14 січ. 2005р. № 15. URL: https://ukrstat.org/uk/metod_polog/metod_doc/2006/481/metod.htm.

14. Про заходи щодо забезпечення формування та функціонування аграрного ринку: Указ Президента України від 6 черв. 2000 р. № 767/2000. URL:https://zakon.rada.gov.ua/laws/show/767/2000

15. Благоразумова О., Спащенко Г. Порівняльна характеристика суб'єктів підприємництва у сфері організації торговельних процесів. *Торгівля і ринок України: темат. зб. наук. пр. 2013. № 36. С. 127–139.*

16. Про затвердження Порядку набуття юридичною особою статусу оптового ринку сільськогосподарської продукції: постанова Кабінету Міністрів України від 11 лют. 2010 р. № 141. URL:https://zakon.rada.gov.ua/laws/show/141-2010-%D0%BF#Text.

17. Батигіна О. Особливості правового регулювання оптових ринків сільськогосподарської продукції в Україні. *Вісник Національної академії правових наук України. 2012. № 3. С. 159–167.*

18. Про зерно та ринок зерна в Україні: Закон України від 4 лип. 2002 р. № 37-IV. URL: https://zakon.rada.gov.ua/laws/show/37-15.

19. Про молоко та молочні продукти: Закон України від 24 черв. 2004 р. № 1870-IV. URL: https://zakon.rada.gov.ua/laws/main/1870-15.

20. Про зовнішньоекономічну діяльність: Закон України від 16 квіт. 1991 р. № 959-XII. URL: https://zakon.rada.gov.ua/laws/show/959-12.

21. Ляхович О. Торгівля через офшорні зони: раціональна необхідність чи перепона для розвитку України? URL: https://commons.com.ua/ru/torgivlya-cherez-ofshorni-zoni-ratsionalna-neobhidnist-chi-perepona-dlya-rozvitku-ukrayini/.

ИНФОРМАЦИЯ ОБ АВТОРЕ
Анна Сергеевна КОРНИЕНКО, кандидат юридических наук, доцент, доцент кафедры земельного и аграрного права Национального юридического университета имени Ярослава Мудрого;

INFORMATION ABOUT THE AUTHOR
Anna Sergeyevna KORNIYENKO, Candidate of Legal Sciences, Associate Professor of Land and Agricultural Law Department of Yaroslav Mudryi National Law University; gannakor@ukr.net

УДК 340 – 33

# МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БАНКОМАТОВ И БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК

**Юлия КУЗЬМЕНКО**
доктор педагогических наук, доцент,
профессор кафедры административного права и административного процесса Херсонского факультета Одесского государственного университета внутренних дел

Статья посвящена вопросу противодействия преступным манипуляциям с банкоматами и банковскими платежными карточками, поскольку данный вид мошенничества в банковской сфере влечет за собой крайне негативные последствия в виде торможения распространение безналичной формы оплаты, которая является залогом развития глобальной финансовой системы. Описаны характеристики самых распространенных видов мошеннических схем, таких как «траппинг», «скимминг», «шимминг», «фантом», «шаттер», «трешинг», «фарминг», «фишинг». Представлены основные меры безопасности клиентам банков, которые должны соблюдаться в целях сохранения своих счетов от незаконного завладения или хищения денежных средств.

***Ключевые слова:*** *мошенничество, банковская платежная карта, банкомат, преступные схемы, меры безопасности.*

## FRAUD WITH USING OF ATMs AND BANK PAYMENT CARDS

**Yuliya KUZMENKO**
PhD., Assistant Professor, Professor,
of Kherson Faculty of Odesa State University of Internal Affairs

The article is devoted to the issue of combating criminal manipulation of ATMs and bank payment cards, as this type of fraud in the banking sector has extremely negative consequences in the form of braking the spread of cashless form of payment, which is the key to the development of the global financial system. There are described the characteristics of the most common types of fraudulent schemes, such as “trapping”, “skimming”, “shimming”, “phantom”, “shutter”, “trashing”, “farming”, “phishing”. Also, there are presented the basic security measures to bank customers, which must be followed in order to preserve their accounts from illegal seizure or theft of funds.

