УДК 316.324.8

БРИЖКО В.М., *доктор філософії (Ph.D.) з юридичних наук, с.н.с.*
ORCID: https://orcid.org/0000-0002-3941-1013.

БЕЗПЕКА ІНФОРМАЦІЙНОЇ ПРИВАТНОСТІ: ВИДИ ТА СХЕМИ ШАХРАЙСТВА У СФЕРІ ЕЛЕКТРОННО-ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ

Анотація. *Розглянуто та узагальнено сучасні види та схеми шахрайської діяльності, зокрема злодійства карткових даних, у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку. Наведено норми, у яких визначаються правові наслідки порушення чинного законодавства у зв'язку з шахрайським злодійством персональних даних та відомостей про людину. Сформульовані пропозиції з удосконалення законодавства.*

Ключові слова: *інформаційне право, інформаційна безпека, захист даних та інформації, шахрайство, види та схеми шахрайської діяльності.*

Summary. *Modern types and schemes of fraudulent activities, in particular theft of card data, in the field of use of electronic computing machines, systems, as well as computer and telecommunication networks, are considered and summarized. The norms are given, which determine the legal consequences of violating the current legislation in connection with the fraudulent theft of personal data and information about a person. Formulated proposals for improving the legislation.*

Keywords: *information law, information security, data and information protection, fraud, types and schemes of fraudulent activity.*

Постановка проблеми. Останнім часом банківські пластикові картки використовують не лише для зняття готівки в банкоматах, а все більше для оплати товарів та послуг в магазинах, в Інтернеті тощо. Паралельно з розвитком банківської карткової справи та сфери електронно-інформаційної взаємодії, з'явилась індустрія шахрайства, заснована на крадіжці даних з карток, з наступним зняттям грошей з банківських рахунків та можливостями несанкціонованого отримання відомостей про людину.

Згідно деякій статистиці, у минулому році в Україні сталося майже 72 тисячі випадків незаконних дій із платіжними картками, 58 % із них – в Інтернеті. У першому півріччі банки повідомили про фіксацію 47,5 тис. випадків шахрайства з картками на загальну суму 86,4 млн. грн., тоді як за перше півріччя 2019 року було зафіксовано 34,7 тис. випадків на 72,6 млн. грн. [1].

За 2021 рік кіберполіції вдалося задокументувати злочинну діяльність та скерувати до суду понад 2000 кримінальних проваджень, що стосуються саме Інтернет-шахрайства, до їх вчинення були причетні 422 зловмисники. У роботі перебуває ще понад 6600 проваджень. Саме шахрайські дії в Інтернеті становлять майже 70 % від усіх звернень, які надходять до кіберполіції. У цілому за минулий рік, у зафіксованих Нацполіцією випадками, кіберзлочинці ошукали громадян на понад 193 млн. грн.

Розповсюдженими шахрайськими схемами є: телефонні шахрайства, продаж неіснуючих товарів, псевдовиграші, фішингові ресурси для привласнення грошей або збору персональних даних, заволодіння грошима під приводом надприбутків та прохання знайомих про допомогу в соціальних мережах. Найбільш поширеним методом шахрайства з платіжними картками в Україні, як і у світі, залишається соціальна інженерія, завдяки застосуванню якої люди самі переказують гроші аферистам або розкривають їм дані своїх карток [2; 3].

Результати аналізу наукових публікацій. Сьогодні на сторінках Інтернету можна побачити значну кількість публікацій, присвячених незаконним операціям з використанням банківських пластикових карток за допомогою електронно-обчислювальної техніки, про що йдеться, зокрема, у [3]. Зловмисниками вже не раз з 2019 р. запускається у Facebook шахрайська схема, яка пропонує українцям 8900 гривень "допомоги від ЄС" [4], розмішено фейковий чат-бот державної платформи "Дія", у якому пропонують "отримати 3000 гривень грошової підтримки від держави" [5]. Навіть від імені Президента України, завдяки фальшивому (фейковому) відео щодо "гарантованої виплати у розмірі 8000 грн. кожному громадянинові", шахраї намагаються отримувати персональні дані, а через них – гроші довірливих людей [6].

Як вважаємо, продовжує існувати потреба в подальшому узагальненні та систематизації сучасних видів та схем (методів) шахрайської діяльності у сфері електронно-інформаційної взаємодії, в цілях більшого уявлення про підходи у методах злодійства карткових даних і відомостей про людину.

Метою статті є узагальнення та систематизація сучасних видів та схем (методів) шахрайської діяльності у сфері електронно-інформаційної взаємодії та надання пропозицій з удосконалення законодавства.

Виклад основного матеріалу. У законодавстві України правила використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку визначаються нормативними актами, що регулюють діяльність у сфері інформаційних та електронно-інформаційних відносин, за порушення яких, зокрема завдяки різним засобам і методам обману, що має назву "шахрайство", передбачені адміністративна, цивільна та кримінальна відповідальність. При цьому, слово "шахрайство" у Кодексі про адміністративні правопорушення [7] згадується безпосередньо лише у ст. 51 "Дрібне викрадення чужого майна", а у Цивільному кодексі України [8] його не застосовують.

