imf.org/external/pubs/ft/wp/2003/wp03147.pdf.

4. Atish R. Ghosh, Jonathan D. Ostry, and Mahvash S. Qureshi. Exchange Rate Management and Crisis Susceptibility: A Reassessment. IMF Working Paper. 2014. — [Електронний ресурс]. — Режим доступу: https://www.imf.org/external/pubs/ft/wp/2014/wp1411.pdf.

5. Rodrik D. Disequilibrium Exchange Rates as Industrialization Policy // Journal of Development Economics. — 1986. — Vol. 23. Is.1. — P. 89—106.

6. Aghion P., Bacchetta Ph., Ranciere R., Rogoff K. Exchange Rate Volatility and Productivity Growth: the Role of Financial Development. NBER Working Paper No. 12117. 2006. — [Електронний ресурс]. — Режим доступу: http://www.nber.org/papers/w12117.pdf.

7. Polterovich V., Popov V. Accumulation of foreign exchange reserves and long-term growth. New Economic School. 2003. — [Електронний ресурс]. — Режим доступу: http://mpra.ub.uni-muenchen.de/20069/1/MPRA_paper_20069.pdf.

8. Bhagwati J.N. Rethinking Trade Strategy, in P.L. Johnand V. Kallab (eds.). Development Strategies Reconsidered. New Brunswick: Transaction Books. — 1986. — p. 23.

9. Balassa B. Intra-Industry Specialization in a Multi-Industry Framework. — Economic Journal. — 1987. — № 97. — P. 923—939.

10. Bhagwati J.N. Export-Promoting Trade Strategy: Issues and Evidence. The World Bank Research Observer. — 1988. — Vol. 3. — № 1.— P. 27-57.

11. Frank, C.R. Jr., K.S. Kim, and L.E. Westphal. Foreign Trade Regimes and Economic Development: South Korea. National Bureau of Economic Research, New York. 1975. — [Електронний ресурс]. — Режим доступу: https://www3.nd.edu/~kellogg/publications/workingpapers/WPS/166.pdf.

12. Мадиярова Д. М. Стратегия формирования внешнеэкономической деятельности. — Алматы: Экономика, 1999. — 184 с. — (Kazakhstan source).

13. Шаров О. Монетарні та валютні війни як інструмент економічної політики // Вісник Національного банку України. — 2013. —- № 10. — С. 12—19. — (Ukrainian source).

14. Harvie Ch., Lee H. H. Export Led Industrialisation and Growth — Korea's Economic Miracle 1962-89. Working paper 03-01, Department of Economics, University of Wollongong, 2003. — [Електронний ресурс]. — Режим доступу: http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1066&context=commwkpapers.

15. Hsueh L. M., Hsu C.K., Perkins D. H. Industrialization and the State: the Changing Role of the Taiwan Government in the Economy, 1945—1998, Cambridge, Mass: Harvard. 2001.

16. Economic Survey of Singapore, various years and Yearbook of Statistics, Singapore, various issues. — [Електронний ресурс]. — Режим доступу: http://www.mti.gov.sg/ResearchRoom/Pages/Economic-Surveys-ESS.aspx.

Безпека/

Кіберзлочинність — загроза банківській системі

Cibercrime — a threat to a banking system

В Університеті банківської справи Національного банку України відбувся круглий стіл на тему "Кібербезпека: міфи чи реальність?", організований УБС НБУ, Національним аерокосмічним університетом ім. М.Жуковського (м. Харків) і громадською організацією "ІТ Альянс" за підтримки профільного комітету Верховної Ради України та Державної служби спеціального зв'язку і захисту інформації України. В засіданні взяли участь також представники Ліги протидії кібертероризму та інформаційним війнам, Міністерства внутрішніх справ, СБУ, банків, організацій, які відповідають за захист від загроз кіберзлочинності, юристи.

On 11 February 2015, in the University of Banking of the National Bank of Ukraine, there was held the round table meeting on "Cyber Security: Myth or Reality", which was organized by the NBU University of Banking, M. Zhukovskyi National Aerospace University (City of Kharkiv), and public organization "IT Alliance" with the support of the profile committee of the Verkhovna Rada of Ukraine and State Service of Special Communication and Information Protection of Ukraine. Representatives of the League of Cyberterrorism and Information War Counteraction, Ministry of Internal Affairs of Ukraine, Security Service of Ukraine, banks, lawyers, and organizations responsible for the protection against cyber threats also took part in the meeting.

