ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ ЗАСОБІВ ДОСТУПУ ДО БАНКІВСЬКИХ РАХУНКІВ

Курсант 403 навчального взводу факультету підготовки кадрів кримінальної міліції **Тріпник О.М.**
Науковий керівник: старший науковий керівник лабораторії з проблем досудового розслідування **Садченко М.М.**

На хвилі сучасного розвитку суспільства, коли ми живемо в епоху інформаційних технологій, і коли комп'ютерні системи охопили всі галузі життєдіяльності людини, стає в край гострим питанням протидія злочинності у сфері інформаційно-телекомунікаційних технологій.

Стаття 200чинногоКримінального кодексу України передбачає відповідальність за незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення. Кваліфікуючими ознаками складу злочину є вчинення зазначених дій повторно або за попередньою змовою групою осіб.

Засоби доступу до банківських рахунків (у п. 1.31 ст. 1 *Закону України "Про платіжні системи та переказ грошей в Україні" від 5 квітня 2001 р., № 2346-III* [1] вони іменуються платіжними інструментами) – це засоби певної форми на паперовому, електронному чи іншому виді носія інформації, використання якого ініціює переказ грошей з відповідного рахунка платника. Банки в Україні, згідно з ч. 4 ст. 51 *Закону України "Про банки і банківську діяльність" від 7 грудня 2001 р., № 2121-III* [2] можуть використовувати як засоби доступу до банківських рахунків платіжні доручення, платіжні вимоги, вимоги-доручення, векселі, чеки, банківські платіжні картки та інші дебетові і кредитові платіжні інструменти, що застосовуються у міжнародній банківській практиці. Безпосередньо у диспозиції ч. 1 ст. 200 КК названі два види засобів доступу до банківських рахунків – документи на переказ та спеціальні платіжні засоби.

Документами на переказ – це документ у паперовому або електронному виді, що використовується банками чи їх

клієнтами для передачі доручень або інформації на переказ грошових коштів між суб'єктами переказу грошових коштів (розрахункові документи, документи на переказ готівкових коштів, а також ті, що використовуються при проведенні міжбанківського переказу та платіжного повідомлення, інші).

Незаконні дії з документами на переказ полягають упідробці платіжних документів, що проявляється не тільки у формі їх підроблення, у тому числі фальсифікації відповідних справжніх документів, внаслідок якої з їх застосуванням здійснюється незаконне переведення грошових коштів (готівкових чи безготівкових). Доступ до інформації щодо певного банківського рахунка отримує не уповноважена на це особа.

Підробка може бути здійснена за допомогою спеціального технічного обладнання, комп'ютерних програмних засобів або у будь-який інший спосіб (дописка, підчистка, виправлення у паперових документах). Наприклад, за допомогою комп'ютерного обладнання особа здійснює цифровій електронний підпис, який дає доступ до банківського рахунку.

Незаконні дії з платіжними картками, на далі ПК, розрізняють як повну та часткову підробку платіжних карток. Найбільшу загрозу для фінансових установ складають повністю підроблені ПК. Спосіб виготовлення таких ПК отримав назву "білий пластик". На такому "білому пластику" розміром з ПК знаходяться числа рахунку, дата випуску та відомості про власника. Також на ньому є магнітний носій інформації. Знаючі ПІН-код, за допомогою "білого пластика" можна безперешкодно викрасти гроші із банківських автоматів самообслуговування [3].

Часткова підробка ПК пов'язується: 1) із зміною інформації магнітного носія ПК; 2) із зміною інформації, що ембосована на лицьовому боці ПК; 3) із зміною підпису власника ПК [4].

Створення мікропроцесорів привело до появи старт-картки, яка має можливості "мікрокомп'ютера" і може використовувати кілька різноманітних програм опрацювання інформації з порівняно великим обсягом операцій. ПК такого типу взаємодіє з пристроєм, що зчитує інформацію, забезпечує

збереження й опрацювання інформації про клієнта, його фінансовий стан та про всі його фінансові операції. Отже, як підробку слід розглядати заміну безпосередньо мікропроцесора такої смарт-картки або зміну самої інформації [5].

Технічному вдосконаленню ПК відповідає і розвиток технології їхнього використання. Поряд з власне кредитними електронними картками з'явилися і так звані дебетові ПК. Вони відрізняються від кредитних карток тим, що кошти клієнта резервуються на його рахунку і записуються на ПК. У міру їх витрачання вони списуються з картки. У цьому випадку плата за надання кредиту банком з клієнта не стягується.

Фінансові операції з кредитними картками здійснюються за допомогою банківських автоматів самообслуговування та платіжних терміналів. Згідно з п. 1 *Положення про порядок емісії платіжних карток і здійснення операцій з їх застосуванням, затвердженим постановою Правління НБУ від 27 серпня 2001 р., № 367*[6] банківський автомат самообслуговування (банкомат) – це програмно-технічний комплекс, що дає змогу держателеві платіжної картки здійснити самообслуговування з операціями одержання грошей у готівковій формі, внесення їх для зарахування на відповідні рахунки, одержання інформації щодо стану своїх рахунків, а також виконати інші операції згідно з функціональними можливостями цього комплексу.