Згідно ст. 190 Кримінального кодексу України (далі – КК України): "шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою" [9]. Ст. 361-363 КК України мають відношення лише до несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж.

Об'єктами шахрайського злодійства даних з банківських карток стають люди, комп'ютери, сервери та мережеве обладнання, веб-ресурси, мобільні пристрої, банкомати та POS-термінали, а також Інтернет речей (IoT).

Методи, з допомогою яких працюють хакери (або гакери), майже незмінні: шахраї збирають облікові дані та відомості про осіб (персональні дані), застосовують маніпулятивні прийоми соціальної інженерії та експлуатують вразливості веб-ресурсів, використовують шкідливе програмне забезпечення.

Основний мотив шахрайства – фінансова вигода, через одержання різноманітних відомостей про особу (персональних даних), її діяльність, інтереси, соціальні зв'язки тощо. Незважаючи на те, що інформація, як і персональні дані, законодавчо не визначаються об'єктом власності, їх можна купувати і продавати, зокрема, для обману, шантажу, афер, дезінформації, демагогії та, взагалі, для інформаційно-психологічного впливу та маніпуляції свідомістю людини [10, с. 41-82].

Згідно сучасного законодавства України [11] та держав-членів ЄС [12] *персональні дані* – це ім'я та прізвище, місце й дата народження, паспортні дані, адреса проживання, сімейний статус, освіта, професія, посада та доходи тощо.

У статті 4 Регламенту (ЄС) 2016/679 від 27.04.16 р. "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також

про скасування Директиви 95/46/ЄС (Загальний Регламент про захист даних)" встановлено: *персональні дані* означає будь-яку інформацію, що стосується фізичної особи, що ідентифікована або може бути ідентифікована ("суб'єкта даних"); фізична особа, що може бути ідентифікована – це особа, яка може бути ідентифікована, прямо чи опосередковано, зокрема за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місце розташування, он-лайн-ідентифікатор або на один чи декілька факторів, специфічних для фізичної, фізіологічної, генетичної, ментальної, економічної, культурної або соціальної ідентичності цієї фізичної особи [12, с. 45].

Таким чином, *формально персональні дані,* які визначають особисту інформацію кожної людини, охоплюють паролі та логіни банківських карток, адреса е-пошти, акаунти в соцмережах, онлайн-рахунки, побутове та ділове листування в Інтернеті – так званий цифровий профайл, який є важливим економічним та правовим активом у житті будь-якої людини [13]. До прикладу, розмістивши у мережі фото з обладнання, яке має програму геолокаційного відстеження (див. [14]), позначивши статус у фейсбуці, оплативши будь-що карткою або з допомогою смартфону, залишається цифровий слід і навколо людини створюється особистий інформаційний простір, відкритий для зловмисників. МВС вже зверталось із проханням виключити геолокацію на мобільних телефонах, оскільки ворог нібито починає орієнтуватися по скупченню мобільного трафіка [15].

У топі шахраїв – крадіжка номерів (даних) кредитних карток і банківських рахунків, захоплення акаунтів у соцмережах, злом паролів, поширення шкідливого програмного забезпечення, порушення авторських прав та багато ін.

У табличному вигляді відобразимо деякі основні види, зміст шахрайської діяльності та можливості захисту від неї.

Види-схеми	Зміст	Захист
Шахрайство (зняття даних) при використанні пластикової картки		
Повідомлення про надходження коштів	Шахраї розсилають SMS-повідомлення (далі – SMS) клієнтам банків про нібито надходження коштів на їхній рахунок. Пропонують слідувати по посиланнях.	Такі SMS можуть містити фішингові посилання (див. далі). Виконувати без особистого звернення до банку не рекомендується.
Посередницькі послуги	Пропонуються нібито "посередницькі послуги" по одержанню гарантованого відшкодування Фондом гарантування внесків фізичних осіб. За такі послуги просять "комісію".	НБУ уточнює, що виплати гарантованого відшкодування проводяться тільки через банки-агенти фонду, що підключені до автоматизованої системи виплат [16**].** Виплату можна одержати звернувшись до відділення одного з банків-агентів з паспортом і ідентифікаційним кодом, або – онлайн. Дистанційні виплати здійснюють три банки: Приватбанк, Укргазбанк і Південний.
Підробка банківської картки *(неелектронний фішинг)*	Пов'язаний зі збільшенням обсягів емісії мікропроцесорних	Звичайно, людина не одержує підроблену картку, оскільки їх