***Keywords:*** *fraud, bank payment card, ATM, criminal schemes, security measure.*

## FRĂUDĂ CU UTILIZAREA ATM-urilor ȘI CARDURILOR BANCARE

Articolul este dedicat problemei combaterii manipulărilor penale cu bancomatele și cardurile de plată bancare, deoarece acest tip de fraudă în sectorul bancar atrage consecințe extrem de negative sub forma inhibării răspândirii plăților fără numerar, care este cheia dezvoltării sistemului financiar global. Sunt descrise caracteristicile celor mai obișnuite tipuri de scheme frauduloase, cum ar fi „captarea”, „zgârietura”, „creșterea”, „fantomă”, „obturatorul”, „curățarea”, „agricultura”, „phishingul”. Măsurile de securitate de bază sunt prezentate clienților băncilor, care trebuie să le respecte pentru a-și păstra conturile de confiscarea ilegală sau furtul de fonduri.

***Cuvinte-cheie:*** *fraudă, card bancar de plată, bancomat, scheme criminale, măsuri de securitate.*

**Постановка и актуальность проблемы.** Современный уровень развития научно технической сферы, вместе со всеми благами, которые они обеспечили, обеспечил появление новых самых разнообразных способов нарушение установленных законом норм, в том числе и банковской деятельности. Как показывает статистика правоохранительных органов в Украине прослеживается стремительный рост количества преступлений в банковской сфере с использованием платежных карточек, потому что основной проблемой выступает латентность совершенных действий. Банковские учреждения терпят существенный вред также вследствие действий с платежными карточками, а именно такие операции, которые не были согласованы с непосредственными пользователями платежных карт. Поэтому одной из стратегических задач банковской системы для ее эффективной работы в целом является максимально возможное страхование всех ее участников от противоправных посягательств. Безопасность банковской системы является неотъемлемым условием продуктивного функционирования экономики страны, а также гарантией экономической безопасности. Поэтому данные вопросы очень актуальны для современного поиска решения данных проблем.

**Состояние исследования.** Отдельные аспекты данной темы исследовались многими учеными, такими как М. Садченко, А. Клочко, О. Дудоров, В. Навроцкий, С. Чернявский, В. Пивоваров, О. Олейничук т.д. Несмотря на большое количество подобных исследований, стремительное развитие новых технологий актуализирует данные вопросы.

**Целью и задачей статьи** является исследование вопроса поиска мер защиты от мошенничества с банкоматами и банковскими платежными карточками.

**Изложение основного материала.** Проанализируем в научном дискурсе формулировку таких понятий как «мошенничество», «банковская платежная карта».

В соответствии с Уголовным кодексом Украины мошенничество – это завладение чужим имуществом или приобретение права на имущество путем обмана или злоупотребления доверием. Способы совершения мошенничества – обман и злоупотребление доверием. Обман как способ мошеннического завладения чужим имуществом или приобретение права на такое имущество состоит в сообщении потерпевшему ложных сведений или сокрытие определенных сведений, сообщения которых имеет существенное значение для поведения потерпевшего, с целью введения в заблуждение. Злоупотребление доверием заключается в недобросовестном использовании доверия со стороны потерпевшего.

Банковская платежная карта – это персонифицированная пластиковая карточка с магнитной полосой или чип-модулем, которая является ключом доступа к управлению банковским счетом и предоставляет ее владельцу возможность безналичной оплаты товаров или услуг в различных торговых и сервисных предприятиях, принимающих карты к оплате, получать наличные в отделениях банков и в банкоматах, а также пользоваться другими дополнительными услугами и определенными преимуществами [5, с. 43]. Сегодня правовым полем охвачены все направления банковской деятельности, что способствует максимальной защите прав и интересов как клиентов, так и самих банковских учреждений [2, с. 102].