Питання кібербезпеки завжди були дуже актуальними в різних сферах людської діяльності в усьому світі, оскільки шкідливі програми, запроваджені в мережі державних і комерційних структур, банків, конкуруючих фірм та різних суб'єктів, а також інші види кіберзлочинності з кожним роком завдають усе більшої шкоди. Її обсяги обчислюються мільярдами доларів, а прибутки від такої діяльності знаходяться на рівні прибутків від торгівлі зброєю чи наркотиками. Більше того, останнім часом з'явився особливий вид програм, які за своїми функціональними характеристиками належать до кіберзброї, і за їх створенням стоять навіть державні структури. Тому гарантування кібербезпеки є одним із головних аспектів національної безпеки кожної країни. Це безпосередньо стосується й України, особливо в нинішній період, коли кібератаки можуть бути серйозною зброєю в руках терористів та російських окупантів на сході нашої країни і завдавати не меншої шкоди, ніж

військова зброя. Тож круглий стіл, присвячений цій гострій проблемі, викликав велику зацікавленість в усіх його учасників, безпосередньо пов'язаних із гарантуванням кібербезпеки в різних сферах діяльності.

Відкриваючи зібрання, ректор Університету банківської справи НБУ **Тамара Смовженко** підкреслила важливість цієї проблеми для банківської системи і зазначила, що саме тому їхній ВНЗ став співорганізатором круглого столу. Останнім часом у банківській сфері активізувалися такі злочинні явища, як шахрайство з платіжними картками через Інтернет, а також фішинг, тобто виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказування або обміну валюти, інтернет-магазинів. Шахраї вдаються до різних хитрощів, які змушують користувачів самостійно розкривати конфіденційні дані, наприклад, надсилаючи електронні листи з пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на вебсайт в Інтернеті, зовні абсолютно схожий на дизайн відомих ресурсів. Також почастішали кібератаки на електронні банківські системи та офіційні інтернет-сайти й програми. Для таких злочинів використовується й соціальна інженерія, яку в наш час активно експлуатують в Інтернеті з метою отримання закритої інформації чи такої, яка має велику цінність. Її зловмисник одержує, наприклад, шляхом збору інформації про службовців об'єкта атаки за допомогою звичайного телефонного дзвінка або шляхом проникнення на їхні інтернет-сайти. "Всі кіберзлочини призводять до значних фінансових втрат, витоку важливої інформації, а в кінцевому результаті й до погіршення репутації банків і втрати довіри населення до банківської системи, якої нині так бракує, – підсумувала Тамара Смовженко. – Тому сьогодні дуже важливими є питання, винесені на розгляд учасників круглого столу, зокрема, яку модель управління кібербезпекою вибрати, які основні напрями її створення, як урегулювати взаємовідносини між державними органами і приватними особами та структурами, як протидіяти кібершпигунству та закріпити це на законодавчому рівні".

Саме питанням законодавчого врегулювання цієї проблеми й приділили основну увагу представники одного з головних "бійців" на цьому "кібер-фронті" – Державної служби спеціального зв'язку і захисту інформації України. Її голова **Володимир Звєрєв** у своєму вітальному слові зазначив, що в нашій країні досі не розроблено державної стратегії та належної законодавчої бази кібербезпеки, яка б ураховувала міжнародний досвід у цій сфері, а також національні особливості. Він закликав об'єднати під егідою Ради національної безпеки та оборони зусилля всіх причетних до забезпечення захисту від такої небезпеки, включаючи силові структури та банківську спільноту (адже саме банки виступили піонерами електронного підпису), а також громадянське суспільство.

Стурбованість недосконалістю законодавчого врегулювання цієї сфери розділив і заступник начальника відділу адміністрації Держспецзв'язку **Павло Смолянінов**. Він поінформував учасників зібрання про перипетії створення закону, який сприяв би гарантуванню кібербезпеки в нашій країні. Ще з 2012 року проект Закону "Про основні засади забезпечення кібербезпеки України", розроблений їхньою службою за завданням РНБО, не може прийняти парламент через постійні "недоробки". До того ж логічно було б, щоб Кабінет Міністрів водночас прийняв Стратегію національної безпеки, яка враховувала б усі аспекти кібербезпеки. Поки що обидва основоположні документи перебувають на стадії доопрацювання.

