УДК 378:004
ОРЛОВ Роман Русланович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-7755-3071

ВИЯВЛЕННЯ ПІДОЗРІЛИХ ФІНАНСОВИХ ОПЕРАЦІЙ, ЯКІ МОЖУТЬ БУТИ ПОВ'ЯЗАНІ З ВІДМИВАННЯМ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

Незважаючи на винахідливість кіберзлочинців і використання широкого інструментарію для схем легалізації незаконних доходів, представляється можливим розділити фінансові операції за рівнем ризику. Більш того, можливо також визначити сфери і послуги, які мають підвищений ризик і, відповідно, вимагають підвищеної уваги. Слід зазначити, що клієнтам, які встановлюють ділові відносини з банком або користуються банківськими послугами з використанням новітніх технологій без безпосереднього контакту з банком часто встановлюється більш високий рівень ризику відмивання злочинних доходів. Індикаторами підозрілості фінансових операцій зазначеної спрямованості для банківських установ побічно можуть бути наступні фактори:

– спроба входу з забороненої / нової IP-адреси;

– спроба використання прострочених первинних / робочих або старих ключів після сертифікації нових;

– використання для банківських операцій IP-адрес або імен користувачів, щодо яких попередній моніторинг виявив причетність до шахрайських операцій;

– проведення трансакції в нестандартний час або підключення до системи у вечірній час;

– незвичайні умови або складність операції: висока частота переказів протягом невеликого періоду часу, велика кількість різноманітних джерел походження коштів і платіжних методів (інструментів);

– особа не поінформована про характер діяльності юридичної особи, яку вона представляє;

– особа не може пояснити необхідність надання тієї чи іншої банківської послуги;

– залучення до проведення операцій осіб молодого віку і / або новостворених підприємств; проведення операцій з використанням загублених документів;

– відкриття рахунку, на який зараховуються кошти в результаті несанкціонованого списання незадовго до проведення таких операцій;

– спроби зняти кошти в день їх зарахування;

– спроби клієнта отримати дві або більше банківських карт, що не відповідає суті його діяльності або обороту.

Надзвичайно швидкий розвиток інформаційних і комп'ютерних технологій останнім часом призводить до стрімкого розвитку кіберзлочинності, тому особливої актуальності набувають питання попередження та протидії злочинам у кіберпросторі.

Удосконалення нормативно-правового забезпечення у сфері запобігання та протидії легалізації доходів, пов'язаних зі злочинами в сфері кіберзлочинності, можливо також за наступними напрямками: посилення відповідальності за злочини в сфері комп'ютерних та інформаційних технологій; введення обов'язкової ідентифікації при особистому контакті клієнтів, що користуються послугами дистанційного банківського обслуговування або електронних платіжних систем; визнання електронних документів та інших електронних даних в якості доказової бази при розслідуванні кіберзлочинів; регулювання питань, що стосуються юрисдикції, при наданні послуг через інтернет; зниження кількості анонімних платежів і

переказів грошових коштів; введення сертифікації електронних платіжних засобів; чітка регламентація механізмів взаємодії між клієнтом і банком, між банком відправника грошей і банком одержувача коштів у разі несанкціонованого списання коштів клієнта.

З метою попередження кіберзлочинів банківськими установами можуть впроваджуватися такі технічні та організаційні заходи: періодичний огляд банкоматів для виявлення незаконно встановлених пристроїв; впровадження для клієнтів банку карт з мікропроцесором (чіпом), як більш захищених від підробки; ведення «чорного» списку рахунків (ідентифікаційних кодів, IP-адрес) шахраїв для своєчасного блокування операцій; вимоги двохфакторної / двоканальної автентифікації; використання токенів для зберігання електронних цифрових підписів; обов'язкове інформування клієнтів про кожну проведену операцію; підтвердження платежу в телефонному режимі; генерація клієнтського ключа самим клієнтом, що робить неможливим вчинення неправомірних дій з боку працівників банку; прив'язка ключа клієнта до серійного номеру жорсткого диску / флеш-накопичувача, що унеможливлює копіювання ключів і доступ до сторінки клієнта за допомогою інших комп'ютерів; використання ряду логічних правил для типових / нетипових / підозрілих платежів в системі Клієнт-Банк; використання клієнтом окремого комп'ютера, який призначений тільки для системи Клієнт-Банк (інтернет-банкінг), з налаштованими мережевими фільтрами; статистичний аналіз трафіку (Netflow) для виявлення аномалій; введення лімітів на проведення операцій в мережі Інтернет.

Одержано 08.04.2021

УДК [004;343.6]

ПЕРЕЦЬ Олексій Вячеславович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-7755-3071

ВИКОРИСТАННЯ ВІРТУАЛЬНИХ БАНКІВСЬКИХ КАРТОК, ЯК ЗАХІД ПРОТИДІЇ ШАХРАЙСЬКИМ ДІЯМ

Завдяки зручності використання системи дистанційного банківського обслуговування (далі – ДБО) активно застосовуються майже всіма верствами населення як в Україні, так і за кордоном нашої держави. Пластикова банківська карта – платіжний інструмент, який набагато зручніше і, головне, вигідніше готівки. Але у пластикових карток є і недоліки: можливість механічного пошкодження або втрати, наприклад внаслідок крадіжки. Карту завжди можна перевипустити або заблокувати, але це зайвий клопіт. Потрібно бути обережним, розраховуючись нею на касах або знімаючи готівку в банкоматах. Різними способами шахраї при цьому можуть спробувати дізнатися реквізити картки: номер, термін дії, CVV-код, пін-код.

Пластику є альтернатива – віртуальні картки, які позбавлені цих недоліків. Це банківські карти, у яких є всі ті ж реквізити, що і у звичайних. Додавши таку карту в смартфон (технології ApplePay і GooglePay), користувач ДБО значно збільшує ступінь безпеки розрахунків за допомогою свого платіжного інструменту, що є досить актуальним у період всесвітньої пандемії, коли різко зросла кількість шахрайств, які вчиняють злочини з використанням платіжних інструментів та онлайн-сервісів у мережі Інтернет.

Віртуальну картку не потрібно носити з собою і тому неможливо втратити. У магазині ніхто не зможе підгледіти її реквізити, адже в процесі оплати держатель платіжного інструменту підносить до терміналу не карту, а смартфон. Але головне призначення віртуальних