Банковские карточки являются основным элементом электронных банковских систем, все более активно вытесняя традиционные чековые книжки и наличные. Та особенность, что карта содержит определенную информацию, которая нужна для доступа к банковскому счету, осуществления расчетов за товары и услуги, а также снятия наличных, позволяет ей служить простым и прогрессивным средством в организации безналичных расчетов и одновременно быть привлекательным объектом для мошеннических операций со стороны преступников [1, с. 92].

По данным Украинской межбанковской ассоциации членов платежных систем ЕМА за 2019 год мошенникам в банковской сфере с использованием платежных карточек удалось «добыть» почти 362 млн гривен. Это в полтора раза больше, чем в 2018 году. На первом месте в 2019 году оказались так называемые «мошеннические сайты», которые способны обманом склонить человека потратить деньги на несуществующие материальные блага или услуги. В ЕМА насчитали более 300 подобных сайтов. Кроме того, участились физические атаки (когда их взрывают, ломают, выпиливают и т.п.) на банкоматы – 77 официально выявленных инцидентов, для сравнения в 2018 году таких случаев начислено всего 20 [3].

На данный момент правоохранительным органам известно широкий круг видов мошенничества с банковскими картами и банкоматами: «скимминг», «траппинг», «фантом», «шаттер», «шиммминг», «трешинг», «фарминг», «фишинг» и другие. По сути выбор преступником определенного способа не влияет в целом на квалификацию его действий с точки зрения уголовного права, вместе с тем преступники придумывают все новые способы использования современных технологий для достижения своих целей.

Один из вышеупомянутых

способов мошенничества с платежными картами является «скимминг». Для этого преступники устанавливают на банкоматы специальные устройства – скиммеры, которые считывают номер карточки и PIN-код. После чего карта дублируется и деньги могут поменять своего владельца за секунды. Еще один вариант – прикрепление на банкомат миниатюрной видеокамеры, которая снимает введение PIN-кода, делает запись в модуль памяти или же передает его дистанционно на компьютер преступника.

Следующим способом совершения мошеннических действий является «траппинг». Специальным устройством блокируется окно подачи карты так, чтобы она застряла в банкомате. Злоумышленник предварительно подглядывает PIN-код, а затем сочувствует и рекомендует срочно идти и звонить в банк или сервисную службу. Только владелец уходит, преступник извлекает карту, освобождает окно банкомата и снимает деньги [5].

«Фантом» – это вид мошенничества с помощью непосредственно банкомата. Нередки также случаи полной замены банкомата. С виду обычный банкомат может оказаться муляжом, оборудованным специальными устройствами для считывания информации. На фантом-банкомате все запросы, поля ввода данных отображаются в точном соответствии с настоящего. Однако в конце всех операций, деньги не будут выданы пользователю платежной карты, что по факту их отсутствии в банкомате. Таким образом мошенник получает всю цифровую информацию для следующих преступных шагов.

Также одним из видов мошенничества с банкоматом является способ «шаттер». Деньги воруются из банкоматов. Денежные купюры упираются в установленную мошенником накладку, банкомат же выполнит и завершит соответствующие операции, но клиент денег не получит. Когда же он отходит от банкомата с намерением позвонить в свой банк, то аферист, который следит за ситуацией неподалеку снимает накладку к которой прилипли все деньги.

«Шимминг» – незаконное снятие денег с помощью тонкой пленки, похожей на скотч. Такая пленка наклеивается на клавиатуру, а затем из нее считывается необходимая информация. Необычная клавиатура банкомата не вызывает никаких подозрений у пользователей, что значительно облегчает задачу преступникам [6, с. 148].