Чимало пунктів законопроекту Держспецзв'язку викликали жваве обговорення та зауваження присутніх, зокрема представника Міністерства внутрішніх справ **Володимира Шеломенцева** та президента київського відділення Міжнародної асоціації з розробки методологій та стандартів у галузі управління, аудиту і безпеки інформаційних технологій ISACA **Олексія Янковського**.

Кореспондент "Вісника Національного банку України" попросив деяких учасників круглого столу розповісти про проблеми кібербезпеки у банківському секторі. Заступник керівника служби безпеки ПАТ "КБ "Приватбанк" **Михайло Фролов**, зокрема, зазначив, що актуальність цієї проблеми в умовах нинішньої війни значно загострилася. Адже в регіонах, де відбуваються військові дії, функціонування банківських установ і правоохоронних органів значно утруднене, а в багатьох містах і повністю припинене. Не працюють банкомати, термінали самообслуговування, пропадає мобільний зв'язок та Інтернет. Це змушує різного роду злочинців, у тому числі й хакерів, мігрувати в інші регіони, де немає війни, а також удосконалювати методи інтернет-шахрайства та психологічного впливу на клієнтів банків. І хоча в цілому зростання кількості злочинних дій у банківській сфері не спостерігається, ситуація контрольована, та суспільна небезпека таких злочинів залишається дуже великою. "Актуальність посилення заходів кібербезпеки в банківській сфері пов'язана також і з тим, що банківські технології масово переміщуються у сферу безконтактних платежів у вигляді дистанційного банківського обслуговування, – зазначив Михайло Фролов. – Клієнти мають можливість здійснювати платежі й отримувати грошові перекази в мережі Інтернет без використання платіжної картки, шляхом обміну SMS-повідомленнями з банком і з використанням інших сучасних, зокрема й інтернет-технологій. З одного боку, це

Господарі зібрання (в центрі зліва направо) проректор Університету банківської справи НБУ Анжела Кузнєцова та ректор УБС Тамара Смовженко радо приймали гостей.

полегшує клієнту доступ до банківських послуг, а з другого – робить його вразливішим до різного роду кіберзлочинів. Тому кожен банк повинен приділяти захисту своїх клієнтів, а також власної бази велику увагу, як це робиться в нашому банку, де застосовують спеціальні антивірусні та інші програми, новітні технології. Ми розуміємо, що наш банк є одним із системних, тож його захищеність важлива для стійкості всієї банківської системи України і водночас є складовою частиною системи національної безпеки нашої держави. Ми значно посилили свою кібербезпеку в воєнний період, щоб не дати ворогові можливості підірвати валютно-фінансову систему держави. Також міжнародні платіжні системи та Національний

банк України не допускають використання банківських продуктів, які не відповідають вимогам кібербезпеки. Хоча є випадки, коли клієнти банків усе ж стають жертвами шахрайства при використанні платіжних технологій, у чому вони фактично самі винні. Аналіз таких інцидентів свідчить, що громадяни в процесі телефонних переговорів із шахраями повідомляють їм недопустимі до розголошування персональні дані й банківські реквізити. Тому слід нагадати, що не потрібно розголошувати дані про ПІН-код платіжної картки, термін її дії, тризначний код CVV2/CVC2, нанесений на її тильній стороні, який використовується для перевірки достовірності платіжної карти при оплаті через Інтернет і інших видах операцій. Нікому не можна повідомляти дані, які надійшли з банку в SMS-повідомленнях, а тим більше під впливом сторонніх осіб уводити отримані в них конфігурації цифр або літер у банкоматах, терміналах чи в мобільних додатках смартфонів. Неприпустимо переходити за посиланнями, які надходять на смартфони клієнтів, адже хитрість кібершахраїв полягає в тому, що вони надсилають їх із телефонів, які викликають довіру, а насправді поширюються через інші, заражені вірусами, смартфони. Це призводить до вірусного зараження смартфонів клієнтів і доступу шахраїв до банківських рахунків. Особливо важливим є використання клієнтами банків на своїх комп'ютерах ліцензійного програмного забезпечення – як операційних систем, так і антивірусних програм. Купівля вживаного комп'ютера зі встановленими програмами загрожує тим, що вони можуть бути заражені вірусами і скомпрометувати сервіси дистанційного банківського обслуговування клієнта".

