ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ДИСТАНЦІЙНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ

ORGANIZATION OF DATA PROTECTION IN REMOTE BANKING SYSTEMS

УДК 336.7

Тищенко О.І.
к.е.н., доцент кафедри фінансів і банківської справи,
Східноукраїнський національний університет імені Володимира Даля

У статті розглянуті організаційні аспекти захисту інформації в системах дистанційного банківського обслуговування. Досліджено сучасний стан систем ДБО та ступінь їх уразливості для зовнішніх загроз. Виявлено основні передумови виникнення загроз, урахування яких дозволить знизити негативні наслідки при їх виникненні. Визначені три найсуттєвіші типи загроз, що існують для систем електронного банкінгу та доцільні засоби захисту інформації в них.

Ключові слова: *дистанційне банківське обслуговування (ДБО), загрози, уразливості, системи захисту, троян, вірус, банкінг.*

В статье рассмотрены организационные аспекты защиты информации в системах дистанционного банковского обслуживания. Исследовано современное состояние систем ДБО и степень их уязвимости для внешних угроз. Выявлены основные предпосылки возникновения угроз, учет которых позволит снизить негативные последствия при их возникновении. Определены три существенные типы угроз, существующих для систем электронного банкинга и целесообразные средства защиты информации в них.

Ключевые слова: *дистанционное банковское обслуживание (ДБО), угрозы, уязвимости, системы защиты, троян, вирус, банкинг.*

The organizational aspects of information security in remote banking services systems are considered in the article. The present state of the DB systems and the degree of their vulnerability to external threats are investigated. The basic preconditions of occurrence of threats are revealed, the account of which will allow reducing negative consequences at their occurrence. Three most important types of threats that exist for e-banking systems and the appropriate means (areas) for protecting information in them are identified.

Key words: *remote banking services (RBS), threats, vulnerabilities, security systems, Trojan, virus, banking.*

Постановка проблеми. Однією з основних особливостей сучасної вітчизняної банківської системи є використання комп'ютерних і телекомунікаційних технологій у процесі надання послуг клієнтів. Це дозволяє значно розширити асортимент послуг, підвищити їхню якість, швидкість надання, скоротити обсяги готівкового обороту та залучити нових клієнтів. Використання Інтернет-простору в банківському просторі перетворилося з конкурентної переваги на конкурентну необхідність. Банки не лише мають застосовувати вже існуючі інформаційні технології, але й шукати нові засоби надання банківських послуг, активно використовуючи можливості інтернет-мережі. Одним з найважливіших завдань банків при наданні дистанційних послуг є забезпечення найвищого рівня безпеки систем електронного банкінгу, що дозволить мінімізувати ризики несанкціонованого доступу до інформації та рахунків клієнтів.

Аналіз останніх досліджень і публікацій. Дослідженням теоретичних основ використання систем дистанційного обслуговування присвячені праці вітчизняних й закордонних вчених: В. Кравця, О. Гаврилової, О. Вовчака, О. Чуба, Л. Одегової, А. Новицького та ін. Питання інформаційної безпеки фінансово-кредитних установ широко розглянуті в роботах А. Володина, А. Козлова, А. Лукацького, А. Мамонтова, Н. Романова, А Румянцева. Основний акцент у роботах зроблено на висвітлення теоретичних основ, визначення переваг та недоліків систем дистанційного обслуговування. Втім, проблемам забезпечення безпеки і захисту інформації при використанні віддалених сервісів не приділено достатньої уваги. Внаслідок цього виникають різного роду шахрайства, пов'язані з незаконним доступом до інформації клієнтів та використанням їхніх коштів.

Тому питання визначення основних типів загроз, що виникають у системах віддаленого доступу та пошук сучасних шляхів захисту інформації в них потребують подальшого дослідження.

Постановка завдання. Метою статті є визначення типів загроз й ступеня їх впливу на системи дистанційного банківського обслуговування та пошук доцільних засобів захисту інформації в них.

Виклад основного матеріалу дослідження. Дистанційне банківське обслуговування – це загальний термін для технології, яка використовується з метою надання банківських послуг клієнтам на основі розпоряджень, переданих ними на відстані (без обов'язкового візиту до банку), за допомогою різноманітних засобів самообслуговування, найчастіше з використанням комп'ютерних і телефонних мереж [1].

