ФІНАНСИ, БАНКІВСЬКА СПРАВА ТА СТРАХУВАННЯ

УДК: 336;
DOI: 10.31388/2519-884X-2020-41-5-12

Баханова М. В*., к. е н., доцент*
Чорноморське вище військово-морське училище імені П.С. Нахімова
Синяєва Л.В., *д.е.н., професор,*
Таврійський державний агротехнологічний університет імені Дмитра Моторного

КІБЕРШАХРАЙСТВА ТА КІБЕРБЕЗПЕКА У БАНКІВСЬКІЙ СФЕРІ

Анотація*. Статтю присвячено проблемі незаконного використання інформаційних систем у банківській сфері. Розглянуто основні популярні кібершахрайські атаки у фінансовій сфері і принципи протидії їм. Даються рекомендації щодо захисту від кібератак як фізичним особам, так і превентивно в масштабах державного адміністрування.*

Ключові слова*: інформаційні загрози, інформаційні технології, інформаційна безпека, цифрові технології, кібершахрайство, кібербезпека,*

JEL code classification: G21, G29

Bakhanova M. V.*, PhD, Ass. Prof*
P.S. Nakhimov Black Sea Higher Naval School
Sinyayeva L.V., *Doctor of Economics, Professor,*
Dmytro Motornyi Tavria State Agrotechnological University

CYBER SHIP AND CYBER SECURITY IN THE BANKING SPHERE

Abstract. *The article is devoted to the problem of illegal use of information systems in the banking sector. The analysis shows the lack of information security and data protection in information and telecommunications systems of government agencies due to the obsolescence of automatic systems for detecting and assessing information threats, failure to use the potential for forecasting and anticipation of threats to prepare the system for possible attack. The main popular cybershake attacks in the financial sphere and the principles of counteracting them are considered. The author believes that it is necessary to create a favorable legal environment that will involve leading experts in the field of cybersecurity, as well as to promote the creation of a national information system, platform and products to reduce the share of foreign cybersecurity software used by public authorities. management. The types and the most common types of cybercrime are considered in detail - namely: skimming, carding, phishing (SMS phishing and Internet phishing), vishing, skimming, shimming, online fraud, piracy, refilling and others. There are recommendations for protection against cybercrime, as well as ways to protect against fraud, which can significantly minimize the risk of loss of bank codes and security passwords that the bank sends to the client to confirm financial transactions. Thus, it is safe to say that cyber fraud and cybercrime are the main problems of the XXI century, the solution of which requires modern methods, active, decisive measures and timely regulatory response, and the rapid development of digital technologies has caused significant growth and spread of cyber fraud and cybercrime. It is to be hoped that the level of security in Ukraine's Internet space will soon increase significantly. Only a concerted effort can counter this threat to the 21st century.*

Keywords: *information threats, information technologies, information security, digital technologies, cyber fraud, cybersecurity.*

Постановка проблеми. У наш час людство переживає бурхливий розвиток автоматизації, інформатизації та комп'ютеризації всіх сфер життя. Це надає нові можливості для

розвитку національної культури, освіти, науки й економіки. Але поширення інформаційних технологій має й негативний аспект: відкриває шлях до антисоціальної та злочинної поведінки. Комп'ютерні системи надають нові, дуже досконалі можливості для невідомих раніше правопорушень та для скоєння традиційних злочинів, але нетрадиційними засобами.

В останнє десятиліття в Україні спостерігається стрімкий розвиток інформаційних технологій. Нажаль він супроводжується динамічним розвитком злочинів у даній сфері. З абсолютною впевненістю можна сказати, що саме, так звані, кіберзлочини є найдинамічнішою групою суспільно небезпечних діянь, адже з кожним роком кіберзлочини стають більш масовими і небезпечними.

