АВТОМАТИЗАЦІЯ

УДК 004:336.71

Р.О. Баглай, асп.
Київський національний торговельно-економічний університет, м. Київ, Україна
E-mail: romanbaglai@gmail.com

Механізми управління безпекою банківських інформаційних систем

В статті проведено аналіз сучасних тенденцій щодо проблем та механізмів управління безпекою банківських інформаційних систем, на основі хмарних технологій. Розглянуто підходи до управління безпекою ІТ банківських установ для мінімізації загроз, в тому числі породжених хмарними технологіями. Запропоновано сучасний підхід до побудови механізмів забезпечення безпеки ІТ через запровадження довіреної третьої сторони, застосування єдиної авторизації в інформаційних системах (від англ. Single sign-on, надалі SSO) та федеративних сценаріїв доступу. Розглянуто майбутній обсяг покриття проблем щодо ІТ безпеки та рішення постачальників відповідного програмного забезпечення, які базуються на хмарних сервісах
архітектура ІТ банку, хмарниі технології Trusted Third Party, Single sign-on, Identity as a Service

Р.О. Баглай, асп.
Киевский национальный торгово-экономический университет, г. Киев, Украина

Механизмы управления безопасностью банковских информационных систем

В статье проведен анализ современных тенденций относительно проблем и маханизмов управляния безопасностью банковских информационных систем на основе облачных технологий. Рассмотрены современные подходы по управлению безпасностью ИТ банковских учреждений для минимизации угроз, в том числе пораженных облачными технологиями. Предложен современный подход построения систем с механизмами обеспечения безопасности ИТ, через внедрение доверенной третьей стороны, применение единой авторизации в информационных системах (от англ. Single Sign-on) и федеративних сценариев доступа. Рассмотрен будующий охват покрытия проблем относительно ИТ безопасности и решения от поставщиков соответствующего программного обеспечения, которое основано на облачных сервисах.
архитектура ИТ банка, облачные технологии, Trusted Third Party, Single sign-on, Identity as a Service

Постановка проблеми. При дослідженні питань безпеки інформаційних систем виникає низка нештатних ризиків та викликів переміщення до хмари, які значно знижують ефективність традиційних механізмів захисту. Зокрема, що хмарне середовище унеможливлює концепцію захисту від загроз шляхом встановлення периметра безпеки. Периметровий захист – це сукупність фізичних та програмних політик безпеки, яка забезпечує захист від віддаленої зловмисної діяльності на умовному периметрі. Традиційно вважається, що будь-який зв'язок з системами або організаціями поза межами організації надає можливість для неавторизованих осіб (персоналу або процесів) отримати доступ або втрутитись в інформаційні процеси. За цим статичним підходом до захисту встановлюються умовні кордони, в межах яких розгорнуті політики безпеки для захисту інформаційних систем. У моделі хмарних обчислень периметр стає нечітким, зводячи нанівець ефективність цієї концепції захисту [1 с. 583].

© Р.О. Баглай, 2018

З огляду на вищезазначене для забезпечення сильної авторизації і як наслідок конфіденційності, цілісності та доступності банківських інформаційних систем (надалі ІС), ІС на основі хмарних технологій, слід використовувати інші механізми захисту, зокрема, – механізми єдиної авторизації в інформаційних системах з підтримкою федеративних сценаріїв. Крім значного підвищення рівня безпеки хмарних сервісів ці інноваційні технології також дозволяють підвищити ефективність банківських операційних процесів.