Одним з нагальних питань, пов'язаних з наданням банками послуг з дистанційного обслуговування клієнтів є забезпечення максимально можливого рівня безпеки систем електронного банкінгу. Ступінь популярності системи дистанційного обслуговування обумовлює ступінь зацікавленості до неї шахраїв. Серед поширених поміж клієнтами видів дистанційного обслуговування (інтернет-банкінг; мобільний банкінг; SMS – банкінг; відео-банкінг; PC-банкінг) найбільш вразливими до несанкціонованого втручання є системи мобільного банкінгу та інтернет-банкінгу. Існуючі проблеми безпеки віддалених сервісів є актуальними не тільки для банків, але і для їх клієнтів.

Отже, захисту потребує не лише банківська частина системи, що забезпечує дистанційні послуги, а й технічні та програмні засоби клієнта, за допомогою яких клієнт здійснює доступ до послуг [2, с. 138]. Утім, за оцінкою фахівців у галузі забезпечення безпеки, високий рівень організації процесів у банківській системі, наявність постійного контролю з боку головного регулятора дозволяє значно знизити рівень небезпеки в порівнянні з небанківськими установами.

Основним джерелом загроз для систем ДБО є Інтернет, що пов'язано з неможливістю здійснення контролю цієї мережі з боку банків. При цьому в разі використання банківських онлайн-додатків реалізація загроз призводить до серйозних наслідків, включаючи розкрадання грошових коштів, несанкціонований доступ до персональних даних і банківської таємниці, а також втрати репутації для бізнесу. Проведені фахівцями дослідження продовж останніх років підтверджують цей факт.

Так за результатами дослідження, проведеного на початку липня 2017 року Positive Technologies, було виявлено, що частка фінансових додатків, що містять критично небезпечні уразливості в 2016 році знизилася на 8%, а частка уразливостей середнього рівня ризику -18%. Проте, загальний рівень ризиків виявлених уразливостей став значно вищий. Найбільш поширеними виявилися недоліки механізмів ідентифікації, автентифікації і авторизації. Більшість систем онлайн-банкінгу (71%) мають недоліки в реалізації двофакторної автентифікації, понад 30% додатків містять уразливості, що дозволяють вкрасти гроші, а в 27% додатках зловмисник має можливість отримати доступ до відомостей, що становлять банківську таємницю.

Дослідження показали, що найбільша частка уразливостей (майже в два рази більше) виявлена в продуктивних системах, ніж у системах, що знаходяться в розробці. До того ж ступінь ризику у фінансових програмах, розроблених вендорами, в середньому в два рази більше, ніж у тих, що банки розробляють самостійно. Отже, основний рівень загроз криється у системах, що вже функціонують та розроблені спеціалізованими фірмами.

Окрім недосконалостей самих систем дистанційного банківського обслуговування, на думку спеціалістів «Альфа Страхування», причиною різкого зростання кількості шахрайських дій є недостатня поінформованість населення в частині правильного використання нових Інтернет-технологій.

Велика кількість випадків несанкціонованого зняття відбувається з вини самих власників карток, так як вони самі надають доступ третім особам до інформації, призначеної для особистого користування, не розуміючи можливих наслідків. До того ж з кожним роком вік власників банківських карт зростає, а їх знання в області сучасних банківських технологій залишаються на досить низькому рівні [3].

Отже задля запобігання подальшого зростання кількості, частоти та потужності загроз при роботі в системі ДБО слід ураховувати низку факторів, що їх обумовлюють.

Так можна виділити декілька передумов для розвитку загроз при використанні систем дистанційного банківського обслуговування.

1) перша передумова – кількісне зростання користувачів послуг. Збільшення кількості платних послуг, що надаються банками за допомогою ДБО, від оплати мобільного телефона до оплати кредитів і штрафів, веде до зростання кількості користувачів системи ДБО, що збільшує можливості для виникнення усякого роду загроз.