Аналіз останніх досліджень і публікацій. Проблемою кібершахрайств у банківській сфері займаються останні 10-15 років. Це пов'язано із зростанням науково-технічного прогресу в галузі інформаційних технологій та програмного забезпечення, а також збільшенням доступності до інформації звичайного користувача. Типологія суб'єктів фінансового шахрайства в комерційних банках досліджувалася в наукових працях Д.Н. Козлова, В.В. Левіна, Н.С. Подосенка, О. Саяпіна, А.М. Шевченка та інших. Способи проведення шахрайських операцій в банківський сфері представлені в наукових роботах О.В. Кришевича, С.В. Поперешняка, С.В. Шапочки та інших. М. В. Карчевський і В. В. Невгад зазначають, що терміни «кіберзлочинність», «кібершахраї», «хакери», «комп'ютерний злом», «крадіжка машинного часу» перестали бути екзотикою для юристів. Ю. А. Бельський, П. А. Воробей, А. В. Савченко та О. Г. Колб, аналізуючи особливості кримінальної відповідальності за злочини, передбачені ст. 361 Кримінального кодексу України, зазначають, що завдяки глобальному проникненню комп'ютерних технологій у сфери суспільного життя створюються нові умови та способи для вчинення комп'ютерних злочинів, що призводить до їх зростання. Статистичні дані Генеральної прокуратури свідчать, що в Україні спостерігається тенденція до зростання кількості злочинів, скоєних у сфері використання комп'ютерів та комп'ютерних мереж.

Найбільшу частку комп'ютерних злочинів (73,8% від загальної кількості) становлять діяння, передбачені ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». Впродовж 2014-2017 рр. Державним центром кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України було зареєстровано 792 випадки різних типів посягань на інформацію, яка обробляється засобами ЕОМ.

Формулювання цілей статті. Метою статті є аналіз основних типів кібершахрайських атак, що відбуваються у фінансовій сфері, принципи протидії їм та формування можливих напрямів організації їх виявлення та попередження.

Виклад основного матеріалу. У контексті забезпечення державної безпеки України питання захисту державних інформаційних систем є актуальним. Кількість спроб втручання в інформаційні системи держави постійно зростає, зростає також і кількість способів та варіацій таких дій.

Слід зазначити про недостатній рівень інформаційної безпеки та захисту даних в інформаційно-телекомунікаційних системах державних органів через застарілість автоматичних систем виявлення та оцінки інформаційних загроз, невикористання потенціалу прогнозування та передбачення загроз з метою завчасної підготовки системи до можливої атаки. Потребують модернізації системи автоматичного стримування і запобігання можливим кібератакам.

Для вирішення зазначених проблем необхідно обробляти значні обсяги даних, які надходять з різних систем інформаційної безпеки підприємства. Для цього найкраще підходять методи і алгоритми роботи з великими обсягами даних та штучним інтелектом.

Для вирішення проблем кібербезпеки у державному секторі необхідним є створення сприятливого законодавчого середовища, яке дозволить залучати провідних фахівців у сфері кібербезпеки. Важливо також виважено підходити до питання ліцензування іноземних розробок у сфері кібербезпеки, особливо у державному секторі, зважаючи на

питання забезпечення національної безпеки України.

Необхідно сприяти створенню національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління.

Пріоритетними напрямами з розробки програмного забезпечення у сфері кібербезпеки можна визначити: захист критичної інфраструктури зі зберігання та обробки даних у державному секторі (енергетика, транспорт, оборона, космічна галузь тощо), відстеження політичної дезінформації (фейкові новини).

З кожним днем у світі зростає число злочинів, пов'язаних з використанням інформаційних технологій, у тому числі й у сфері фінансів. У щорічному звіті «Hi-TechCrimeTrends 2019/2020», де аналізуються глобальні тренди розвитку кіберзлочинності і прогнозуються майбутні цілі проурядових хакерських груп і фінансово-вмотивованих хакерів, спостерігається зростання економічних збитків від кібершахрайства у банківській сфері. За минулий рік збитки становили близько 200 млрд. доларів США [3].

Кібершахрайство – це вид злочину, спрямований на завдання матеріальної або іншої шкоди шляхом розкрадання особистої інформації користувача з використанням інтерактивних технологій [1]. Якщо взяти дані про стан злочинності, наприклад, в Росії з січня по грудень 2019 р., то можна констатувати, що найбільша кількість злочинів у сфері економіки відбувалась у сфері інформаційно-телекомунікаційних технологій. Зареєстровано понад 294 тисяч злочинів, що майже на 70% більше, ніж за аналогічний період минулого року.