Байдужих до обговорюваних питань не було.

Михайло Фролов підкреслив, що нормативна база Національного банку України достатня для того, щоб протидіяти кіберзагрозам у банківському секторі, оскільки вона побудована відповідно до законодавства України, яке постійно вдосконалюється, і згідно з ним удосконалюється нормативна база НБУ. ПАТ "КБ "Приватбанк" у співпраці з Незалежною асоціацією банків України бере участь в обговоренні законопроектів з актуальних проблем удосконалення законодавства й нормативної бази, в тому числі з питань гарантування кібербезпеки. Багато їхніх спільних пропозицій прийнято й імплементовано в законодавство, над іншими завданнями робота триває. Проте дуже актуальними, на думку Михайла Фролова, залишаються соціально-психологічні проблеми, оскільки банки використовують технології, які відповідають міжнародним вимогам із кібербезпеки й захисту персональних даних клієнтів і їхніх активів, а шахраї користуються необізнаністю клієнтів щодо гарантування безпеки своїх банківських рахунків і завдають їм збитків. Представник Приватбанку вважає також, що слід посилити кримінальну відповідальність за злочини у сфері інформаційних технологій, адже нинішнє віднесення їх до категорії нетяжких утруднює роботу правоохоронних органів із викривання, оскільки не дає змоги проводити весь комплекс оперативно-розшукових заходів. Для ефективної протидії кіберзлочинності необхідно також забезпечувати повну взаємодію банківського співтовариства, громадських організацій, засобів масової інформації, вчених та правоохоронців щодо вироблення спільних рішень у сфері гарантування кібербезпеки.

Виступають представники Держспецзв'язку України.

Керівник команди реагування на комп'ютерні надзвичайні події України CERT-UA **Іван Соколов** повідомив, що їхніми фахівцями в рамках виявлення та ліквідації кіберзагроз в українському сегменті мережі Інтернет було зафіксовано численні випадки розсилання електронних листів начебто від імені державних органів України (Міндоходів, Державної реєстраційної служби, НАК "Нафтогаз України" та інших). Під час відкриття файла відбувалась експлуатація вразливості в програмному забезпеченні MS Word, а комп'ютер уражався шкідливою програмою ("банківським трояном"). Таким чином ці комп'ютери автоматично "долучалися" до складу бот-мережі, яка використовувалася для викрадення грошових коштів із систем дистанційного банківського обслуговування за посередництва шкідливої програми. У квітні 2014 року фахівці центру змогли ідентифікувати фактичне місцезнаходження сервера управління бот-мережею та на деякий час припинити її діяльність. Було з'ясовано, що за період із січня до квітня 2014 року ця бот-мережа налічувала 46 234 уражених шкідливими програмами комп'ютерів (ботів), а в базі даних сервера управління бот-мережею було близько 40 000 000 одиниць скомпрометованих даних (сертифікатів, логінів/паролів, зображень з екрана). Здебільшого жертвами цих злочинців були наші співвітчизники, адже понад 86% уражених комп'ютерів знаходились у межах українського Інтернету і належали бухгалтерам або керівникам українських підприємств. Зважаючи на те, що загроза стосувалася безпосередньо фінансового сектору, CERT-UA спільно з Українською міжбанківською асоціацією членів платіжних систем ЄМА розпочали спільний проект щодо ідентифікації скомпрометованих засобів та інформування відповідних кредитно-фінансових установ з метою подальшого вжиття необхідних заходів. Ця взаємодія полягала в передаванні за координації ЄМА початкової інформації щодо скомпрометованих комп'ютерів до відповідальних фахівців банків (переважно служб безпеки),

Великий круглий стіл ледве вмістив усіх запрошених на обговорення гострих проблем.