2) до другої передумови належить розширення якості та кількості послуг, що надаються. Активне використання для здійснення банківських операцій користувачами різного роду мобільних пристроїв має як позитивні, так і негативні наслідки. З одного боку це дозволяє банкам мінімізувати витрати на офіси, знижуючи витрати на обслуговування користувачів. З іншого – зростає ступінь загрози несанкціонованого входу до системи, оскільки взаємодія з банком відбувається в Інтернеті, і якщо серверна частина є добре захищеною (адже основна частина операцій ведеться в локальних мережах банку, не виходячи за межі організації або локальних офісів), то клієнтська частина є майже не захищеною.

3) третя передумова – використання мобільних платформ для роботи з ДБО. Існуючі програми при використанні їх на сучасних мобільних пристроях споживають занадто багато ресурсів, тому виявляються менш ефективними в порівнянні з повноцінними комп'ютерами, оскільки мають обмежені параметри. Отже, виникає потреба в новому підході до захисту, який полягав би не в постійному моніторингу нових загроз і захисту саме від них, а в проактивному захисті самої інфраструктури пристроїв, що працюють з банками. Такий підхід, крім оптимального споживання ресурсів і відсутності необхідності в регулярних оновленнях, має додатковий плюс – забезпечення цілісності системи,захищає не тільки від епідеміологічних загроз, а й від «націлених» атак і загроз нульового дня, які не виявляються антивірусами на момент появи.

4) до четвертої передумови слід віднести недостатній на сьогоднішній день захист всього спектру пристроїв і платформ. Для забезпечення в майбутньому інтересів своїх клієнтів рівень безпеки систем дистанційного обслуговування має вийти на новий виток розвитку. Задля зменшення збитків від несанкціонованого втручання необхідне впровадження в пов'язані з ДБО системи, нових технологій проактивного захисту.

Таким чином, урахування визначених вище факторів дозволить зменшити наслідки від неба-

жаного та незаконного втручання в роботу систем ДБО та підвищити рівень їхньої безпеки як для банків, так і для клієнтів.

Системи електронного банкінгу постійно піддаються атакам шахраїв. Умовно можна виділити три основні типи загроз, що існують для систем дистанційного банківського обслуговування (рис. 1).

Розглянемо особливості впливу на систему ДБО кожного з типів загроз.

1. «Шпигун у браузері». Сутність даного типу загроз полягає у використанні певної групи троянських програм, таких як Zeus, Silon, Torpig, Yaludle тощо, які дозволяють контролювати браузери. На сьогоднішній день вони є одним з найпоширеніших типів загроз. У той момент, коли в браузері відкривається вікно для проведення платежу або оплати товару, троянська програма перехоплює управління браузером і від імені користувача проводить власний платіж на користь власника шпигунської програми. Найбільш часто такі шкідливі програмні засоби проникають на комп'ютери користувачів через невідомі вразливості в браузері, інтегруються в нього і працюють разом з ним при перегляді Інтернет-сторінок [4].

Історія використання троянських програм розпочалася у 2007 році, коли з'явився просунутий фінансовий троян під назвою Zbot (Zeus). Він був створений Російським письменником вірусів під ніком Slavik/Monstr і продавався на чорному ринку за тисячі доларів. Два роки по тому було розроблено ще один троян під назвою Spyeye, автором якого був дехто Gribodemon. Ціна нового продукту була більш доступною і становила 700 доларів США. Отже, троянські програми стали об'єктом «чорного» ринку.

У подальшому ринок троянських програм дещо змінився. У 2011 році вихідний код Zeus був вкрадений і викладений у відкритий доступ, що призвело до різкого обвалу його ціни та появі безлічі версій Zeus, включаючи допрацьовані Ice IX і Citadel, які стали боротися за ринок. У цей період було створено альтернативні варіанти Zeus, призначені для приватного використання, як, наприклад, знаменитий Gameover, який з'явився в липні 2011 р. Через місяць після публікації вихідного коду Zeus дехто Xylibox шляхом злому отримав доступ до вихідного коду Spyeye, що призвело до аналогічного обвалу ціни. На даний момент будь-яка інформація про подальшу розробку двох цих троянів їх творцями відсутня. Багато нинішніх фінансових троянів запозичили прийоми і архітектуру саме Spyeye і Zeus.