За даними МВС у 2019 р. кількість злочинів, скоєних через Інтернет, зросла на 44%. В 1,3 рази частіше стали фіксуватися злочини з банківськими картами, а на 91% – злочини з використанням мобільних телефонів [2].

Шахрайство в банківській сфері з кожним роком набирає обертів, особливо в режимі самоізоляції і віддалених платежів: при оформленні заявок, реєстрації на сайтах, і навіть під час підписання договору, обов'язково мають бути зафіксовані персональні дані (паспорт, номер телефону, дата народження), а при оплаті товару – номер банківської карти. При цьому, відсутня стовідсоткова гарантія того, що дані не потраплять до рук зловмисників. За останні п'ять років в Україні кількість інформаційних злочинів зросла мінімум в 2,5 рази, а в даркнеті (анонімній мережі) стає все більше пропозицій для хакерів. Як пояснює платформа для роботи з відкритими даними «Опендатабот» (українська компанія, що збирає, об’єднує та аналізує дані основних публічних реєстрів країни), злочини в сфері інформаційних технологій (кіберзлочини) – це різні види злочинів, які здійснюються за допомогою комп'ютера і мережі Інтернет.

Зокрема, кіберзлочинці полюють на персональні дані, банківські рахунки, паролі та іншу інформацію, яка існує в електронному вигляді. Потерпілими можуть стати як фізичні особи, так і бізнес, і державний сектор. Так, у 2017 р. в Україні відбулася масштабна атака вірусом Petya внаслідок чого були вражені енергетичні компанії, українські банки, аеропорт «Бориспіль», аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен тощо. Подібного безпрецедентного масштабного вторгнення в сервери вітчизняних компаній Україна ще не знала. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу Petya склали близько 850 млн. доларів. При цьому заяви потерпілих компаній в кіберполіції про втрату даних часто залишалися без відповіді, адже знайти і притягнути до відповідальності зловмисника в даному випадку виявилося неможливо.

Ключовою кіберзагрозою для українців залишається соціальна інженерія. Оскільки люди набувають більше знань в цій області і знають про основні хитрощі шахраїв, останнім доводиться вигадувати нові схеми обману. На сьогодні в Україні актуальними є такі загрози: вішинг (дзвінки), смішинг (смс-повідомлення), «викрадення» сім-карти, фішинг (підроблені сайти), інтернет-шахраї.

Середня сума шахрайської операції, зробленої за допомогою соціальної інженерії, в 2019 р. склала 3400 грн., у той час як у 2018 р. вона дорівнювала 2333 грн. А середня сума операції, яку шахраї проводять із застосу-

ванням заміни сім-карти, склала в 2019 р. 6200 грн. (в 2018 – 3620 грн.).

Існує величезна кількість шахрайських схем, тому розглянемо найпоширеніші. Що стосується класифікації кіберзлочинів, то в Конвенції Ради Європи про кіберзлочинність, яка ратифікована і імплементована Верховною Радою України в українське законодавство починаючи з 11.10.2005 р., виділено чотири основних типи кіберзлочинів:

• правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем – незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями;

• правопорушення, пов'язані з комп'ютерами, – підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами;

• правопорушення, пов'язані з утриманням, – правопорушення, пов'язані з дитячою порнографією;

• правопорушення, пов'язані з порушенням авторських та суміжних прав.

Найпоширенішими видами кіберзлочинів є такі.

