний контроль над управлінням картковими рахунками. У випадку вже наявного зареєстрованого облікового запису клієнта в системі ДБО, зловмисник виконує процедуру відновлення паролю, у результаті чого отримує повний доступ до керування обліковим записом. Шляхом здійснення транзакцій грошові кошти жертви перераховуються на підконтрольні карткові рахунки зловмисника.

Слід зазначити, що останнім часом поширюються випадки «скімінгу» банківських карток в торгівельних мережах. Під «скімінгом» в даному випадку слід розуміти дії особи, націлені на незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток, тобто отримання банківських персональних даних клієнта шляхом використання спеціального обладнання. Отримані відомості компрометуються шляхом копіювання на «білий пластик» та в подальшому використовується для незаконного отримання готівкових коштів в мережі банкоматів обслуговуючого банку [5].

У серпні 2018 році було викрито групу осіб, які, діючи на території

Дніпропетровської області, встановлювали «скімінгові» пристрої в закладах харчування. Після чого останні використовували скомпрометовані банківські картки відвідувачів закладу для викрадення коштів з їх банківських рахунків, чим спричинили збитків близько 400 тис. грн. [6].

Боротьба зі злочинами у сфері платіжних систем залежить не тільки від правоохоронних органів, а й в першу чергу від обізнаності користувачів банківських та фінансових послуг, що полягає у постійному інформуванні клієнтів про можливі шахрайські загрози, поінформованість власників карток щодо правил ефективного та безпечного використання платіжних інструментів та вчасне інформування правоохоронних органів про факти, які можуть свідчити про шахрайські дії. Варто зазначити, що не менш важливим аспектом у боротьбі зі злочинами у сфері платіжних систем є посилення заходів з питань безпеки суб'єктів надання фінансових та банківських послуг, сутність яких повинна полягати у вдосконаленні методів боротьби з кіберзлочинністю з метою недопущення матеріальних та репутаційних втрат.

1. Деякі сучасні тенденції кіберзлочинності. URL: http://dspace.kntu.kr.ua/jspui/bitstream/ 123456789/5111/1/Cyber-Security _November2016_p54.pdf.

2. Кіберзлочинність. «Правове регулювання інформаційних технологій в Україні: проблеми та перспективи сучасності». URL: http://ukrainepravo.com/legal_publications/essay-on-it- law/it_law_ prytula_ cybercrime.

3. Кіберзлочинність та відмивання коштів. Департамент фінансових розслідувань. Державна служба фінансового моніторингу України – 2013 рік. URL: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf.

4. Кіберполіція відмічає збільшення кількості правопорушень у сфері платіжних систем та кібербезпеки. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vidmichaye-zbilshennya-kilkosti-pravoporush en-u-sferi-platizhnyx-system-ta-kiberbezpeky-1519.

5. Скімінг та ліміти на зняття готівки в банкоматах України. URL: https://ema.com.ua/skimming-and-limits-on-cash-withdra wals-from-atms-ukraine.

6. Кіберполіція викрила групу скімеристів, які спустошували банківські рахунки громадян. URL: https://cyberpolice. gov.ua/news/kiberpolicziya-vykryla-grupu-skimerystiv-yaki spustoshuvaly-bankivski-raxunky-gromadyan-4443.