За результатами проведеного експертами аналізу більше 1000 конфігураційних файлів восьми троянських програм, спрямованих проти банківських систем було визначено таке. Стратегії атак, що здійснювалися за допомогою троянських програм, варіюються від простого перенаправлення користувачів до складних веб-Інжектів (Web-injects), здатних автоматично здійснювати транзакції в фоновому режимі. Дослідження показали, що майже 95% атак приходилося саме на фінансові установи всіх типів – від комерційних банків до кредитних кооперативів. Отже, основна мета троянських програм – це атака на цілі, що здатні приносити прибуток. Також у спробах максимізувати прибуток зловмисники починають атакувати популярні і відповідно прибуткові мережі фінансових транзакцій такі, як американська Automated Clearing House, а також європейська Single Euro Payments Area (SEPA) [3].

2. До другого типу загроз, що виникають в системі ДБО, належить «шпигун у мережі». Сутність даної загрози полягає у тому, що шахраї можуть перехоплювати сеанс роботи користувачів із системою оплати, наприклад, за допомогою перенаправлення веб-запитів на власний сайт або зміни роботи DNS-системи. Злочинці можуть перехопити важливу інформацію, за допомогою якої в подальшому можна буде проводити власні фінансові транзакції, або просто втручаються в існуючий сеанс обміну даними, модифікуючи його на свій розсуд. При цьому шахраям не обов'язково вбудовувати своє шкідливе програмне забезпечення в операційну систему конкретного користувача – їм достатньо атакувати провайдера, а потім маніпулювати сеансами користувачів [4].

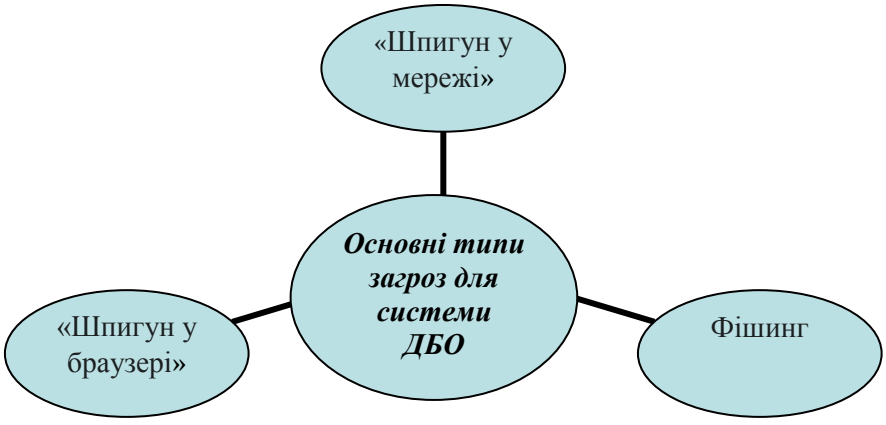

Рис. 1. Основні типи загроз для системи дистанційного банківського обслуговування

3. До третього типу загроз належить «фішинг». Фішинг – це один з різновидів соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки. Метою цього виду інтернет-шахрайства є отримання доступу до ідентифікаційних даних користувачів – логінів і паролів. Сутність фішингу полягає

у створенні шахраями спеціального сайту, який дуже схожий за оформленням на банківський або торговий ресурс, і за допомогою різних прийомів (наприклад, спаму) заманюють на нього відвідувачів. Користувачі, не розуміючи, що знаходяться на сторонньому сайті, передають йому свою конфіденційну інформацію, яку надалі шахраї можуть використовувати для здійснення покупок або переказів. Більшість серверів, на яких розміщувалися фішингові сторінки, були зареєстровані на територіях США, Великобританії, Німеччини, Росії та Індії [5, с. 140].

Основними ознаками наявності фішингових атак є:

• надходження повідомлень на електронну пошту з невідомих адрес (не внесених до адресної книги);

• наявність у фішингових повідомленнях орфографічних помилок та/або прохання перейти за посиланням для уникнення від можливих проблем;

• заклик у шахрайських повідомленнях до необхідності введення паролю, особистих даних, даних про фінансові рахунки [6].