Скіммінг. Цілковитою несподіванкою для багатьох може стати безслідне зникнення коштів на банківській картці. Більшість людей відразу звертаються в банк для з'ясування, інші ж констатують факт списання лише через кілька тижнів або місяців. Найчастіше працівники банківських установ розводять руками і повідомляють, що кошти з вашої картки було знято в банкоматі. Скіммінг – це крадіжка даних карти за допомогою зчитувальних пристроїв. Найчастіше їх ставлять на банкоматах або POS-терміналах. При введенні в банкомат карти, закріплена поруч відеокамера дізнається PIN-код користувача і передає його злочинцям. Далі шахраї виготовляють дублікат карти, і знання PIN-коду, дозволяє знімати гроші з рахунку [4]. Для захисту від скіммінгу рекомендується використовувати картки лише в тих місцях, які заслуговують на довіру і охороняються. Необхідно обов'язково уважно оглянути банкомат на наявність підозрілих предметів. І найважливіше – ніколи не давати в руки свою карту і не повідомляти нікому пароль від неї (в т.ч. CVV-код). При введенні ПІН-коду необхідно прикривати його і вводити швидкими рухами, ніколи не втрачаючи при цьому пильність. Варто також підключити СМС-інформування для відстеження стану рахунку. Необхідно регулярно перевіряти роздруківки своїх банківських рахунків на предмет можливих шахрайств, а в разі будь-якої підозри терміново звертатися в банк і правоохоронні органи. Варто також зберегти в телефоні номер банку для термінового блокування карти.

Для захисту експерти рекомендують постійно контролювати картковий рахунок, не залишати персональні дані про себе і свою картку на інтернет-сайтах, регулярно оновлювати антивірусний захист, особливо з функцією безпечних платежів. Крім того, банкіри радять відкрити окрему платіжну карту для розрахунків в Інтернеті – віртуальна карта. Ефективною є також регулярна зміна паролів (раз на місяць, квартал). Для передачі конфіденційної інформації бажано використовувати захищені з'єднання. Безкоштовні або незахищені мережі Wi-Fi можуть спростити перехоплення даних користувача зловмисниками. Не передавати конфіденційні дані, будучи підключеними до таких мереж або ж використовувати персональний VPN-клієнт. Необхідно бути обережним при зберігання даних на хмарних дисках, з обережністю ставитись до того, хто має доступ до особистих файлів, і по можливості користуватися вбудованими інструментами захисту.

Кардінг – це шахрайські операції з кредитними картами (реквізитами кредитних карт), які не узгоджені з власником карти. Це може бути крадіжка або незаконне отримання кредитної картки, викопіювання даних карти для подальшої її підробки, викопіювання реквізитів картки для здійснення покупок через Інтернет без участі власника карти. У будь-якому випадку основною метою злочинців є отримання доступу до чужих грошових коштів. Для досягнення цієї мети зловмисники вигадують різні способи отримання необхідної інформації у неуважних і легковірних громадян. Одним з таких способів є фішинг.

Фішинг – один з різновидів соціальної інженерії, заснований на введенні в оману довірливих Інтернет-користувачів. Фішинг – це шахрайські дії, спрямовані на виманювання реквізитів картки у її власника. Як правило, власник кредитної картки сам добровільно

повідомляє шахраям потрібну інформацію. Якщо на електронну пошту, телефон або інші веб-сервіси користувача приходять повідомлення від імені банку, то необхідно бути більш уважним. За даними лабораторії комп'ютерної криміналістики Group-IB *фішинг* є найпопулярнішим видом кібершахрайства. Шахраї можуть: 1) підсунути підроблену інтернет-сторінку і спонукати користувача ввести свої конфіденційні дані: номер карти, CVV-значення, ПІН-код; 2) дзвонити жертвам як представники банку або будь-якої держструктури. Маючи дані, кіберзлодії отримують доступ до акаунтів і банківських рахунків [4]. Для захисту від фішингу виробники основних Інтернет-браузерів домовилися про те, що вони будуть застосовувати однакові способи інформування користувачів про те, що людина потрапила на підозрілий сайт, який може належати шахраям. Якщо користувачу телефонують, і вимагають швидко перевести гроші, то необхідно переконатися, що інформація, яку доводять до відома, правдива. Фішинг буває декількох видів:

СМС-фішинг, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну карту заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник карти отримав виграш, але потрібно заплатити за його доставку. Варіацій СМС-повідомлень дуже багато, тому потрібно бути особливо уважними та обережними, якщо ви отримуєте повідомлення.

Інтернет-фішинг – коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів тощо. На жаль, не всі уважно перевіряють назву сайту, вводячи дані кредитної картки, що на руку кібершахраям.