Аналіз останніх досліджень і публікацій. Проблеми безпеки застосування хмарних технологій в різних соціально-економічних сферах досліджували вітчизняні та зарубіжні науковці Зіссіс Д., Леккас Д., Бобиль В.В., Корольов В.Ю., Кондратьєв А.А. та інші. У публікаціях Бобиль В.В [2,3] враховано специфіку банківського сектору, але не міститься конкретних рекомендацій щодо механізмів забезпечення конфіденційності, цілісності, доступності даних банківських інформаційних систем (надалі – ІС). Праці інших науковців зокрема Корольов В.Ю. [4], Кондратьєв А.А. [5] не враховують, в повній мірі, специфіку забезпечення безпеки ІТ для банківських установ. Проте, особливості діяльності банківських установ, яка регулюється нормативно-правовими актами Національного банку України, а в контексті євроінтеграції, – Європейський центральним банком, Базельським комітетом з банківського нагляду, Радою стандартів безпеки платіжних карт, Товариством всесвітніх міжбанківських фінансових телекомунікацій, та іншими міжнародними установами, зумовлюють специфіку організації системи забезпечення безпеки ІТ, що визначає необхідність вивчення механізмів захисту від загроз безпеки ІТ для банків.

Постановка завдання. Метою даної статті є дослідження перспективних технологій захисту від загроз безпеки ІТ, що дозволить здійснити впровадження хмарних технологій для банківських ІС, для скорочення витрат та підвищення ефективності підтримки ІТ для бізнес-процесів банку.

Виклад основного матеріалу. З огляду на те, що встановлення фізичного периметру безпеки за умов розгортання банківської ІС на хмарній інфраструктурі неможливе, слід застосовувати інші механізми захисту. За таких обставин, в межах хмари, ми пропонуємо визначити довірену третю сторону (надалі ДТС). Для забезпечення довіри та впровадження політики використання криптографії, гарантування конфіденційності, цілісності та автентичності даних та зв'язків, потрібно вирішити конкретні ризики та убезпечити вразливі місця безпеки.

У цьому контексті механізми SSO є незамінними, оскільки вони забезпечують засоби сильної автентифікації на різних фізичних ресурсах. У середовищі SSO користувачеві не потрібно повторно вводити паролі для доступу до ресурсів через мережу. Замість цього користувач авторизується, коли використовує пароль, смарт-картку або інший механізм автентифікації і тим самим отримує доступ до декількох ресурсів на різних пристроях. Обсяг довіри до ДТС визначається потребами щодо надання сервісів безпеки, які всеціло охоплюють процеси служб безпеки, що масштабуються, працюють на основі стандартів в різних доменах, географічних районах і враховують специфіку банківського сектора.

Принцип роботи SSO. В основі концепції SSO лежить принцип «Користувач вводить пароль лише раз за сесію», застосований при розробці протоколу Kerberos вченими Массачусетського технологічного інституту у восьмидесятих роках минулого століття. Kerberos – це вбудований протокол автентифікації Active Directory, що використовується мережами Windows. Таким чином, користувачі мають доступ до всіх сервісів, на які вони авторизовані, без потреби заново вводити пароль під час сесії. Ця властивість також відома як SSO.

Для забезпечення конфіденційності, цілісності та автентичності SSO спирається на інфраструктуру ключів, ДТС та служби каталогу облікових записів користувачів.

SSO інтегрований з Windows. Ці служби дозволяють підключатися до кількох додатків у мережі, які використовують загальний механізм автентифікації. Вони запитують та підтверджують обліковий запис користувача після входу в мережу та використовують ці облікові дані, щоб визначити дії, які користувач може виконувати на основі наданих прав. Наприклад, якщо програми інтегруються за допомогою Kerberos, після того, як система автентифікує облікові дані, користувач може отримати доступ до будь-якого ресурсу в мережі, що інтегрований з Kerberos.

Серверне SSO внутрішньої мережі. Ці служби дозволяють інтегрувати неоднорідні програмні додатки та системи в корпоративне середовище. Ці програмні додатки та системи можуть не використовувати загальну автентифікацію. Кожний програмний додаток має свій власний каталог облікових даних користувачів. Наприклад, Windows використовує службу каталогу Active Directory для автентифікації користувачів, а менфрейм комп'ютери використовують Інструмент контролю доступу до ресурсів (від англ. Resource Access Control Facility IBM (RACF) для автентифікації тих самих користувачів. В межах підприємства корпоративна шина даних інтегрує програмні додатки «фронт-ендів» (від англ. front-end) та «бек-ендів» (від англ. back-end). Корпоративний SSO дозволяє користувачам підприємства під'єднуватися як до програмних додатків «фронт-енду», так і «бек-енду», використовуючи лише один набір облікових даних. Це дає можливість при ініціації як з Windows Single Sign-on (в якому початковий запит виконується з середовища домену Windows), так і Host Initiated Single Sign-On (в якому початковий запит здійснюється з середовища, не пов'язаного з Windows) отримати доступ до ресурсу в домені Windows.