Результати досліджень, оприлюднених компанією PhishMe, станом на березень 2016 року свідчать, що 93% метою всіх фішингових листів було намагання заразити комп'ютер жертви шкідливими програмами криптографічного здирництва. Їхня головна ідея полягала у вимаганні грошей у жертви за розшифровку даних, що попередньо були зашифровані на жорсткому диску. Також серед різновидів фішингових атак були відзначені часті випадки підлаштування вмісту листів під певну категорію жертв (за їхнім фахом) та із включенням певних елементів особистої інформації (звернення до жертви за ім'ям та інше) [7]. Отже, даний вид загроз має досить значні негативні наслідки для системи дистанційного обслуговування та її клієнтів.

Досвід робіт із забезпечення безпеки систем дистанційного обслуговування показує, що стійкий стан системи, за якого відображаються всі можливі атаки зловмисників, реалізувати дуже важко. Виходом може бути вироблення додаткових і дієвих вимог щодо забезпечення безпеки дистанційних розрахунків і правильна реалізація цих вимог.

Серед основних засобів захисту систем дистанційного банківського обслуговування можна виділити наступні (рис. 2).

1) перехід на технології двох факторної автентифікації зі зберіганням ключової інформації у нерозгорнутому вигляді на e-Token або в смарт-карті. Застосування даної технології дозволить знизити ризики несанкціонованого доступу до особистих кабінетів користувачів, у яких, як правило, містяться персональні дані, інформація про рахунки і одержувачів платежів. Крім того, за наявності призначеного для користувача доступу зловмисник отримує можливість розвивати атаку не тільки в напрямі обходу авторизації і проведення транзакції від імені користувача, але і з метою

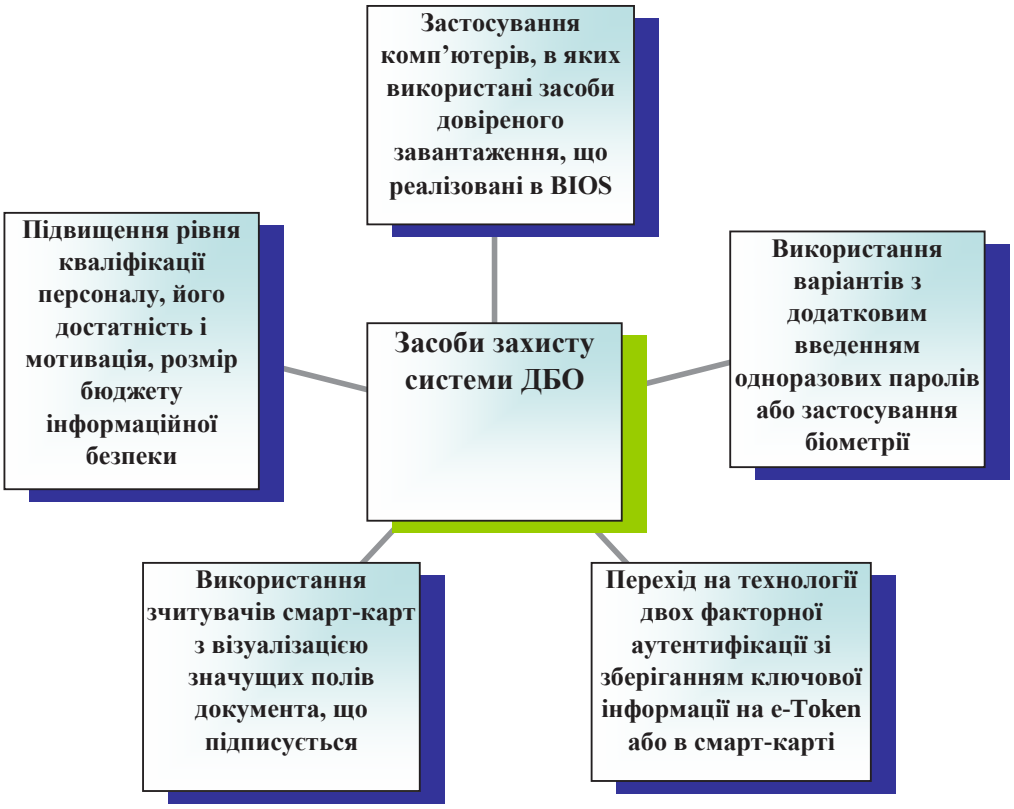

Рис. 2. Засоби захисту системи дистанційного банківського обслуговування

виявлення і експлуатації уразливостей серверних компонентів системи (наприклад, уразливостей типу «Впровадження зовнішніх сутностей XML» і «Впровадження операторів SQL») [8].