Вішинг – це практично той же фішинг, однак виманювання реквізитів картки здійснюється зловмисниками за допомогою телефонних дзвінків (шахраї часто представляються співробітниками банку і намагаються вивідати у власника картки ПІН-код або змусити зробити якісь дії зі своїм рахунком). Найчастіше використовується для заволодіння коштами на банківських рахунках жертв, хоча може також використовуватись для проникнення до інформаційних систем приватних або державних установ, крадіжки конфіденційної інформації.

Шімінг – модернізований різновид скіммінгу, це коли вмонтовують в сам картоприймач більш дрібні пристосування. Вони товщиною з людський волос, практично непримітні і розміщуються всередині картридера. Таким чином дані кредитки копіюються непомітно.

Онлайн-шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою, це фальшиві інтернет-аукціони, інтернет-магазини, сайти і телекомунікаційні засоби зв'язку.

Піратство – протиправне поширення об'єктів інтелектуальної власності в Інтернеті, належить до порушень у сфері інтелектуальної власності суб'єктів господарювання і є проявами недобросовісної конкуренції. М. Мельников визначає піратство як спосіб існування за рахунок інших осіб [8; с. 72].

Мальваре – шкідливий програмний засіб, шкідливе програмне забезпечення (англ. *Malware* — скорочення від **mal**icious — зловмисний і soft**ware** — програмне забезпечення) — програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем.

Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

Рефайлінг – незаконна підміна телефонного трафіку на локальний шляхом перенаправлення VoIP дзвінка з-за кордону в місцеву GSM мережу.

Програма-вимагач. Це тип шкідливого програмного забезпечення, який запобігає частковому або повному доступу до комп'ютера або файлів користувача, вимагаючи викуп за доступ до них. Вірус шифрує файли на комп'ютері або блокує доступ до нього. На екрані видно тільки картинку-блокер, і вимога провести платіж (найчастіше в криптовалюта як анонімне засіб платежу) для того, щоб розшифрувати або розблокувати систему.

У світі вже була ситуація, коли вірус-вимагач завдавав шкоди світовій спільноті.

WannaCry – це програма-вимагач, що працює під управлінням операційної системи MicrosoftWindows. Вірус робить дані марними за допомогою шифрування і закликає жертву виплатити викуп в біткоінах, обіцяючи видалити всі файли, якщо жертва не заплатить гроші. Крім того, вимагач діє як черв'як, заражаючи інші комп'ютери. Кіберзлочинці використовували цього вимагача в масовій кібер-атаці, яка була запущена 12 травня 2017 р. Зловмисна атака торкнулася понад 230 000 комп'ютерів у більше ніж 150 країнах, що завдало величезних економічних збитків, і призвело до блокування роботи багатьох організацій. Сбербанк, у свою чергу, повідомив, що зафіксував спроби хакерської атаки на свою інфраструктуру, проте всі вони були відбиті, тому що було своєчасно зафіксовано спроби проникнення [6].

Щоб не «підхопити» шкідливе програмне забезпечення, рекомендується ніколи не клікати по посиланнях на сайти банків або інших фінансових установ. Необхідно вводити адресу вручну, оскільки можна потрапити на підроблену сторінку. Бажано використовувати сервіси для доступу до інформації про новітні загрози і пристрої, які підтримуються офіційними представниками компаній [6].

Ще одним видом відомих вірусів, є *Троян* – це тип шкідливих програм, який здійснює різні несанкціоновані користувачем дії: збір інформації і її передачу зловмиснику, руйнування або зловмисну модифікацію, порушення працездатності комп'ютера. 14 червня 2019 р. компанія «Доктор Веб» повідомила, що її фахівці виявили троянця, який завантажує в GoogleChrome сумнівні веб-сайти, де користувачів підписують на повідомлення. Після активації підписки сайти починають відправляти численні, найчастіше помилкові, повідомлення: про надходження деяких фінансових бонусів або перекладів, про повідомлення, що надійшли в соцмережах, реклама гороскопів, товарів і послуг і новин.