Как показывает практика в мошенничестве с непосредственно платежными карточками можно выделить три вида:

1) «Трешинг» – форма мошенничества, которая заключается в том, что так называемые трэшеры ищут в разных источниках в том числе и мусоре неразорвавшиеся чеки-слипы, бухгалтерскую документацию, содержащую конфиденциальную информацию о платежных картах для дальнейшей перепродажи. В такой ситуации очень важно измельчить документ перед тем, как он окажется на свалке для предотвращения считывания вышеупомянутой информации [4].

2) «Фарминг» – во время нахождения на сайте, на компьютер жертвы устанавливается вирус. Во время посещения сайта интернет-банкинга, вирус переадресовывает и направляет все действия к фиктивному сайту, который внешне очень схож с настоящим. После введённая клиентом информация фиксируется и используется для дальнейших мошеннических действий.

3) «Фишинг» – это вид мошенничества, который применяется с целью получения у пользователя банковской платежной карточки информации о реквизитах карты путем использования поддельных сайтов, введение в заблуждение и др.

Именно реквизиты платежной карточки, выведывают мошенники, занимающиеся фишингом: 1. Номер карточки. 2. Дата выпуска / завершения действия карты. 3. Код CVV2. 4. Написание фамилии и имени клиента латыни. 5. ПИН-код.

Способов фишинга множество, вот самые распространенные из них:

- письмо на электронную почту с уведомлением о выигрыше (в лотерею, бонус, игре) и просьба прислать реквизиты карты для зачисления денежного приза;

- письмо от фальш-банка с просьбой прислать реквизиты карты для ее подтверждения, разблокировки и т. п.;

- использование мошеннических интернет-сайтов (Интернет-магазинов). Это могут быть копии оригинальных интернет-сайтов компаний или другие сайты, на которых обычно предлагается приобрести какую-то вещь по очень низкой (акционной) цене с использованием банковской платежной карточки;

- использование всплывающих окон, не имеющих отношения к сайту;

- перенаправление на мошеннические сайты с помощью модификации ссылок;

- телефонные звонки из фальш-банка или других коммунальных, контролирующих, правоохранительных органов с просьбой подтвердить реквизиты карты в связи с подозрением мошеннических операций, наличия несуществующей задолженности и тому подобное;

- кража данных с компьютера с помощью вредоносного программного обеспечения (вирусы, программы удаленного доступа и т. д.) [4].

Для борьбы и противодействия преступным действиям в банковской сфере в Украине в 1999 году украинскими банками и членами платежной системы Europay International была создана Ассоциация «ЕМА», с 2004 года Украинская межбанковская ассоциация членов платежных систем «ЕМА». Эта структура взаимодействует с членами международных платежных систем и других систем, использующих платежные карточки, электронные средства платежей и работают по общепринятым международным или отраслевым стандартам [1, с. 93].

Изучив самые распространенные виды мошенничества, выделим рекомендации по безопасному пользованию банкомата и банковской платежной карточки. Это станет одним из шагов предотвращения мошеннических схем и махинаций для обеспечения безопасности денежных средств от незаконного завладения:

1. При условии получения телефонного звонка, когда представляются работником банка, мобильным оператором связи и говорят, что с вашими счетами возникла проблема, необходимо положить трубку. Нельзя выполнять их USSD-команды на телефонные просьбы сотрудников банка. Необходимо сделать звонок в свой банк или оператору мобильной связи за официальным номером, и убедиться, что это не обманное действие.

2. Если вы получили телефонный звонок от вашего знакомого, родственника, друга или приходит смс-сообщение с просьбой о перерасчете денег на лечение члена семьи, или перевода для других целей следует также положить трубку и перезвонить лично. Поскольку мошенники могут перехватить этот номер, и как результат у вас на экране высветится номер телефона знакомого вам человека. Ни при каких условиях нельзя переводить средства по требованию работника банка на любые указанные им расчетные счета.

3. Нельзя переходить по ссылкам в смс-сообщениях якобы от вашего банка, мобильного оператора или другого государственного учреждения.