які, в свою чергу, визначали клієнтів, чиї комп'ютери були уражені шкідливими програмами, та проводили профілактично-превентивну роботу. Орієнтовна сума грошових коштів, які могли бути викрадені з рахунків 1 657 "скомпрометованих" клієнтів, становила приблизно 43 567 000 грн. Такий формат взаємодії державного та приватного секторів позитивно вплинув на зменшення рівня можливого шахрайства в системах дистанційного банківського обслуговування. Між Державним центром захисту інформаційно-телекомунікаційних систем Держспецзв'язку, на базі якого функціонує CERT-UA, та Українською міжбанківською асоціацією членів платіжних систем ЄМА було підписано Меморандум про співпрацю, який дає змогу протидіяти викраденню грошових коштів із рахунків фізичних та юридичних осіб України, організованого з використанням банківських троянських програм.

"Слід зазначити, що враження шкідливими програмами відбувається шляхом надсилання зловмисником на електронну пошту жертви (бухгалтера або керівника) листа, який складається таким чином, щоб отримувач без вагань відкрив його (тобто застосовуються методи соціальної інженерії), а також містить посилання на шкідливу програму або додаток зі шкідливою програмою, – попередив Іван Соколов. – Після проведеного аналізу інциденту фахівцями CERT-UA було встановлено, що реалізації загрози також сприяє нехтування керівниками підприємств і відповідальними співробітниками елементарними правилами інформаційної безпеки. Вони використовують неліцензійне програмне забезпечення (як операційні системи, так і офісні програми); не перевіряють джерела надходження інформації (наприклад, шляхом дзвінка відправнику та перевірки факту відправки ним електронного листа); некоректно використовують носії ключової інформації (наприклад, замість підключення USB-токена тільки для здійснення трансакції підключають його до комп'ютера на весь робочий день); використовують комп'ютери, на яких встановлено системи "Клієнт-банк", для ігор, доступу до Інтернету, перегляду новин, користування соціальними мережами тощо, тоді як такий комп'ютер має бути якомога більше ізольованим. Тож ми просимо відповідальних керівників і співробітників підприємств, установ та організацій України в разі отримання підозрілого електронного листа або виявлення ознак нештатного поводження комп'ютера інформувати CERT-UA та банк, послугами якого вони користуються. Також рекомендуємо розглядати електронну пошту як основне джерело загроз інформаційній безпеці та вжити всіх необхідних заходів (наприклад, змінити електронну адресу на нову та поширювати її лише довіреним колегам/контрагентам, а в разі отримання електронного листа перевіряти факт його надходження за допомогою відправника та ін.).

Голова правління Ліги протидії кібертероризму та інформаційним війнам **Юрій Когут** вважає, що крадіжка грошей просто з банківських рахунків чи з використанням викрадених особистих даних – не єдиний мотив, який криється за зломом систем захисту. Такі кібератаки часто можуть бути спрямовані на підрив репутації фінансової установи. DDoS-атаки також використовують для відволікання уваги служб безпеки банків від шахрайських схем і зламів облікових записів. Атаки часто проводять на веб-сайти великих банків, у яких немає належного захисту. За даними експертів, нині чотири із п'яти банківських ресурсів є вразливими, а три з чотирьох атак здійснюються через незахищені додатки, причому одна маленька вразливість може становити загрозу для цілої фінансової організації. Останнім часом кіберзлочинці активно використовують мобільні технології. Більшість мобільних шкідливих додатків орієнтована передусім на крадіжку грошей – нині явно простежується "банківська" спрямованість розвитку мобільних злочинів. Творці вірусів стежать за розвитком сервісів мобільного банкінгу і за успішного інфікування смартфона відразу перевіряють, чи прив'язаний він до банківської карти.