Платіжний термінал – це електронний пристрій, що дає змогу, як наслідок взаємодії ПК, здійснювати авторизацію та формувати платіжні чеки за операціями з використанням ПК *(див. п. 1Положення про впровадження пластикових карток міжнародних платіжних систем у розрахунках за товари, надані послуги та при видачі готівки, затвердженого постановою Правління НБУ від 24 лютого 1997 р., № 37)*. Фінансові операції, які здійснюються банкоматом, як правило, протоколюють на папері за допомогою двох принтерів. Один з них використовують для чека, що видають користувачу, з вказівкою суми разом із грошима. Інший, що може розташовуватися на відстані від банкомату, є аналогом контрольної стрічки касового апарата і фіксує всі операції. Крім того, для підвищення безпеки застосовуються апаратні методи шифрування інформації, якою обмінюються банкомат і ПК, а

також інформації, що циркулює між банкоматом і центральним офісом.

Таке обладнання (відповідно для отримання і/або для переказу готівкових і/або безготівкових грошових коштів) не є предметом ст. 200 КК. Однак, на практиці все ж таки зустрічаються шахрайства з використанням фальшивих банкоматів і торгових терміналів. Відомі випадки, коли злочинці встановлювали фальшивий банкомат і приймали в нього реальні кредитні картки, знімаючи персональний ідентифікаційний номер (ПІН-код), введений користувачем, а також наявні кошти, які користувачі намагалися через банкомат покласти на свій рахунок у банку. При спробі ж отримати готівку з банкомату з'являлося повідомлення, що в банкомат не завантажені купюри потрібної вартості. Справжні сусідні банкомати при цьому були виведені з ладу [7].

У нашій країні вже сьогодні знаходиться досить розвинена система електронного зв'язку, яка не може бути абсолютно надійною та захищеною. Така ситуація надає можливість злочинцям отримувати несанкціонований доступ до комп'ютерних інформаційних систем для проведення незаконних маніпуляцій у корисливих цілях. Процес комп'ютеризації суспільства призводить до збільшення кількості комп'ютерних злочинів, зростання їх ваги за розмірами сум, що використовуються в загальній частині матеріальних витрат, у порівнянні із звичайними видами злочинів.

Для нормального функціонування економіки необхідна надійна, стабільна і розвинена банківська система, при якій банки будуть здійснювати платежі, вчасно надавати своїм клієнтам кредити, послуги по операціям з цінними паперами тощо. Якщо фінансове становище банку "похитнулось", то разом з ним може похитнутися і фінансове становище сотень його клієнтів.

Список використаних джерел:

1. Відомості Верховної Ради України. – 2001. – № 29. – С.137.

2. Відомості Верховної Ради України. – 2001. – № 5-6. – С.30.

3. *Берзин П.С.* Особенности расследования хищений, совершаемых с использованием поддельных банковских платежных карточек // Актуальні проблеми сучасної криміналістики: матеріали міжнар. наук.-практ. конференції (Сімферополь – Алушта, 19-22 вересня): У 2-х ч. – Сімферополь: „ДОЛЯ", 2002.–С.113.

4. *Котляревський О.І.* Шахрайства з використанням пластикових платіжних карток // Збірник наукових праць. – Запоріжжя: Запорізький юридичний інститут, 1998. – № 1. – С.49.

5. *Кобылянский О.Л.* Проблемы исследования пластиковых карточек // Теорія та практика судової експертизи і криміналістики. Випуск 2: Збірник матеріалів міжнарод. наук.-практ. конф. – Харків: Право, 2002. – ст. 235-239.

6. Офіційний вісник України. – 2001. – № 47. – ст. 21-25.

7. *Смаглюк О.* Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки // Підприємництво, господарство і право. – 2002. –№ 6. – С.86.

ПРОЦЕСУАЛЬНИЙ СТАТУС АДВОКАТА У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Курсант 410 начальної групи **Троп О.В.**
Науковий керівник: начальник кафедри кримінального процесу НАВС, доктор юридичних наук, професор**Удалова Л.Д.**

Забезпечення права на захист є конституційним принципом кримінального процесу і тісно пов'язана з діяльністю захисника. Саме тому важлива роль у діяльності із захисту від порушення конституційних прав особи належить адвокату.

Метою наукового дослідження є процесуальний статус адвоката під час здійснення захисту у кримінальному провадженні.

До проблем діяльності адвокатури ще до прийняття КПК 2012 року зверталися багато українських учених. Питання організації адвокатури і здебільшого діяльності адвоката у