2) використання варіантів з додатковим уведенням одноразових паролів або застосування біометрії. Використання одноразових паролів при проведенні транзакцій дозволяє підвищити безпеку системи в частині здійснення несанкціонованого доступу. Ця система може бути реалізована по-різному: у вигляді OTP-токенів або додатків, що функціонують на мобільному телефоні, з використанням SMS-каналу, спеціальних SIM-карт або захищених SD-карт, встановлених у мобільний пристрій. Прийнятним варіантом додаткового фактору автентифікації є біометрія. Вона може використовуватися, як засіб доступу до токену, якщо зчитувач смарт-карти оснащений ще й біометричним датчиком. Застосування біометрії робить перехоплення пароля до USB-ключа набагато більш проблематичним.

3) застосування комп'ютерів, у яких використані засоби довіреного завантаження, що реалізовані у BIOS (наприклад, фірми Kraftway). Це дозволить виключити вплив вірусів, що завантажуються до запуску системи, і вірусів, що модифікує сам BIOS (реалізованих у вигляді гипервізора у BIOS – такий вірус неможливо виявити засобами, що запускаються після нього).

4) використання зчитувачів смарт-карт з візуалізацією значущих полів документа, що підписується. Платіжний документ після формування передається по USB у зчитувач і на його екран виводяться значущі поля документа. Накладення підпису ініціюється натисканням кнопки на пристрої і відбувається в його ізольованому середовищі, а вже підписаний документ передається назад в комп'ютер. Таким чином, виключається можливість атак з підміною документа і з захопленням управління комп'ютером.

5) підвищення рівня кваліфікації персоналу, його достатність і мотивація, а також розмір бюджету інформаційної безпеки. Недостатня кваліфікація і мотивація ведуть до таких проблем, як встановлення паролю за замовчуванням на мережевому обладнанні, наявність єдиного паролю на різних ресурсах, віддалений доступ в обхід загальних правил і політик. Обмеженість бюджету фінансових організацій, дефіцит фахівців часто ведуть до затягування процесу впровадження повного комплексу необхідних технологій і уповільнення реакції на виникаючі нові загрози.

Отже, щоб ефективно протистояти діям шахраїв при використанні дистанційних сервісів, необхідно не тільки мати систему безпеки, але ще й налаштувати цю систему на можливі атаки зловмисників.

Необхідно враховувати, що різні уразливості системи призводять до різних наслідків. Украй важливо проводити роботи з максимального виявлення уразливостей систем дистанційного обслуговування і максимальним чином протидіяти порушенню безпечного функціонування цих систем. Для цього банківські установи активно використовують спеціальні програми захисту інформації.

На сьогодні вже розроблено та активно використовується певна кількість програм захисту інформації в системах дистанційного обслуговування. До найбільш відомих розробників систем захисту інформації можна віднести такі.

1. Компанія ESET – міжнародний розробник антивірусного програмного забезпечення і рішень в області комп'ютерної безпеки для корпоративних і домашніх користувачів [9].

2. Компанія «Лабораторія Касперського» – найбільш відомий в Європі виробник систем захисту від шкідливих програм, спаму та хакерських атак і найбільша антивірусна компанія в Європі. Є одним з провідних світових виробників програмних рішень для забезпечення інформаційної безпеки для кінцевих користувачів [10].

3. Компанія «Доктор Веб» – російський розробник засобів інформаційної безпеки під маркою Dr.Web®. Основними споживачами продуктів компанії є домашні користувачі з усіх регіонів світу, підприємства різного рівня й системоутворюючі корпорації [11].