"Згідно з даними за 2013 рік Україна входить до трійки світових лідерів за кількістю заражених мобільних пристроїв, – зазначив Юрій Когут. – Її частка у світовому показнику таких пристроїв становить 5.9%. У 2012 році з банківських рахунків у нашій країні було викрадено 11.4 млн. грн. (в основному при проведенні грошових розрахунків у системі інтернет-банкінгу чи на сайтах торгово-роздрібних мереж). За даними МВС України, за 2012 рік порушено 139 кримінальних справ щодо протиправного списання 116 млн. грн. за допомогою систем "Клієнт – банк". За інформацією НБУ, за цей же рік кількість банків, із рахунків яких було викрадено кошти, збільшилася з 35 до 57. Для ефективного захисту від кіберзлочинності, на мою думку, необхідно вдосконалити і доповнити законодавчу базу та національні стандарти у сфері кібербезпеки, а також розробляти програми, які гарантують кібербезпеку фінансових структур і громадян, та системи управління інформаційною безпекою і протидії кібертероризму. Слід впроваджувати передовий досвід зарубіжних країн у цій сфері. Регулярно проводити інвентаризацію та аналіз вразливості систем захисту від кіберзлочинів, а також аудит ІТ-процесів, який дасть змогу точно оцінити стан ІТ-системи, виявити ризики та отримати рекомендації щодо їх усунення. Постійно контролювати персональну техніку співробітників фінустанов, які працюють у корпоративній мережі з конфіденційною інформацією. Їхній низький рівень комп'ютерної грамотності та незнання можливих варіантів кіберзагроз є однією з причин зараження комп'ютерів вірусами та витоку інформації. Тому варто постійно проводити навчання персоналу. Зважаючи на те, що кількість кібератак зростатиме, слід приділити увагу превентивним способам захисту банків".

Учасники круглого столу внесли пропозиції щодо вироблення елементів концепції розвитку кібербезпеки в Україні, розгляду можливості створення спеціального національного науково-освітнього центру та робочої групи з розробки декларації чи меморандуму з розвитку кібербезпеки, які б лягли в основу законодавчих ініціатив. Крім того, наголошували виступаючі, необхідно розвивати внутрішній ринок розробок із кібербезпеки всіх структур, зокрема й банківських, а не орієнтуватися на аутсорсинг. Особливу увагу слід приділити стандартизації безпеки, а також створити перелік понять і класифікатор, використовуючи міжнародний досвід. Зважаючи на важливість питання та велику кількість проблем із кібербезпеки, було запропоновано частіше розглядати їх у якомога ширшому колі фахівців.

❐

Микола Пацера,
Mykola Patsera,
"Вісник Національного банку України".
"Herald of the National Bank of Ukraine".

Фото ***Владислава Негребецького.***
Photos by ***Vladyslav Nehrebetskyi .***

ДО ВІДОМА ДЕРЖАТЕЛІВ ПЛАТІЖНИХ КАРТ

Останнім часом на адресу Національного банку України надходить багато звернень громадян стосовно здійснення невстановленими особами несанкціонованих дій чи шахрайських операцій із використанням платіжних карток або їхніх реквізитів. Найчастіше увагу злочинців привертають громадяни, які розміщують оголошення про купівлю чи продаж товарів на сайтах інтернет-аукціонів та безкоштовних оголошень у мережі Інтернет. Видаючи себе за потенційних покупців або співробітників банку (служби клієнтської підтримки, служби безпеки тощо), зловмисники вивідують персональні дані держателів платіжних карток. У зв'язку з цим НБУ застерігає громадян не повідомляти третім особам власні персональні дані чи реквізити платіжної картки (її номер, ПІН-код, CVV2, термін дії картки, а також код, який надходить на мобільний телефон для підтвердження переказу чи платежу) та інші дані, потрібні для здійснення переказів чи платежів. Під час здійснення операцій із використанням платіжних карток (у тому числі мобільних платежів) Національний банк рекомендує дотримуватися правил безпеки, встановлених банком-емітентом, а також рекомендацій, розроблених НБУ та розміщених у розділі "Фінансова грамотність/Фінансові питання та поради"/"Рекомендації держателям платіжних карток щодо їх використання" на сторінці Офіційного інтернет-представництва Національного банку України. Витяг із цього документа пропонуємо нашим читачам.