Синхронізація паролів спрощує адміністрування бази даних SSO та зберігає паролі в синхронізації через каталоги користувачів. Це можна зробити за допомогою адаптерів синхронізації паролів, які можна налаштувати та якими можна керувати за допомогою інструментів синхронізації паролів.

SSO зовнішньої мережі (Web SSO). Ці служби дозволяють отримувати доступ до ресурсів через Інтернет за допомогою єдиного набору облікових даних користувача. Користувач надає набір облікових даних для входу на різні веб-сайти, що належать різним організаціям. Прикладом цього типу SSO є мережа Microsoft Passport для додатків споживачів. Для федеративних сценаріїв служби федерації Active Directory надає Web SSO.

Одним із прикладів програмного забезпечення SSO з відкритим кодом є система Shibboleth, яка підтримує федерації хмар та ідентифікацію між багатьма сайтами, що використовують стандарт SAML. На рівні програмного забезпечення основна частина системи Shibboleth – це бібліотеки OpenSAML. Додана вартість цього програмного забезпечення полягає в підтримці конфіденційності, удосконаленні бізнес-процесів через атрибути користувачів, підтримці масштабованих політик контролю та федерацій через метадані.

Федерація – це набір груп юридичних осіб (доменів безпеки), які встановили зв'язки для безпечного обміну ресурсами. Юридичні особи, що входять до групи, поділяють набір узгоджених політик та правил доступу до онлайнових ресурсів, зокрема у відповідності до стандарту ISO 270001. Постачальник ресурсів з однієї групи може надати авторизований доступ до ресурсу, яким він розпоряджається в іншій групі, на основі запиту щодо атрибуту (такого як обліковий запис або інший визначальний атрибут користувача), які підтверджені постачальником сервісу ідентифікації користувачів (або сервісом видачі квитків безпеки). Федерація забезпечує структуру та

правову основу, яка дає змогу проводити автентифікацію та авторизацію в різних організаціях.

Федеративний сценарій особливо актуальний для великих банків, яким необхідно надати захищений доступ до даних. Такими, наприклад, можуть бути дані кредитного бюро або платіжної інфраструктури «бек-ендів» через інтерфейс програмування додатків (від англ. Application Programming Interface, API) згідно вимог оновленої директиви щодо платіжних сервісів (від англ. Revised Payment Service Directive, PSD2). В окремих випадках банку необхідно надати доступ до веб-сервісів для використання як власними співробітниками, так і уповноваженими співробітниками бізнес-партнерів, або корпоративних клієнтів. Через використання стандартних механізмів IT рішень щодо федеративних сценаріїв доступу, таких як WS-Federation, банк має змогу надати доступ до веб-сервісів без необхідності здійснювати адміністрування облікових записів працівників партнерів, що знижує витрати банку, адже облікові записи партерів адмініструються самими партнерами.

Хмарна інфраструктура може бути організована у відокремлених доменах безпеки (програмний додаток або сукупність програм, які всі довіряють спільному фактору безпеки для автентифікації, авторизації або управління сесією), що дозволяє створити федеративні хмари.

Федеративні хмари – це сукупність окремих хмар, які можуть взаємодіяти, тобто обмінюватися даними та обчислювальними ресурсами через певні інтерфейси. У федерації хмар кожна окрема хмара залишається незалежною, але може взаємодіяти з іншими хмарами в федерації через стандартизовані інтерфейси.

Застосування федерацій спільно з технологією інфраструктури відкритих ключів (від англ. Public Key Infrastructure, PKI) та полегшеним протоколом доступу до каталогів (від англ. Lightweight Directory Access Protocol, LDAP) призведе до ефективних довірчих відносин між залученими суб'єктами.