Банківський троян активно набирає обороти. Кінцевою метою зловмисників є крадіжка грошових коштів з рахунків юридичних осіб. Крадіжка відбувається за допомогою підміни реквізитів в платіжних дорученнях [7]. 19 лютого «Kaspersky» повідомила, що за два місяці 2019 р. були зафіксовані спроби зараження. Банківські троянці Buhtrap і RTM націлені на малий і середній бізнес, зловмисників, насамперед, цікавлять бухгалтерія, а серед професійних сфер – інформаційні технології, переважно регіональні компанії.

Для захисту від даної загрози необхідно звернути особливу увагу фахівців з безпеки на захист робочих станцій співробітників фінансових відділів. Необхідно встановити останні оновлення та захисні рішення з модулем поведінкового детектування, заборонити запуск утиліт віддаленого адміністрування на таких комп'ютерах.

Існують шахрайські схеми, коли власник електронного гаманця надає доступ шахраям до своїх акаунтів і вони переводять десятки тисяч доларів на інший гаманець. Кіберполіція кваліфікує цей вид злочину, як шахрайство з використанням електронно-обчислювальної техніки. Крім того, на думку А. Гринчака, криптовалюта повинна бути легалізована і підконтрольна, адже з її допомогою здійснюється багато злочинів, таких як продаж наркотиків, зброї тощо.

Наведений перелік шахрайських дій не є винятковим, але, дотримуючись кілька простих правил, можна суттєво полегшити життя користувача, зберігши і нерви, і гроші: зберігати ПІН-код кредитки, паролі, дані для входу в Інтернет-банкінг в надійному місці, найкраще тримати їх у власній пам'яті; ні в якому разі не повідомляти третім особам паролі і реквізити карти; бути дуже обережними при здійсненні Інтернет-покупки і не надавати доступ стороннім особам до свого комп'ютера і (або) телефону.

Зазначені заходи не є панацеєю від усіх можливих загроз, які існують в Інтернеті, проте дозволяють значно мінімізувати ризики втрати важливої інформації.

Висновки. Отже, стрімкий розвиток цифрових технологій, незважаючи на позитивний вплив на всі сфери людського життя, викликав значне зростання і поширення кібершахрайств та кіберзлочинів. З упевненістю можна сказати, що кібершахрайства і кіберзлочини – це основні проблеми XXI ст., вирішення яких вимагає сучасних методів, активних, рішучих заходів і своєчасного нормативного реагування.

В нашій країні пріоритетними внутрішньополітичними напрямами її розвитку є

кібербезпека і протидія кіберзлочинності. Здійснення кібершахрайських операцій з банківськими картками та різними платіжними операціями має негативні наслідки для стабільності фінансової системи держави. Це проявляється у гальмуванні поширення безготівкової форми оплати, зниженні довіри населення до банків у частині зберігання коштів та кредитування. Недостатні знання про механізми кіберзлочинів ускладнюють процес визначення шахрайства. Вивчення ознак шахрайства, в першу чергу, необхідно для розробки більш дієвих засобів і методів захисту від даного виду злочину. Аналіз наслідків кібершахрайств дозволяє виявити слабкі місця в банківській системі та сприяє накопиченню інформації щодо способів, методів шахрайства, портретів шахраїв та їх жертв, формування ознак шахрайства. В результаті проведеного в статті аналізу виявлено, що збитки банків в результаті кібершахрайств зростають, не дивлячись на заходи служб безпеки. Клієнти та банки втрачають кошти завдяки різним шахрайським способам, серед яких найбільшої шкоди завдають методи соціальної інженерії. Для боротьби з такого роду шахрайствами запропоновано ряд заходів, реалізація яких потребує застосування методів Data Mining та розвинутих інформаційних технологій.

1. Не використовувати свій фінансовий номер в соціальних мережах, оголошеннях для контактів з клієнтами. Для цих цілей можна підключити послугу додаткового (віртуального) номера, який буде підключений до сім-карти і який можна використовувати для того, щоби дати номер малознайомим людям, розмістити оголошення в Інтернеті, зареєструвати номер для отримання СМС-розсилки і т.д.

2. Перейти на контрактне обслуговування у оператора. Це кращий спосіб захистити номер від шахраїв. Якщо ж користувач не готовий до цього, то хоча б ідентифікуватися у оператора (для цього можна в будь-який пункт обслуговування принести копію паспорта), зареєструватися в особистому кабінеті мобільного оператора і відключити можливість віддаленого перезапуску сім-карти.