	карток і програми міжнародних платіжних систем “чип і PIN”, тобто здійсненням покупки у підприємстві торгівлі (послуг) за допомогою обов’язкового введення PIN-коду. На відміну від традиційного фішингу, у схемах неелектронного фішингу створюють реальні торгово-сервісні підприємства/ офіси або використовують вже існуючи. Власники платіжних карток роблять покупки товарів, одержують послуги або знімають кошти в касі банку. Операції проводяться з використанням банківських мікропроцесорних карток і супроводжуються введенням клієнтом свого PIN-коду. Шахраї негласно копіюють інформацію з магнітної смуги картки і роблять запис особистого ідентифікаційного номера. Далі виготовляється підроблена банківська картка, і в банкоматах проводиться зняття коштів з рахунку клієнта.	видають винятково банки. Щоб не дозволити зловмисникам зробити копію платіжної картки бажано користуватися тільки тими банкоматами, у яких установлені спеціальні прозорі антіскимери – як правило, зеленого кольору. Віддавати перевагу слід банкоматам у відділеннях банків, які обладнані відеокамерами. *Примітка.* Пластикова картка із чипом (вбудованою мікросхемою) безпечніше картки, у якої є тільки магнітна смуга. Чип має захищену область пам’яті, що дозволяє зберігати в ній конфіденційну інформацію й проводити її криптографічну обробку, може самостійно обробляти інформацію й обчислювати коди, допомагає провести авторизацію транзакції, що сприяє безпеці платежів. Переваги картки з чипом не є очевидними у випадку платежів через Інтернет. Тут вони нічим не краще магнітних. Шахраю досить знати дані, розміщені на лицьовій стороні картки, і три цифри CVC (код безпеки) з її зворотної сторони.
Шахрайство при оплаті карткою в мережі Інтернет		
Продаж товару *(надання послуги)*	Під маскою продавців шахраї “продають” не існуючі товари (або послуги). Можуть створюватися фейкові (клоновані) Інтернет-магазини або сайти з привабливими акціями або розіграшами, на яких розміщаються оголошення на платформі онлайн-об’яви. Аферисти переконують зробити передплату за товар (акцію, розіграш), відправляють фішингові	Щоб купувати онлайн безпечно, необхідно дотримуватися простих правил: - купуйте й оплачуйте тільки на перевірених сайтах. Назви та адреси справжнього й шахрайського сайту можуть бути майже однаковими, за винятком одного або декількох символів. На підроблених сайтах часто сторінки мають різні адреси, нерідко – граматичні помилки; використовуйте післяоплату;

	посилання для оплати, а потім зникають. Після того, як людина переходить по фішинговому посиланню і робить оплату, шахраї дізнаються банківські реквізити й привласнюють гроші на рахунках покупців.	не переходьте в месенджери, якщо купуєте на платформі онлайн-оголошень, обмовляйте деталі угоди тільки в чаті цієї платформи. Завжди тримайте в секреті: - тризначний номер (код) на звороті картки; - коди банків; - паролі до Інтернет-банкінгу. У мережі бажано використовувати псевдонім, при цьому ідентифікуюча інформація буде відома лише провайдеру послуг Інтернет.
Махінації з Інтернет-гаманцем *(електронним гаманцем)*	"Продавець" пропонує здійснити передоплату за товар. Після того як покупець відправляє гроші, "продавець" блокує користувача й не виходить на зв'язок. У підсумку ні грошей, ні товару.	Електронний гаманець – це віртуальний платіжний інструмент (програмне забезпечення, яке встановлено на смартфоне або комп'ютері) для зберігання грошей у цифровому виді (електронні гроші), їх переведення і оплати за допомогою Інтернету. Випускати електронні гроші в Україні можуть тільки банки. Не переходьте за посиланнями від незнайомців. Виконувати без перевірки сайту не рекомендується.
Фішинг ("телефон+рибний лов") – це крадіжка реквізитов картки, паролів, кодів банків. Дані крадуть за допомогою розсилання клієнтам листів, email, або SMS, що маскуються під повідомлення від банків або відомих компаній, брендів про блокування картки, про надходження коштів, пропозицій про зміну настроювань, або рекомендацій передзвонити на номер мобільного телефону з метою одержання інструкцій з розблокування картки.	Містять посилання на підроблений сайт, зовні не відрізняється від сьогоденного (буде схожий на посилання офіційного сайту банку або платформи онлайн-продаж, але з мінімальними змінами, наприклад зайвою літерою в адресі сайту). На ньому клієнтові пропонують увести логін і пароль для доступу до Інтернет-банкінгу. Одержавши ці дані, шахраї знімають гроші з рахунку. Часто підроблені сайти маскуються під Інтернет-магазин, який пропонує товар за низькою ціною. Обов'язковою умовою покупки на такому сайті є передоплата. Клієнт, що не підозрює, надає повні дані	Щоб не стати жертвою фішера, необхідно: - коли заходите на сайт, вивчите, як він виглядає зовні, зверніть увагу на адресу. Усього лише одна неправильна буква в назві повинна насторожити; - якщо на сайті мається на увазі виконання якої-небудь операції (наприклад, уведення карткових даних), то посилання обов'язково повинне починатися з "https://", що означає "безпечне з'єднання". Якщо ж в адресі зазначене просто "http:// ", це відразу має насторожити; - не спішите переходити по посиланнях, які приходять у рекламних листах або SMS, вони можуть бути від шахраїв.