Основні вимоги побудови Системи управління інформаційною безпекою та автентифікації користувачів банківських ІС

Основні вимоги та підходи до побудови визначені у стандартах Міжнародної організації зі стандартизації (від англ. International Organization for Standardization, надалі ISO) ISO 27000, 27001, 27002, 27005. Національний банк України (надалі НБУ) адаптував ці вимоги у нормативному документі «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» (надалі – Положення) [6].

На рівні програмного додатку мають застосовуватись механізми захисту для забезпечення сильної автетифікації користувача, контроль цілісності та конфіденційності на всіх етапах обробки інформації.

Крім того користувачі з привілейованими правами доступу до банківських ІС (адміністратори) мають застосовувати механізм двофакторної автентифікації, для мінімізації ризику несанкціонованого доступу до даних, які становлять банківську таємницю. В Положенні зазначено, зокрема, таке: «Банк зобов'язаний використовувати механізми двофакторної автентифікації під час надання доступу до систем автоматизації банку та управління базами даних» [6].

Положення також регламентує порядок управління та блокування облікових записів користувачів, аудит подій доступу, застосування алгоритмів криптографічного захисту інформації, захисту від зловмисного коду, використання актуальних версій операційних та прикладних систем.

Світові тенденції щодо пріоритетів безпеки. Зміна пріоритетів щодо забезпечення безпеки хмарних технологій підтверджується результатами досліджень

компанії Kuppingercole [8 с. 53]. На рис. 1 графічно зображено три виміри: хмарні обчислення (моделі розгортань), соціальні обчислення (популяції користувачів), мобільні обчислення (типи пристроїв). Традиційне покриття проблем щодо безпеки ІТ, щодо хмарних обчислень, охоплює наступні моделі розгортань: встановлення банківських ІС на власних серверах в приміщеннях банку (від.англ. On-premise), аутсорсинг/оренда серверного апаратного забезпечення, приватна хмара, або використання хмарних сервісів та потужності апаратних ресурсів на власному фізичному/орендованому апаратному забезпеченні банку. В контексті соціальних обчислень традиційне покриття ІТ безпеки охоплює внутрішніх користувачів та партнерів, а контексті типів пристроїв охоплюються лише персональні комютери (надалі – ПК) та ноутбуки. Автор вважає, що традиційне покриття ІТ безпеки цілком вписується в не застосовну до хмарних технологій концепцію периметрового захисту.

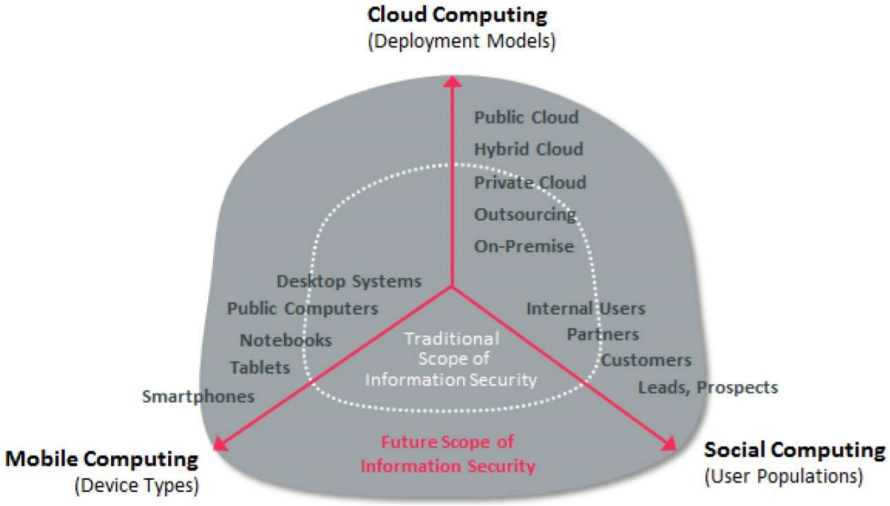

Рисунок 1 – Майбутній обсяг покриття проблем щодо ІТ безпеки [8, с. 53]

На думку автора, в умовах глобальної тенденції щодо діджиталізації, тобто масової міграції кінцевих користувачів з ПК до мобільних пристроїв, таких як планшети та телефони, біометричних методів автентифікації користувачів (відбиток пальця, обличчя тощо) відмови від використання паперових носіїв інформації (договорів, заяв, виписок, чеків та інше), до електронного документообігу слід застосовувати інші механізми забезпечення конфіденційності, цілісності, доступності банківської інформації, що відповідають сучасним (в контексті рис.1. – «майбутнім») підходам до забезпечення безпеки ІТ, таких як SSO з підтримкою федеративних сценаріїв доступу та запровадження ДТС.