4. Рекомендуется, как профилактическая мера, привязать свою платежную карту к номеру телефона, которым вы не пользуетесь для совершения звонков. Этот шаг позволит свести к минимуму шансы мошенников подобраться к вашим счетам через номер телефона.

5. Если возникли сомнения, то Вы можете проверить подозрительные для вас сайты, номера телефонов и номера банковских карточек на сайте киберполиции или в черном списке Ассоциации ЕМА.

6. Необходимо хранить отдельно платежные карточки и записанные их пароли, паспорт и идентификационный код. Нельзя оставлять документы без присмотра в машине, на работе, в общественных местах.

7. С целью контроля проводок по вашей карточке целесообразно заказать в банке опцию SMS-сообщения о состоянии вашего банковского счета и всех операциях (поступления и снятия денег).

8. Обязательно проверьте, что после осуществления оплаты покупок вам вернули вашу карту.

9. После получения платежной карты в банковском учреждении на ее обратной стороне необходимо создать образец своей подписи.

10. Перед началом работы с банкоматом визуально осмотрите его. Если возникли сомнения по изменению внешнего вида картоприемника лучше не вставлять вашу карточку. Позвоните в банк и сообщить о своих подозрениях. Особое внимание уделяйте лишним предметам у экрана – они могут маскировать скрытую камеру.

11. Не сообщайте и не позволяйте никому подсматривать ваш PIN-код. Прикрывайте клавиатуру руками во время набора PIN-кода.

12. Экстренную связь с банком делайте через официальный номер, он указан на обратной стороне карты или сайте банковского учреждения. Целесообразно его записать в свою телефонную книгу.

Нами был предложен список мер по обеспечению безопасности при пользовании банкоматами и банковскими платежными карточками, соблюдение этих рекомендаций сохранит от мошеннических схем завладения вашими деньгами.

**Выводы.** Таким образом можно сделать вывод, что мошеннические схемы и манипуляции в банковской сфере с каждым годом все больше совершенствуются, тем самым подрывая стабильность и экономическую безопасность страны. Мошенничество с банкоматами и банковскими платежными карточками влекут за собой негативные последствия в виде торможения распространение безналичной формы оплаты, которая является залогом развития глобальной финансовой системы. Поэтому приоритетом в предотвращении и противодействии таким преступным деяниям является максимальное информирование населения о существующих рисках и мерах безопасности пользования платежными инструментами.

Современными видами мошеннических схем с банкоматами и банковскими платежными карточками есть «траппинг», «скимминг», «шимминг», «фантом», «шаттер», «трешинг», «фарминг» и «фишинг». Они могут угрожать практически каждому участнику банковской системы, поэтому нами описаны основные меры

безопасности, направленные на сохранение счетов от незаконного завладения или хищения денежных средств.

**Список использованной литературы**

1. Олійничук О. Банківські картки як об'єкт шахрайства: стан і протидія явищу. *Актуальні проблеми правознавства*. 2017. №1. С. 91–94.
2. Кузьменко Ю. В. Банківська діяльність в Україні: правовий аспект. *Юридичний бюлетень*. 2018. Вип. 7. Ч. 2. С. 98–102.
3. Ліга Новини. Обманом витягнути з жертви «фінансову» інформацію і переобладнання банкоматів. URL: https://ua-news.liga.net/economics/articles/u-2019-mushahrai-vkrali-z-nashih-kartok-362-mln-grn-chotiri-sposobi-yak-voni-tse-zrobili
4. Незалежна асоціація банків України. URL: http://anticyber.com.ua/index.php
5. Пиріг С. О. Платіжні системи: навч. посіб. Київ: ЦУЛ, 2008. 239 с.
6. Стрєлков Л. О. Кримінальна відповідальність за незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення. *Юридична наука*. 2011. № 21. С. 145–151.