	своєї банківської картки і через якийсь час виявляє пропажу грошей з карткового рахунку. При цьому, ніякого товару він не одержує.	
Фармінг – спрямовування користувачів на підроблені сайти	Шахрай спрямовує на комп'ютери користувачів спеціальні шкідливі програми, які після його запуску спрямовують користувача до іншого підробленого сайту. Зайшовши на такий сайт, користувач для виконання операції по своєму рахунку, змушений підтвердити свої паролі і вказати реквізити банківської картки, які тим самим стають відомі шахраям. Крім того, власники стільникових телефонів можуть одержувати SMS, що заманюють їх на інфікований веб-сайт. У тексті SMS повідомляється про те, що він підписаний на якусь платну послугу, за яку з його рахунку буде утримуватися певна сума, і якщо він прагне відмовитися від даної послуги, то йому потрібно зайти на сайт. Зайшовши на зазначений в SMS сайт, користувач активує троянську програму, яка заражає комп'ютер і надає шахраям до нього доступ (вид шахрайства "смішинг" – від SMS+phishing).	Фармінг, як і фішинг та ін. шахрайські схеми переслідують мету отримання даних банківської картки з наступним доступом до банківського рахунку. Надавати паролі та реквізити картки без перевірок не рекомендується. *Єдине, що можна використовувати при пересилці коштів, здійснення оплати отримання коштів на картку від іншої особи або організації* – 16-значний номер картки. ПІБ – не обов'язково. Ще раз звернемо увагу – *не слід повідомляти інші дані своєї картки* такі, як: - PIN-код; - CVC2/CVV2-код; - термін дії; - паролі Інтернет-банкінгу; - коди підтвердження онлайн-платежів в SMS або в повідомленнях у месенджері. Контролюйте рух коштів на баківському рахунку.
Сніферінг (від англ. "винюхувати") – це спосіб шахрайства, при якому зловмисник використовує аналізатор трафіка Інтернет-мережи ("сніфер") – програму для перехоплення даних з можливістю їх декодування та аналізу.	Сніферінг популярний у людних місцях, скрізь, де є загальнодоступна мережа Wi-Fi.	Слід дотримуватися обережності в місцях загальнодоступної мережі. З погляду безпеки існують погрози властиві середовищу передачі сигналу. У бездротових мережах одержати доступ до даних простіше, чим у дротових, так само як і вплинути на канал передачі даних. Досить помістити відповідне обладнання в зоні дії мережі, див., наприклад [17].
Шахрайство через e-mail	На e-mail приходить лист від "адвоката" про те, що загинув	Не слід відправляти кудись гроші, тим більше, надавати

	далекий родич потенційної жертви, який залишив їй значний спадок. Щоб отримати подарунок, потрібно відправити кошти для оплати послуг “адвоката”. Після переказу грошей – “адвокат” зникає.	відомості про себе та дані своєї картки особам, про яких ви нічого не знаєте. Це може відноситися й до телефонних дзвінків з “поліції”, “лікарні”, “знайомих” щодо подій з родичами.
Повідомлення про виплату від держави *(зокрема, за допомогою e-mail*)	Розсилання в соціальних мережах повідомлення про термінову “перевірку” картки, на яку повинні прийти виплати. Для цього пропонується перейти по посиланнях.	Інформація про держвиплатах і порядок їх одержання розміщується на офіційних сайтах. За допомогою посилань крадуться карткові дані і відбувається зараження обладнання вірусом.
Злом сторінки в соцмережах	Один з найпоширеніших способів шахрайства [18] у “просунутих” кібершахраїв.	При зломі сторінки в соцмережі (наприклад Facebook) необхідно: 1. Терміново змінити пароль на сторінку, якщо ви не втратили доступ до свого облікового запису. Для цього: - відкрийте “Меню” у правому верхньому куті сторінки Facebook; - виберіть “Настроювання” і “Конфіденційність”, потім натисніть “Настроювання”; - натисніть кнопку “Безпека” і “Авторизація”; - клацніть “Редагувати” поруч із пунктом “Змінити пароль”; - уведіть поточний і новий паролі; - натисніть “Зберегти зміни”. 2. Повідомити Facebook, що ваш обліковий запис зламали. 3. Якщо немає доступу до своєї сторінки в Facebook. Для цього в шапці сторінки слід натиснути три крапки й вибрати пункт “Допомогти”, далі – “Злом акаунта”.
Вішинг – метод соціальної інженерії, який використовують шахраї для крадіжки карткових даних безпосередньо у клієнта.	1. Під видом працівника банку випитується інформація про картку: номер картки, термін дії, CVV/CVC2-код. Отримавши ці дані, шахраї знімають гроші з картки. 2. Шахраї представляються службою безпеки банку й повідомляють клієнта про підозрілу операцію з його карткою й про можливість	Звичайно шахраї прагнуть знати – номер картки та код CVV2 чи CVC2 (код безпеки), в залежності від платіжної системи (Visa або Mastercard). Якщо стороння людина просить назвати йому ці дані – це шахрай. CVV-код чи CVC2-код – тризначний захисний код на зворотній стороні картки.