Практичне застосування технологій SSO в діяльності банку. За умов гетерогенного ІТ ландшафту, що історично сформувався в більшості банківських установ, на робочих станціях операціоністів встановлено велику кількість різнорідного програмного забезпечення, від різних постачальників, яке, як правило, потребує окремої авторизації через введення логіну та паролю користувача. Це в цілому погіршує ситуацію з безпекою ІТ банківських систем, адже користувачі або встановлюють однакові паролі до кожного програмного додатку, або, в гіршому випадку, зберігають їх на паперових носіях у доступних для сторонніх осіб місцях. Крім того це негативно впливає на продуктивність працівників, адже кожен вхід до системи, введення паролю і логіну – це додатковий не ефективно витрачений час. В

масштабах великого банку з декількома десятками тисяч працівників це суттєво знижує ефективність бізнес-процесів.

Системи управління заставним майном, «фронт-енди» операціоністів по роботі з касовими операціями, проведенням скорингу та андерайтингу, системи по роботі з кредитами та депозитами, системи по роботі з карткою клієнта та перевіркою на приналежність до чорних списків, системи обслуговування карткових рахунків, системи видачі пластикових карток, системи з обслуговування банкоматів, системи обслуговування еквайрингових операцій, системи процесингу клієнтських заявок, системи формуванню управлінської звітності, системи клієнт-банк – це далеко не повний перелік систем, з якими доводиться працювати користувачам на робочій станції.

В середовищі SSO користувач може отримати доступ до всіх цих систем, до яких він уповноважений отримувати доступ, увівши логін і пароль лише один раз, в межах сесії. В комбінації з двофакторною авторизацією це значно підвищує як ефективність процесів, так і рівень безпеки IT. З точки зору графічного інтерфейсу користувача SSO реалізовується як сторінка в браузері (рис 2.), де користувач може отримати доступ до всіх необхідних систем через «тонкий» клієнт (від англ. Thin client).

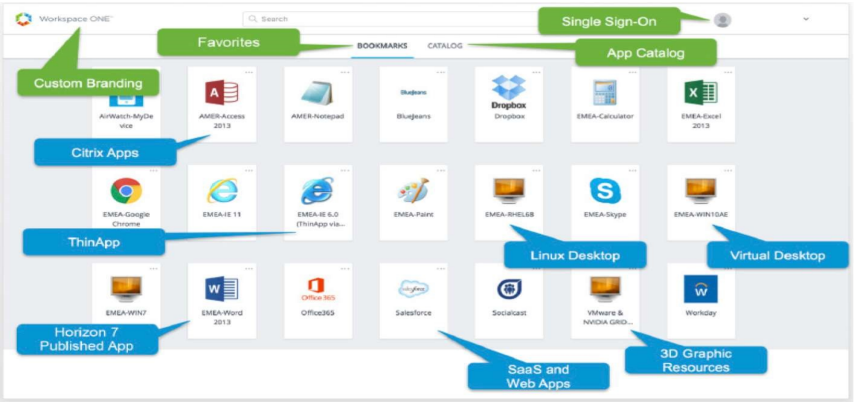

Рисунок 2 – Приклад графічного інтерфейсу користувача, що забезпечує SSO [9, с.8]

Іншим перспективним напрямом застосування SSO з двофакторною біометричною автентифікацією є високо ризиковані операції в системах інтернет банкінгу клієнт-банк та відділеннях банку. Другим фактором при автетифікації клієнта може виступати відбиток пальця або сканування обличчя. Це дозволяє уникнути ризиків шахрайства при здійсненні грошових переказів, кредитних та депозитних операцій, що являють собою зону операційного ризику в діяльності банківської установи.