РЕКОМЕНДАЦІЇ
держателям платіжних карток щодо їх використання

Загальні рекомендації. Не розголошуйте ПІН стороннім особам, у тому числі й родичам, знайомим, працівникам банку, касирам та особам, які намагаються допомогти вам під час використання платіжної картки. Його необхідно запам'ятати або зберігати окремо від платіжної картки в недоступному для сторонніх осіб місці. Не передавайте платіжну картку для використання іншими особами. Якщо на платіжній картці нанесене прізвище та ім'я фізичної особи, то тільки вона має право її використовувати. Не розголошуйте персональні дані або інформацію про платіжну картку (в тому числі ПІН) на вимогу будь-яких сторонніх осіб, у тому числі й працівників банку. У разі виникнення такої ситуації зателефонуйте до банку-емітента, який видав платіжну картку, і повідомте про цей факт. Його телефон зазначено на зворотному боці картки. Також потрібно завжди мати при собі контактні телефони банку-емітента, номер платіжної картки в записнику, мобільному телефоні тощо, але не разом із записом про ПІН. Для запобігання незаконним операціям із використанням платіжної картки та зняття з неї коштів доцільно встановити добовий ліміт на суму та кількість операцій із застосуванням платіжної картки й одночасно підключити електронну послугу оповіщення про проведені операції (наприклад, у вигляді SMS або іншим способом). Не слід відповідати на електронні листи, в яких від імені банку пропонується надати персональні дані, а також відкривати сторінки в мережі Інтернет (сайти/портали), зазначені в листах (включаючи офіційну сторінку банку в мережі Інтернет), оскільки це можуть бути сторінки-двійники, через які здійснюють незаконні операції з використанням даних вашої платіжної картки.

Здійснення операцій через банкомат. Слід здійснювати операції з використанням платіжних карток через банкомати, встановлені в безпечних місцях (наприклад, в установах, банках, великих торговельних комплексах, готелях, аеропортах тощо). Перед використанням банкомата огляньте його на наявність додаткових приладів, які не відповідають конструкції та розташовані в місці набору ПІНу чи в місці, призначеному для приймання карток. Набирайте ПІН таким чином, щоб особи, які перебувають поруч, не змогли його побачити, наприклад, прикривайте клавіатуру рукою. Якщо банкомат працює некоректно (довгий час перебуває в режимі очікування, мимоволі перезавантажується), відмовтесь від його послуг. Не слід проводити ніяких дій за підказками третіх осіб, а також приймати від них допомогу під час здійснення операцій через банкомат.

Здійснення безготівкових розрахунків. Розрахунки з використанням платіжної картки мають виконуватися тільки у вашій присутності. Під час використання платіжної картки для оплати товарів або послуг продавець/касир може вимагати від держателя платіжної картки ввести ПІН. Перед його набором слід переконатися, що треті особи не зможуть його побачити. Якщо під час спроби оплати товарів або послуг із використанням платіжної картки не вдалося здійснити операцію, то необхідно зберігати один примірник виданої терміналом квитанції для перевірки відсутності зазначеної операції у виписці про рух коштів за картковим рахунком.

Виконання операцій через мережу Інтернет. Не використовуйте ПІН під час замовлення товарів або послуг через мережу Інтернет, а також за телефоном/факсом. Не повідомляйте інформацію про платіжну картку або картковий рахунок через мережу Інтернет, наприклад ПІН, паролі доступу до рахунків, термін дії платіжної картки, кредитні ліміти, персональні дані тощо.

Для оплати товарів (послуг) через мережу Інтернет краще використовувати окрему платіжну картку (так звану "віртуальну картку") з граничним лімітом, передбачену лише для цього, та за якою неможливо здійснювати операції в торговельній мережі чи зняття готівки. Слід користуватися послугами лише відомих і перевірених інтернет-магазинів. Переконайтесь у правильності зазначення адреси сторінок у мережі Інтернет (сайтів/порталів), до яких підключаєтесь і через які збираєтеся оплатити товар, оскільки схожі адреси можуть використовуватися для здійснення незаконних або сумнівних операцій із використанням персональних даних платіжної картки. Оплачувати товари чи послуги, придбані через мережу Інтернет, варто лише зі свого комп'ютера з метою збереження конфіденційності персональних даних та/або інформації про картковий рахунок. Якщо це робилося через чужий комп'ютер, то варто переконатися, що персональні дані та інша інформація не збереглася. Слід встановити на свій комп'ютер антивірусне програмне забезпечення і регулярно оновлювати його та інші програмні продукти (операційну систему, прикладні програми), щоб захиститись від проникнення неліцензійного програмного забезпечення (вірусів).