	повернути нібито списані з картки гроші. Або повідомляють про збій у системі банку й необхідність блокувати картку. Для розв'язання проблеми шахраї просять повідомити дані картки, паролі веб-банкінгу. При цьому вони за допомогою сучасних технологій використовують підміну номерів телефонів під офіційні номери банку, тим самим присипляючи пильність клієнта. 3. Шахраї повідомляють, що з банківською карткою клієнта або мобільним додатком відбувся якийсь інцидент, і переконують установити додаток, що нібито захищає кошти. Такі додатки можуть виявитися програмами дистанційного доступу й керування обладнанням клієнта: TeamViewer, AnyDesk чи їх аналоги. Після установки такої програми і одержання ідентифікаційних даних та кодів доступу шахраї підключаються до обладнання жертви й можуть керувати ним, знімати будь-яку інформацію, виконувати операції через веб-банкінг.	Його сутність – ідентифікація банківського рахунку реального власника картки. Використовується для захищеної оплати в Інтернеті. Іноді банк сумнівається, що операція проводиться власником картки, навіть якщо всі реквізити зазначені вірно, у тому числі, з кодом безпеки. Тоді на номер телефону, зазначений при оформленні картки, приходить SMS з одноразовим кодом . Його треба ввести в запропоновану форму для підтвердження. Слід пам'ятати, що банківські працівники та ін. особи не мають права звертатися до клієнтів (дзвонити) з метою уточнення карткових даних, даних рахунків або встановлення нових додатків. Якщо така ситуація відбудеться, з банку мають запросити відвідати особисто. *Примітка.* У разі пропозиції "людини з Інтернету" про зустріч – бажано не поспішати погоджуватися та ставати об'єктом спритного, маніпулятивного поводження, як з річчю.
Шахрайство при використанні банкомата		
Скімінг – вид злодійства, коли шахраї копіюють дані платіжної картки за допомогою скімера – спеціального обладнання, що встановлюється на або усередину карткоприймача банкомата. Надалі це дозволяє їм виготовити дублікат платіжної картки (т.зв. "білий пластик" – пластик з магнітною смугою й нанесеною на неї украденою інформацією).	Скімер-прилад маскується під деталь банкомати. Це може бути: - тонка пластинка, яка вставляється усередину карткоприймача; - накладка, що кріпиться на карткоприймачі банкомата.	Щоб захистити інформацію з картки та PIN-код необхідно: - уважно оглянути банкомат перед використанням; - при введенні PIN-коду прикрити клавіатуру таким чином, щоб його не підглянути за допомогою мікровідеокамери; - якщо банкомат не повертає картку, слід негайно звернутися до відповідного банку. *Примітка.* Передавати будь-

Але скопійована платіжна картка ніщо без PIN-коду. PIN-код картки викрадається при натисканні клавіш. Також, щоб довідатися PIN-код, шахраї можуть застосовувати мікрокамеру, через яку спостерігають, який PIN-код уводиться.		кому картку небажано. Карткові дані можуть бути скопійовані, наприклад, офіціантом у кафе. Бажано особисто скористатися мобільним терміналом.
Вставка в отвір карткоприймача банкомата	Відрізок фотоплівки (вставка) який складається навпіл, а краї загинаються під кутом в 90 градусів, шахрай закладає в отвір карткоприймача банкомата. При цьому, на нижній стороні вставки вирізана невелика пелюстка, відігнута нагору по ходу картки. Банкомат, технічно, не може зчитати дані з магнітної смуги, але й повернути картку через вставку також неможливо. Після того, як ви заклали картку у карткоприймач (насправді, у вставку) й намагаєтесь отримати гроші або повернути картку, підходить шахрай і пропонує свою допомогу, але для цього власникові необхідно зробити ряд дій, у тому числі й набрати PIN-код. Незважаючи на це картка не повертається. Якщо власник іде, щоб зв'язатися з банком, шахрай же спокійно виймає вставку разом із карткою. PIN-код він уже знає, і йому залишається тільки зняти кошти з рахунку.	Слід пам'ятати, що головний захист проти шахраїв сьогодні – це бути уважним.
Фальшиві банкомати	Шахраї створюють фальшиві банкомати або фальшиві PIN-PADи (прилад для введення PIN-коду), які виглядають як справжні. Вони розміщають їх у таких місцях, як, наприклад, торговельні центри, де власники банківських карток нічого не підозрюють, а шахраї намагаються одержати гроші з таких фальшивих	Це дороге у виготовленні обладнання, тому зустрічається рідко. Слід бути уважним.

	банкоматів. Після введення картки й PIN-коду, звичайно, на дисплеї фальшивого банкомата з'являється напис, що грошей у банкоматі немає або що банкомат несправний. На той час шахраї вже скопіювали з магнітної смуги картки інформацію про рахунок людини і її карткові дані.	
Залишення шахраєм картки в банкоматі	Шахрай нібито випадково забуває картку в банкоматі й просить вас її вилучити. Після того, шахрай бере картку, перевіряє її баланс і починає стверджувати, що з його рахунку пропали гроші. Він змушує повернути цю суму у людини, що дістала картку. У цій шахрайської схеми можуть брати участь двоє або троє – будуть зображувати "свідків крадіжки" грошей з картки. Більш того, шахрай почне загрожувати викликати поліцію, обґрунтовуючи це тим, що на його картці залишилися ваші відбитки пальців, і буде легко довести пропажу грошей з картки.	Насправді ж ніякої крадіжки коштів від дотику до карти не відбувається. Шахраї намагаються отримати кошти шляхом інформаційної маніпуляції, обману та залякуванням.

На завершення нагадаємо деякі загальні санкції щодо шахрайської діяльності, які визначені сучасним законодавством.