Крім того використання продуктів Microsoft Office 365 та Sharepoint на базі хмарних технологій, дозволяє досягти економії ліцензій та підвищити ефективність взаємодії між підрозділами банку.

Використання федеративних сценаріїв доступу до ресурсів кредитних бюро, на запит авторизованого користувача з іншого банку є ще одним перспективним напрямом застосування сучасних підходів до управління доступом та обліковими записами. Це дозволить підвищити рівень співпраці, щодо обміну інформацією по проблемним позичальникам та покращити якість кредитного портфелю, в цілому, по банківській системі.

Висновки та перспективи подальших досліджень. В умовах діджиталізації, збільшення мобільності і масового переходу кінцевих користувачів від настільних комп'ютерів і ноутбуків до мобільних пристроїв, банківським установам необхідно адаптуватись відповідно до цих викликів. Критично необхідною є своєчасна адаптація політик і засобів захисту від загроз безпеки ІТ.

Автором аргументовано, що за таких умов периметровий захист є неефективним і має бути замінений сучасними механізмами SSO та стандартами федеративного доступу. Найбільшої економічної ефективності впровадження таких рішень можна досягти за рахунок використання хмарних технологій IDaaS (від англ. Identity as a Service, IDaaS). При такій моделі розгортання програмне забезпечення управління доступом та обліковими записами користувачів використовується як хмарний сервіс. Тобто в повній мірі застосовуються всі можливості хмарних технологій – економія капітальних інвестицій, максимальна ефективність використання ресурсів, гнучка масштабованість апаратних потужностей згідно потреб.

З точки зору програмних продуктів спеціалізовані компанії надають більше функціональних можливостей щодо SSO. Не зважаючи на це, автор вважає, що продукти від глобальних корпорацій (IBM, Oracle, Microsoft) мають переваги для великих банківської установ, з огляду на можливості використання інших функціональних модулів від цих же постачальників, наявності спеціальних цінових пропозицій, що в свою чергу зменшує кількість додаткових програмних додатків і спрощує ІТ ландшафт.

Але вибір конкретного рішення залежить від ІТ стратегії і бачення директора з ІТ. У випадку наявності достатньої кількості кваліфікованих внутрішніх ресурсів можливе використання програмного забезпечення з відкритим кодом (наприклад Shiboleth) та розробка на його базі власних рішень ІТ. Автор впевнений, що такий підхід, є швидше виключенням ніж правилом. Щодо функціональності та якості продуктів управління доступом, в довгостроковій перспективі, банки не зможуть конкурувати з професійними ІТ компаніями. Крім того не має сенсу постійно інвестувати у власну ІС без наміру подальшого продажу ліцензій, що не є статутним видом діяльності банку.

Список літератури

1. Зіссіс Д. Адресуючи проблеми безпеки хмарних обчислень [Текст] / Д. Зіссіс, Д. Леккас // Комп'ютерні системи майбутнього покоління. – 2012. – № 28. – С. 583–592.
2. Бобиль В.В. Управління ризиками «хмарних» технологій в системі ризик-менеджменту банку [Текст] / В.В. Бобиль // Збірник наукових праць Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна. Проблеми економіки транспорту. – 2014. – Вип. 7. – С. 29-36.
3. Бобиль В.В. "Хмарні" технології як фактор збільшення операційного ризику банку [Текст] / В.В. Бобиль, М.А. Дронь // Банківська справа. – 2014. – № 11/12. – С. 47-62.
4. Корольов В.Ю. Захист інформації в корпоративних USB-флеш накопичувачах для хмарних обчислень [Текст] / В.Ю. Корольов // Мат. машини і системи. – 2012. – № 2. – С. 60-69.
5. Кондратьев А.А. Разработка распределенной системы защиты облачных вычислений [Текст] / А.А. Кондратьев, И.П. Тищенко, В.П. Фраленко // Программные системы: Теория и приложения. – 2011. – № 4(8).
6. Постанова Правління Національного Банку України «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28 вересня 2017 року №95 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0095500-17
7. Звіт KuppingerCole щодо управління доступом та федерацій, офіційний веб сайт Identity solutions review [Електронний ресурс]. – Режим доступу : solutionsreview.com/identity-management/kuppingercole-leadership-compass-access-management