4. Компанія КРИПТО-ПРО – розробник засобів криптографічного захисту інформації, займає лідируюче положення з поширення засобів криптографічного захисту інформації та електронного цифрового підпису [12].

Проте, яка б система захисту не існувала, слід намагатися знизити схильність банків та їх клієнтів до неминучих ризиків. Це складний і довгий шлях, який вимагає системного підходу, але тільки завдяки цьому можна домогтися бажаних результатів.

Висновки з проведеного дослідження. У сучасних умовах банки активно використовують засоби комп'ютерних та телекомунікаційних технологій задля створення комфортних умов обслуговування наявних клієнтів та залучення додаткових. Розвиток системи дистанційного обслуговування, окрім позитивних моментів містить безліч загроз як для банків так і клієнтів, основним джерелом яких є Інтернет, що пов'язано з неможливістю здійснення контролю цієї мережі з боку банків. Тому одним з нагальних питань, пов'язаних з наданням банками послуг з дистанційного обслуговування клієнтів є забезпечення максимально можливого рівня безпеки систем електронного банкінгу.

За результатами дослідження було виділено декілька передумов для розвитку загроз при використанні систем ДБО, урахування яких дозволить знизити можливі наслідки при їх настанні. При цьому було визначено три основні типи загроз, що існують для систем дистанційного банківського обслуговування, кожний з яких має свої особли-

вості та різний ступінь фінансових втрат для банків і клієнтів. Було зазначено, що для забезпечення стійкого розвитку систем електронного банкінгу необхідно застосовувати сучасні засоби безпеки.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Дистанционное банковское обслуживание [Электронный ресурс]. – Режим доступа: http://dengibiz.ru/raznoe/distancionnoe-bankovskoe-obsluzhivanie/.

2. Захарченко О.М. Безпека системи дистанційного банківського обслуговування та напрями її забезпечення / О.М. Захарченко // Проблеми і перспективи розвитку фінансової системи України в умовах формування нового світового фінансово-економічного порядку: Матеріали Міжн. наук.-практ. інтернет-конф. 1–6 жовтня 2014 р. – Полтава: ПУЕТ, 2014. – С. 138–142.

3. Безопасная система ДБО [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/

4. Крамар О.І. Безпека систем дистанційного банківського обслуговування / О.І. Крамар [Електронний ресурс]. – Режим доступу: http://libfor.com/index.php?newsid=2636

5. Ріпак А.Д. Використання Trusteer Rapport для безпеки систем дистанційного банківського обслуговування / А.Д. Ріпак // Новітні інформаційні технології в економічній діяльності: зб. тез. VI Всеукраїнської наук.-практ. конференції, 26 березня 2014 р.: в 1 ч. / Нац. унів. ДПС України. – Ірпінь, 2014. – С. 140–142.

6. Фішинг: що це таке і як себе убезпечити? [Електронний ресурс]. – Режим доступу: http://zillya.ua/fishing-shcho-tse-take-i-yak-sebe-ubezpechiti

7. Поняття «фішинг» [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/

8. Статистика уязвимостей систем дистанционного банковского обслуживания (2011–2012) [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Analitika-DBO-rus.pdf

9. Компанія ESET [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/ESET

10. Лабораторія Касперського [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Лабораторія_Касперського

11. Доктор Веб, ліцензійне програмне забезпечення організацій в Softline [Електронний ресурс]. – Режим доступу: http://antyseptyky.com/doktor-veb-litsenzijne-programne-zabezpechennya-organizatsij-v-softline/

12. «КриптоПро» О компании [Электронный ресурс]. – Режим доступа: // https://www.cryptopro.ru/about

REFERENCES:

1. Distantsionnoe bankovskoe obsluzhivanie [Elektronnyy resurs]. – Rezhim dostupa: http://dengibiz.ru/raznoe/distancionnoe-bankovskoe-obsluzhivanie/.