Згідно статті 145 Кодексу України про адміністративні правопорушення порушення умов і правил, що регламентують діяльність у сфері телекомунікацій та користування радіочастотним ресурсом України, тягне за собою накладення штрафу до двох тисяч неоподатковуваних мінімумів доходів громадян. Інші санкції щодо порушення посадовими особами Правил надання та отримання телекомунікаційних послуг визначаються статтями 146-148.

Згідно статті 190 Кримінального кодексу України, "шахрайство" – як заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою, карається штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк від двохсот до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років. Шахрайство, вчинене повторно, або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому, карається штрафом від трьох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк від одного до двох років, або

обмеженням волі на строк до п’яти років, або позбавленням волі на строк до трьох років. А шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки, карається позбавленням волі на строк від трьох до восьми років.

Крім цього, КК України має Розділ XVI “Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” в якому визначені санкції за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку (стаття 361), за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361^1), несанкціоновані дії з інформацією (зміна, знищення, блокування, зберігається, перехоплення або копіювання), яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації (стаття 362) та ін.

24 березня 2022 року Верховна Рада прийняла Закон України “Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану” № 2149-IX. Новою редакцією ст. 361 КК України посилена відповідальність за несанкціоноване втручання у роботу електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, яка може передбачати позбавлення волі на строк від десяти до п’ятнадцяти років, в залежності від наслідків [19].

Стосовно накладання конкретних штрафних санкцій за порушення законодавства у сфері захисту персональних даних, то у Законі України “Про захист персональних даних” застосовано таке бланкетне формулювання: *Стаття 28. Порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом*.

На наш погляд, по-перше, зазначений спосіб викладу норм не дуже сприяє становленню системи захисту персональних даних, як окремої системи у сфері інформаційного права та у складі загальної системи права і законодавства України.

По-друге, згадана вище відповідальність може визначатися статтею 188^{39} Кодексу України про адміністративні правопорушення, яка стосується діяльності та обов’язків органів виконавчої влади, а не Уповноваженого Верховної Ради України з прав людини, як сьогодні згідно до законодавства – головного суб’єкта контролю діяльності у сфері захисту персональних даних. Фактичне здійснення функцій органу виконавчої влади Уповноваженим Верховної Ради України не відповідає положенням ст. 6 Конституції України в частині поділу державної влади в Україні на законодавчу, виконавчу і судову та розподілу функцій відповідних державних органів, про що йдеться, зокрема, у [20].

У загальному організаційно-правовому та нормативному плані, існуюча в Україні система захисту персональних даних не відповідає таким європейським правовим стандартам, як Конвенція Ради Європи № 108 та Регламент (ЄС) 2016/679 від 27.04.16 р., які є обов’язковими у виконанні нормативними актами та передбачають визначення у кожній державі-члена РЄ та ЄС незалежного державного органу, відповідального за контроль застосування цих стандартів та відповідного Закону.

Тому, навіть з цих зауважень можна мати сумніви у наявності ефективної державної системи нагляду та контролю у сфері захисту персональних даних, наявності належного правового механізму притягнення до відповідальності за здійснення

правопорушень, зокрема у банківсько-фінансової діяльності з застосуванням платіжних карток.

Висновки та рекомендації.

Вважаємо за можливе навести деякі узагальнення та надати наступні застереження.

У основі усіх шахрайських схем полягає маніпуляція свідомістю людини, де вона стає об'єктом, засобом досягнення цілей одних людей за рахунок маніпулювання іншими. Маніпуляція, як є фактор соціальної інженерії ("винахід") шахраїв, у інформаціно-психологічному аспекті – не насильство, а спокуса. У принципі це поняття означає набір методів прихованого управління, часто у взаємодії.

Щодо застережень у зв'язку з шахрайським злодійством персональних даних та відомостей про людину можна зазначити наступне.

1. Забезпечення безпеки та захисту при використанні пластикової картки.

Фахівці з інформаційної безпеки сходяться в думці – щоб захистити себе єдиний реальний спосіб знизити ймовірність шахрайства з карткою – це дотримуватися звичайних правил безпеки. Вони закликають усіх уважніше ставитися до своїх карток: не довіряти картки третім особам, не залишати їх без догляду, не записувати PIN-код на самій картці та у легкодоступних місцях. Важливо ніколи нікому не повідомляти свій PIN-код. Його не має права вимагати ні працівник банку, що видав картку, ні персонал, що обслуговує банкомат, тим більше будь-які інші особи.

У жодному разі не слід залишати картку без уваги, розплачуючись у ресторанах або магазинах. Краще попросить, щоб картку пропустили через імпринтер у вашій присутності. Слід уважно дивитися, що роблять із вашою карткою, не розплачуйтеся нею у сумнівних закладах і обов'язково зберігайте в себе чек. Відомі випадки, коли при оплаті послуг у ресторані, протягом усього лише пари хвилин, поки картка перебувала поза полем зору власника, з магнітної смуги картки зчитувалися персональні дані й інша конфіденційна інформація про її власника, а також зникали кошти з карткового рахунку.

Коли виникають сумніви в правильності списання грошей з рахунку, втрати платіжної картки або її крадіжки, необхідно негайно звернутися в банк і, пояснивши ситуацію, просити її заблокувати. Можна також направити заяву в поліцію. Розслідувати шахрайство по "гарячих слідах" набагато легше, ніж якщо власник раптом отямиться через якийсь час.