3. Нікому не передавати СМС-коди від мобільного оператора і банку. Також не довіряти абсолютно всім повідомленням, які надходять нібито від банку користувача і містять будь-які інструкції. Адже в даний час номер і оператора, і банку можна підмінити. Тому якщо користувача просять перейти по посиланню /ввести отриманий код/, краще перестрахуватися і передзвонити за номером телефону банку, зазначеному на платіжній картці.

4. Негайно реагувати на ознаки заміни сім-карти. У разі отримання повідомлення від оператора про заміну сім-карти необхідно терміново поміняти пароль до інтернет-банкінгу і зателефонувати мобільному оператору, щоб зупинити перевипуск сім-карти. Якщо сім-карта перестала працювати, необхідно одразу звернутися до банку, щоб заблокувати картки. А також заблокувати акаунт в усіх фінансових сервісах, які прив'язані до номера користувача.

Це проблема не окремого громадянина, його сім'ї, і держави, а всього світового співтовариства, оскільки кібершахрайство в банківській сфері є потужним знаряддям глобальної фінансової кризи, що призводить до небезпечних наслідків, особливо в період зростання масових кіберплатежей при самоізоляції від вірусів. Тільки загальними зусиллями можна протистояти цій загрозі XXI століття.

Список літератури:

1. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ;
2. Аналитическая справка о состоянии преступности за период январь-декабрь 2019 год;
3. Российская газета, выпуск от 29.01.2020 года №17;
4. https://cyberleninka.ru/article/n/finansovoe-moshennichestvo-v-seti-internet/viewer (дата обращения 23.01.2020 г.)
5. https://pikabu.ru/story/skimming_chto_takoe_i_kakie_skhemyi_sushchestvuyut_18_5484907 (27.01.2020 г.)
6. http://www.tadviser.ru/index.php/Статья:WannaCry (дата обращения 05.02.2020 г.)
7. http://www.tadviser.ru/index.php/ Статья: Троян(дата обращения 05.02.2020 г)
8. Мельников М. Піратство як злочин у галузі авторського права та суміжних прав: погляд на про-блему / М. Мельников // Право України. – 2003. – No 4. – С. 72–75.
9. Федеровская Р. Социальная инженерия – это кибероружие №1 в 21 веке. Источник: https://www.ema.com.ua/contacts/

10. Черненко С.В., Авраменко Н.А. Автомобильно-дорожній інститут ГВУЗ «ДонНТУ»; «Закрытое, открытое и свободное программное обеспечение – основные различия и тенденции развития».– Таврический научный обозреватель, №12(17), 2016

11. Аванесян С. Р. Мошенничество как форма хищения // Право: теория и практика. — М.: Тезарус, 2007, № 4 (93). — С. 65-67;

12. Демедюк С. Пиратство, как и кибермошенничество – это преступления частного обвинения. - *"Интерфакс-Украина", 2018*

13. Кривошапова С. В., Литвин Е. А. Оценка и способы борьбы с мошенничеством с банковскими картами. Международный журнал прикладных и фундаментальных исследований. 2015. No 4. С. 116–120.

14. Fraud Digest 28.09.2017 [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем EMA. – 2017. URL: https://ema.com.ua/fraud-digest-28-09-2017.

15. Fraud Digest 28.07.2017 [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем EMA. – 2017. URL: https://ema.com.ua/fraud-digest-25-07-2017/.

16. Trend Report "Financial Cyber Threats Q1 2017» [Електронний ресурс] // The official site of the company "ElevenPaths". 2017. URL: https://www.elevenpaths.com/wpcontent/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf.

17. Статистика платежного мошенничества – итоги 2017-го года [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем EMA. 2017. URL: https://ema.com.ua/cyberfraud-ema-statistics-results-2017.

18. Некрасов В. Українці збагатили кібершахраїв на півмільярда: як не стати жертвою [Електронний ресурс]. FINANCE.UA. 2018. URL: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly-kibershahrayiv-na-pivmilyarda-yak-ne-staty-zhertvoyu.