8. Технічна документація щодо архітектури рішення IT VMWARE HORIZON 7, офіційний веб сайт Wmware [Електронний ресурс]. – Режим доступу : www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-horizon-7-enterprise-validated-integration-design-reference-architecture.pdf

References

1. Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems.* No. 28, pp. 583–592.
2. Bobyl, V.V. (2014), «Upravlinnia ryzykamy "khmarnykh" tekhnolohii v systemi ryzyk-menedzhmentu banku» [Risk management of "cloud" technologies in the system of risk management of the bank], *Collection of scientific works of Dnipropetrovsk National University of Railway Transport named after academician V. Lazaryan. Problems of transport economy*, No. 7, pp. 29-36.
3. Bobyl, V.V. (2014), «Khmarni tekhnolohii yak faktor zbilshennia operatsiinoho ryzyku banku» ["Cloud" technology as a factor in increasing the operational risk of the bank], *Banking business*, No. 11(12), pp. 47-62.
4. Korolov, V.Yu. (2012), «Zakhyst informatsii v korporatyvnykh USB-flesh nakopychuvachakh dlia khmarnykh obchyslen» [Protecting information in corporate USB flash drives for cloud computing], *Math. machines and systems*, No. 2, pp. 60-69.
5. Kondratev, A.A., Tyshchenko, Y.P. and Fralenko, V.P. (2011), «Razrabotka raspredelennoi systemy zashchyty oblachnykh vychyslenyi» [Development of a distributed system for protecting cloud computing], *Program Systems: Theory and Applications,* No. 4(8).
6. National Bank of Ukraine Board Resolution «On approval of the Regulation on measures to ensure information security in banking system of Ukraine» (2017), official Ukrainian Government web site, available at: zakon2.rada.gov.ua/laws/show/v0095500-17 (accessed 26 March 2018).
7. Kuppinger Cole Report Access Management and Federation (2016), Identity solutions review official website, available at: solutionsreview.com/identity-management/kuppingercole-leadership-compass-access-management (accessed 26 March 2018).
8. Reference architecture VMWARE HORIZON 7 (2018), WMware official website, available at: www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-horizon-7-enterprise-validated-integration-design-reference-architecture.pdf (accessed 26 March 2018).

Roman Baglai, postgraduate
Kyiv National University of Trade and Economics, Kyiv, Ukraine

Banking Information Systems Security Management Mechanisms

Given that the bank has the client data in its possession it needs to be protected against misappropriation, modification, or destruction at all times. The purpose of this article is present relevant approaches for protection from information security threats through the use of cloud technology which will allow to reduce costs and increase efficiency of information technology systems supporting business processes of the bank.

Global digitalization trend with mass migration of the end users from desktop to mobile devices and from paper based to digital work flows requires banks to reconsider the scope of traditional IT security. This means that the bank should review approaches to deliver high quality of service to customers at low cost and still maintaining sustainable level of security. Use-cases for implementation of Single sign-on hereinafter SSO) and Identity as a service cloud based solutions formulated in this article. Implementation will allow to address problems and to improve both security and operational efficiency of bank`s work-flows. Considered future scope of information security and cloud based IT solutions of the Vendors.

State of the art mechanisms for management of banking information systems security to address respective issues were analyzed in scope of the article. Researched trends for steering of IT security to mitigate threats including those originated by cloud technology for bank entireties. Proposed modern approach for building of safety net via introduction of Trusted Third Party, implementation of SSO and federated access scenarios.

The results of the study can be validated through the implementation of relevant projects driven by challenges and trends in the banking sector, market and regulatory changes.

cloud based architecture of a Bank, Trusted Third Party, Single sign-on, Identity as a Service

Одержано (Received) 13.04.2018