2. Забезпечення безпеки та захисту при оплаті карткою в мережі Інтернет.

Не рекомендується спрямовувати дані про себе і свою картку на ті сайти, про які мало що відомо. Можна запитати про ці сайти у знайомих, поцікавитися у відповідних конференціях, довідатися, де розташовується сама організація, з якою збираєтеся робити грошові операції. При цьому слід звертайти увагу на різні сертифікати, що підтверджують безпеку розрахунків через даний сайт. Якщо адреси немає зовсім або вона не викликає довіри, то перш ніж платити, подумайте, а чи варто це робити?

Фахівці з безпеки рекомендують – завжди перевіряйте правильність назви сайтів, на які переходите й уводите свої персональні дані. Адреси справжнього й шахрайського сайту можуть бути схожі за винятком одного або декількох символів. Якщо все-таки необхідно перейти на сайт банку або ін. організації, адресу якої одержали в посиланні, краще введіть у пошуковій системі назву сайту й тільки тоді переходьте на веб-ресурс.

Не використовуйте для оплати в мережі Інтернет картки, на яких перебувають великі суми грошей. Краще завести для таких цілей окрему картку та переводити туди гроші.

У загальному плані важливо пам'ятати наступне.

Інтернет, будь-яка інша мережа, не є безпечним інформаційним середовищем. Слід використовувати всі засоби для захисту персональних даних, зокрема при можливості шифрувати конфіденційні відомості, зберігати паролі доступу до комп'ютера.

Адреса е-пошти також є персональними даними. Вона може бути включена до різних каталогів чи списків користувачів. Користувач Інтернет-послугами може запитувати про призначення каталогів та вимагати виключення своїх персональних даних із них, якщо не бажає у них фігурувати. Необхідно бути обережним з веб-вузлами, які вимагають надання більше відомостей, ніж це необхідно для доступу до вузла.

Провайдер послуг Інтернет несе відповідальність за правильне використання персональних даних. Час від часу варто з'ясовувати: які персональні дані він збирає, зберігає і поширює, яким чином і з якою метою. Він зобов'язаний виправляти дані, якщо вони помилкові, чи знищити їх, якщо вони надлишкові чи застаріли. У тому випадку, коли користувач не задоволений способом, яким збираються, зберігаються та поширюються персональні дані, необхідно перейти до іншого провайдера.

Після кожної операції на вузлах Інтернет, які були відвідані, залишаються сліди. Ці "електронні сліди" можуть бути використані для збирання різних відомостей щодо відвідувача. Бажано використовувати псевдонім, при цьому ідентифікуюча інформація буде відома лише провайдеру послуг Інтернет. Йому чи будь-якій іншій особі можливо надавати лише ті персональні дані, які слугують потребам забезпечення комунікації.

Перед передачею персональних даних у інші країни варто перевіряти її статус щодо ратифікації Конвенції Ради Європи № 108, яка є складовою законодавства України з 6.07.10 р. Якщо країна не ратифікувала Конвенцію, може статися що одержувач, якому надають дані, має надати згоду на укладення договору про захист персональних даних.

3. Забезпечення безпеки у банкомата.

Намагайтеся не користуватися банкоматами в безлюдних місцях, у місцях великого скупчення людей, у темний час доби. У таких випадках при знятті грошей власник картки стає занадто вразливим об'єктом для пограбування. А в юрбі не можна бути впевненим, що ніхто не побачить, якій користувачем вводиться PIN-код. Зовсім крайня ситуація – раптове отримання тілесного ушкодження й пограбування.

Слід бути уважним та не помилятися при введенні PIN-коду. Після трьох помилкових уведень коду банкомат затримає картку.

Перевіряйте, чи все було взято з банкомата. Після завершення операції у власника картки повинні залишитися: картка, гроші та виписка про зроблену операцію. Якщо чогось не вистачає, а банкомат не надав ніякої додаткової інформації, то тут щось не так. Можливо, власник картки ризикує стати жертвою шахраїв.

Бажано завжди перевіряти та зберігати виписки за підсумками операції, які видає банкомат. Це дозволить вести облік витрат і контролювати списання грошей з банківського рахунку.

В якості пропозицій з удосконалення законодавства можна запропонувати ввести у останню версію законопроекту України "Про захист персональних даних" від 07.06.21 р. № 5628-IX [21], якій знаходиться на стадії доопрацювання, наступні формулювання:

– до відповідальності передбаченої цим Законом можуть бути притягнені контролери, оператори персональних даних, треті особи та фізичні особи які здійснюють правопорушення у сфері банківсько-фінансової діяльності з застосуванням платіжних карток;

– порушення вимог цього Закону, що призвело до порушення прав суб'єктів персональних даних у сфері банківсько-фінансової діяльності з застосуванням платіжних карток – тягне за собою накладення штрафу в розмірі від 10000 до 50000 гривень.