ИНФОРМАЦИЯ ОБ АВТОРЕ
Юлия Васильевна КУЗЬМЕНКО,
доктор педагогических наук, доцент, профессор кафедры административного права и административного процесса Херсонского факультета Одесского университета внутренних дел;

INFORMATION ABOUT THE AUTHOR
Yuliya Vasilyevna KUZMENKO,
PhD., Assistant Professor, Professor of Kherson Faculty of Odesa State University of Internal Affairs;
1geoekonomika@gmail.com

УДК: 347.9

# АДМИНИСТРАТИВНО-ПРАВОВЫЕ ОСНОВЫ ВЗАИМОДЕЙСТВИЯ СУБЬЕКТОВ ПРЕДОСТАВЛЕНИЯ БЕСПЛАТНОЙ ПРАВОВОЙ ПОМОЩИ В УКРАИНЕ

**МАГАРРАМЛИ Этибар Вали оглы**
аспирант кафедры государственно-правовых дисциплин, международного права и права Европейского Союза Харьковского национального педагогического университета имени Г. С. Сковороды

В статье автором на основании анализа совокупности нормативно-правовых актов, которые регулируют сферу предоставления бесплатной правовой помощи сделано вывод, что основными способами взаимодействиями между субъектами предоставления бесплатных правовых услуг являются: совместное предоставление правовых услуг; обмен информацией и практическим опытом; содействие в получении различного вида правовых услуг; обеспечение защиты лиц пострадавших от домашнего насилия, вооруженного конфликта, военных действий; подготовка совместных докладов и отчетных документов; организация и проведение коммуникационных мероприятий; проведение конференций, семинаров, круглых столов, встреч; разработка и реализация совместных проектов и / или программ по совершенствованию и повышению эффективности функционирования системы предоставления бесплатной правовой помощи.

***Ключевые слова:*** *бесплатная правовая помощь, система субъектов, взаимодействие, органы государственной власти, правоохранительные органы, меморандум.*

## ADMINISTRATIVE LEGAL BASES OF INTERACTION OF SUBJECTS OF PROVIDING FREE LEGAL AID IN UKRAINE

**MAGARRAMLI Etibar Vali oglu**
Graduate Student of the Department of State Law Disciplines, International Law and European Union Law H.S. Skovoroda Kharkiv National Pedagogical University

Based on the analysis of the set of regulatory legal acts that govern the scope of the provision of free legal assistance, the author concludes that the main methods of interaction between the entities providing free legal services are: joint provision of legal services; exchange of information and practical experience; assistance in obtaining various types of legal services; ensuring the protection of persons affected by domestic violence, armed conflict, military operations; preparation of joint reports and reporting documents; organization and conduct of communication activities; holding conferences, seminars, round tables, meetings; development and implementation of joint projects and / or programs to improve and improve the functioning of the system of providing free legal assistance.

***Keywords:*** *free legal assistance, system of subjects, interaction, public authorities, law enforcement agencies, memorandum.*

## BAZE JURIDICE ADMINISTRATIVE DE INTERACȚIUNE A SUBIECȚILOR CARE FURNIZEAZĂ SERVICII JURIDICE GRATUITE ÎN UCRAINA

Pe baza analizei totalității actelor juridice care reglementează sfera furnizării de asistență juridică gratuită, autorul concluzionează că principalele metode de interacțiune între subiecții furnizării de servicii juridice gratuite sunt: furnizarea în comun de servicii juridice; schimb de informații și experiență practică; asistență în obținerea diverselor tipuri de servicii juridice; asigurarea protecției persoanelor afectate de violență în familie, conflict armat, operațiuni militare; pregătirea rapoartelor comune și a documentelor de raportare; organizarea și desfășurarea activităților de comunicare; organizarea de conferințe, seminarii, mese rotunde, întâlniri; dezvoltarea și implementarea de proiecte și / sau programe comune pentru îmbunătățirea funcționării sistemului de furnizare a asistenței juridice gratuită.

***Cuvinte-cheie:*** *asistență juridică gratuită, sistem de subiecți, interacțiune, autorități publice, agenții de aplicare a legii, memorandum.*