19. Яровенко Г. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу [Електронний ресурс] / Г. М. Яровенко, А. І. Сковронська, М. М. Бояджян // Ефективна економіка. 2018. No 7. URL: http://www.economy.nayka.com.ua/?op=1&z=6453

Reference:

1. Uholovnyi kodeks Rossyiskoi Federatsyy ot 13.06.1996 №63-FZ;

2. Analytycheskaia spravka o sostoianyy prestupnosty za peryod yanvar-dekabr 2019 hod;

3. Rossyiskaia hazeta, vypusk ot 29.01.2020 hoda №17;

4. https://cyberleninka.ru/article/n/finansovoe-moshennichestvo-v-seti-internet/viewer (retrieved from 23.01.2020 h.)

5. https://pikabu.ru/story/skimming_chto_takoe_i_kakie_skhemyi_sushchestvuyut_18_5484907 (27.01.2020 h.)

6. http://www.tadviser.ru/index.php/Statia:WannaCry (data obrashchenyia 05.02.2020 h.)

7. http://www.tadviser.ru/index.php/ Statia: Troian(data obrashchenyia 05.02.2020 h)

8. Melnykov M. (2003) Piratstvo yak zlochyn u haluzi avtorskoho prava ta sumizhnykh prav: pohliad na problem. *Pravo Ukrainy*, No 4, pp. 72–75.

9. Federovskaia R. Sotsyalnaia ynzheneryia – eto kyberoruzhye №1 v 21 veke. URL: https://www.ema.com.ua/contacts/

10. Chernenko S.V., Avramenko N.A. (2016) Avtomobylno-dorozhnii instytut HVUZ «DonNTU»; «Zakrytoe, otkrytoe y svobodnoe prohrammnoe obespechenye – osnovnye razlychyia y tendentsyy razvytyia». *Tavrycheskyi nauchnyi obozrevatel*, №12 (17)

11. Avanesian S.R. (2007) Moshennychestvo kak forma khyshchenyia. *Pravo: teoryia y praktyka*. M.: Tezarus, № 4 (93), pp. 65-67;

12. Demediuk S. (2018) Pyratstvo, kak y kybermoshennychestvo – eto prestuplenyia chastnoho obvynenyia. *"Ynterfaks-Ukrayna"*.

13. Kryvoshapova S.V., Lytvyn E.A. (2015) Otsenka y sposoby borby s moshennychestvom s bankovskymy kartamy. Mezhdunarodnyi zhurnal prykladnykh y fundamentalnykh yssledovanyi, No 4, pp. 116–120.

14. Fraud Digest (28.09.2017) [Online]. Ukraynskaia mezhbankovskaia assotsyatsyia chlenov platezhnыkh sy-stem EMA. URL: https://ema.com.ua/fraud-digest-28-09-2017

15. Fraud Digest (28.07.2017) [Online]. Ukraynskaia mezhbankovskaia assotsyatsyia chlenov platezhnykh system EMA. URL: https://ema.com.ua/fraud-digest-25-07-2017/.

16. Trend Report "Financial Cyber Threats Q1 2017» (2017) [Online]. The official site of the company "ElevenPaths". URL: https://www.elevenpaths.com/wpcontent/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf.

17. Statystyka platezhnoho moshennychestva – ytohy 2017-ho hoda (2017) [Online]. Ukraynskaia mezhbankovskaia assotsyatsyia chlenov platezhnыkh system EMA. URL: https://ema.com.ua/cyberfraud-ema-statistics-results-2017.

18. Nekrasov V. (2018) Ukraintsi zbahatyly kibershakhraiv na pivmiliarda: yak ne staty zhertvoiu [Online]. FINANCE.UA. URL: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly-kibershahrayiv-na-pivmilyarda-yak-ne-staty-zhertvoyu.

19. Yarovenko H.M., Skovronska A.I., Boiadzhian M.M. (2018) Modeliuvannia vyiavlennia oznak kiberzahroz v bankakh iz vykorystanniam intelektualnoho analizu. *Efektyvna ekonomika*, [Online]. No 7. URL:http://www.economy.nayka.com.ua/?op=1&z=6453