2. Zakharchenko O.M. Bezpeka systemy dystancijnogho bankivsjkogho obslughovuvannja ta naprjamy jiji zabezpechennja / O.M. Zakharchenko // Problemy i perspektyvy rozvytku finansovoji systemy Ukrajiny v umovakh formuvannja novogho svitovogho finansovo-ekonomichnogho porjadku: Materialy Mizhn. nauk.-prakt. internet-konf. 1–6 zhovtnja 2014 r. – Poltava: PUET, 2014. – S. 138–142.

3. Bezopasnaya sistema DBO [Elektronnyy resurs]. – Rezhim dostupa: http://www.tadviser.ru/index.php/

4. Kramar O.I. Bezpeka system dystancijnogho bankivsjkogho obslughovuvannja / O.I. Kramar [Elektronnyj resurs]. – Rezhym dostupu: http://libfor.com/index.php?newsid=2636

5. Ripak A.D. Vykorystannja Trusteer Rapport dlja bezpeky system dystancijnogho bankivsjkogho obslughovuvannja / A.D. Ripak // Novitni informacijni tekhnologhiji v ekonomichnij dijaljnosti: zb. tez. VI Vseukrajinsjkoji nauk.- prakt. konferenciji, 26 bereznja 2014 r.: v 1 ch. / Nac. univ. DPS Ukrajiny. – Irpinj, 2014. – S. 140–142.

6. Fishyngh: shho ce take i jak sebe ubezpechyty? [Elektronnyj resurs]. – Rezhym dostupu: http://zillya.ua/fishing-shcho-tse-take-i-yak-sebe-ubezpechiti

7. Ponjattja «fishyngh» [Elektronnyj resurs]. – Rezhym dostupu: https://uk.wikipedia.org/wiki/

8. Statistika uyazvimostey sistem distantsionnogo bankovskogo obsluzhivaniya (2011–2012) [Elektronnyy resurs]. – Rezhim dostupa: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Analitika-DBO-rus.pdf

9. Kompanija ESET [Elektronnyj resurs]. – Rezhym dostupu: https://uk.wikipedia.org/wiki/ESET

10. Laboratorija Kaspersjkogho [Elektronnyj resurs]. – Rezhym dostupu: https://uk.wikipedia.org/wiki/Лабораторія_Касперського

11. Doktor Veb, licenzijne proghramne zabezpechennja orghanizacij v Softline [Elektronnyj resurs]. – Rezhym dostupu: http://antyseptyky.com/doktor-veb-litsenzijne-programne-zabezpechennya-organizatsij-v-softline/

12. KriptoPro o kompanii [Elektronnyy resurs]. – Rezhim dostupa: https://www.cryptopro.ru/about

Tishchenko H.I.
Candidate of Economic Sciences,
Senior Lecturer at Department of Finance and Banking,
Volodymyr Dahl East Ukrainian National University

ORGANIZATION OF DATA PROTECTION IN REMOTE BANKING SYSTEMS

The organizational aspects of information security in electronic banking systems are considered in the article. The characteristic features of a modern domestic banking system are the use of computer and telecommunication technologies in the process of customer service. Using the Internet space in the banking space is not only a competitive advantage and a competitive necessity. One of the most important tasks of banks in providing remote services is to ensure the highest level of security of electronic banking systems. This will minimize the risks of unauthorized access to information and customer accounts. Problems of security and information protection when using remote services in the scientific literature are not considered sufficiently carefully. Consequences are the occurrence of various types of fraud involving illegal access to customer information and the use of their funds. The purpose of the article is to determine types of threats and the degree of their impact on remote banking services and to find the appropriate means of protecting information in them. The degree of popularity of the system of remote servicing determines the degree of interest in it fraudsters. The most vulnerable to unauthorized interference are mobile banking and internet banking systems. In order to prevent further increase in the quantity, frequency, and power of threats when working in the system of distance service, it is necessary to take into account a number of factors that determine them. In the work, a number of prerequisites for the emergence of threats with the use of remote banking services are identified. The current state of the systems of remote banking services and the degree of their vulnerability to external threats are researched in this work. Three most important types of threats that exist for e-banking systems are identified: «browser spy», «net spy» and phishing. In order to ensure a stable state of electronic banking systems, which will reduce the consequences of possible attacks by intruders, it is necessary to apply certain security measures. A number of such means of protection of remote banking services are identified in the work.