Використана література

1. Карткове шахрайство: нові “мутації” старих схем. URL: https://www.ukrinform.ua/rubric-economy/3230485-kartkove-sahrajstvo-novi-mutacii-starih-shem.html

2. НБУ починає кампанію з безпеки безготівкових розрахунків. – (14 лютого 2022 р.). URL: https://finclub.net/ua/news/nbu-prodovzhuie-kampaniiu-z-platizhnoi-bezpeky-shakhraihudbai.html

3. Телефонне шахрайство. URL: https://my.ukrsibbank.com/ua/personal/news/411582; Популярні схеми карткових шахраїв. URL: https://finance.ua/cards/karti-dengi-obman; Як не стати жертвою шахраїв в Інтернеті. URL: https://minjust.gov.ua/m/yak-ne-stati-jertvoyu-shahraiv-v-interneti-ta-scho -robiti-yakscho-vi-potrapili-u-pastku; ТОП 10 видів шахрайства з платіжними картками. URL: https://financer.com/ua/blog/vydy-shahraystva; НБУ попередив про нову схему шахраїв: розсилають посилки “Новою поштою”. URL: https://gazeta.ua/articles/life/_nbu-poperediv-pro-novu-shemu-shahrayiv-rozsil ayut-posilki-novoyu-poshtoyu/1098963

4. Шахраї обіцяють українцям 8900 гривень “допомоги від ЄС” за проходження опитування. URL: https://ms.detector.media/kiberbezpeka/post/29339/2022-04-14-shakhrai-obitsyay ut-ukraintsyam -8900-gryven-dopomogy-vid-ies-za-prokhodzhennya-opytuvannya

5. Шахраї створили фейковий бот “Дії”, у якому пропонують “отримати 3000 гривень”. URL: https://t.me/stop_fake_dp/114?fbclid=IwAR21bhWBfJgbmRCwmaifWuHbgHuh25oCh12 Cl83kl_ 1MJWD_KuOjKiArWqU

6. За допомогою фейкового відео шахраї хочуть заволодіти персональними даними українців. URL: https://armyinform.com.ua/2022/07/17/za-dopomogoyu-fejkovogo-video-de-vykorystano -zjomky-v-zelenskogo-shahrayi-namagayutsya-zavolodity-personalnymy-danymy-ukrayincziv

7. Кодекс України про адміністративні правопорушення (статті 1-212[24]): Закон України від 07.12.84 р. № 8073-X. *Відомості Верховної Ради Української РСР (ВВР),* 1984. Додаток до № 51. Ст. 1122. URL: https://zakon.rada.gov.ua/laws/show/80731-10#top

8. Цивільний кодекс України: Закон України 16.01.03 р. № 435-IV. *Відомості Верховної Ради України (ВВР),* 2003. №№ 40-44. Ст. 356. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

9. Кримінальний кодекс України: Закон України від 05.04.01 р. № 2341-III. *Відомості Верховної Ради України (ВВР),* 2001. № 25-26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/ 2341-14#Text

10. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с. ISBN 978-966-96731-6-9.

11. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI. *Відомості Верховної Ради України (ВВР),* 2010. № 34. Ст. 481; Пилипчук В.Г., Брижко В.М., Баранов О.А., Мельник К.С. Становлення і розвиток правових основ та системи захисту персональних даних в Україні”: монографія / за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ “Видавничий дім “АртЕк”, 2017. 226 с.

12. Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних / І. Майстренко – переклад з англ.; В. Брижко – переклад з англ. та редагування тексту. – (НДІ інформатики і права НАПрН України). Київ: ТОВ “Видавничий дім “АртЕк”, 2018. 177 с.

13. Брижко В.М. Економічні та правові аспекти проблеми захисту персональних даних. *Правова інформатика*. № 1(29)/2011. С. 25-33.

14. Про геолокаційне відстеження. URL: https://search.ukr.net/?q=%D0%B3%D0%B5%D0% BE%D0%BB%D0%BE%D0%BA%D0%B0%D1%86%D0%B8%D1%8F#gsc.tab=0&gsc.q=%D0% B3% D0%B5%D0%BE%D0%BB%D0%BE%D0%BA%D0%B0%D1%86%D0%B8%D1%8F&gsc.page=1

15. Про звернення МВС. URL: https://www.pravda.com.ua/rus/news/ 2022/02/26/7326296

16. Повідомлення НБУ щодо гарантованого відшкодування. URL: https://finance.ua/cards/ karti -dengi-obman

17. Захист в мережах Wi-Fi. URL: https://wifi-solutions.ru/kak-zashchitit-wifi-10-sovetov-dlya-bezopasnosti-besprovodnoj-seti; https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D1%89%D0%B8% D1%82% D0%B0_%D0%B2_%D1%81%D0%B5%D1%82%D1%8F%D1%85_Wi-Fi

18. Злом сторінки в соцсетях. URL: https://ukranews.com/news/864880-gosspetssvyazi-dala-sovety-chto-delat-pri-vzlome-stranitsy-v-sotsseti

19. До 15 років позбавлення волі за втручання у роботу електронних систем. URL: https://lexinform.com.ua/zakonodavstvo/do-15-rokiv-pozbavlennya-voli-za-vtruchannya-u-robotu-elektron nyh-system

20. Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху: монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса: Фенікс, 2020. 260 с. С. 158-159. ISBN 978-966-928-618-5.

21. Про захист персональних даних: версія проекту закона України від 07.06.21 р. № 5628-IX. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~