Захист інформації та кібернетична безпека

УДК 004:336.71 DOI: 10.30748/soi.2018.152.18

Р.О. Баглай

Київський національний торговельно-економічний університет, Київ

ЗАГРОЗИ БЕЗПЕКИ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ БАНКІВ

Проведено аналіз загроз безпеки інформаційних технологій при впровадженні хмарних обчислень для забезпечення безперебійної та ефективної діяльності банківських установ і запропоновано заходи щодо мінімізації цих загроз. Розглянуто проблеми та переваги хмарних технологій на різних рівнях архітектурного ландшафту банку для забезпечення конфіденційності, цілісності, автентичності та доступності даних. Результати дослідження можуть бути імплементовані шляхом впровадження відповідних проектів, зумовлених викликами та тенденціями банківської сфери, ринковими та регуляторними змінами.

Ключові слова: *IT архітектура банку, хмарні технології, проект OWASP, класифікація CAPEC, стандарт PCI DSS, директива PSD2, нормативні вимоги GDPR, стандарт TLS, стандарт SAML, технологія SSO, електронний цифровий підпис.*

Вступ

Постановка проблеми. Застосування хмарних технологій для банківської установи дозволяє якісно підвищити ефективність використання банківських інформаційних систем для скорочення витрат управління бізнес-процесами та надання інноваційних сервісів клієнтам. Водночас існує ряд проблем, які не дозволяють українським фінансовим установам широкомасштабне застосування можливостей хмарних технологій. До них, зокрема, можна віднести такі:

- відсутність системних підходів до захисту інформації та забезпечення конфіденційності клієнтських даних;
- відсутність системних підходів до забезпечення цілісності і шифрування даних;
- низький рівень довіри до постачальників публічних хмарних сервісів;
- обмеження законодавства та НБУ.

Банки як організації, що займаються зберіганням та обробкою персональних даних, зобов'язані дотримуватися вимог законодавства України, яке передбачає необхідність забезпечення відповідного рівня конфіденційності та захисту даних, у тому числі й тих, що становлять банківську таємницю. Хмарна інфраструктура породжує ряд юридичних проблем, пов'язаних із конфіденційністю даних, що зберігаються в декількох місцях у хмарі, додатково збільшуючи ризик порушень конфіденційності. Це зумовлено тим, що дані зберігаються не на серверах банку, а на серверах постачальника послуг, які можуть бути в Європі, Азії, або де інде. Цей принцип хмарних обчислень конфліктує з різними юридичними нормами, які вимагають щоб банк забезпечив контроль і обізнаність щодо розташування даних, які є у його розпорядженні в режимі реального часу.

З точки зору безпеки виникла низка нештатних ризиків [4] 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 із 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.

Аналіз останніх досліджень і публікацій. Проблеми безпеки застосування хмарних технологій в різних соціально-економічних сферах досліджували вітчизняні та зарубіжні науковці Андрощук О.С., Батаєв О.В., Бобиль В.В., Корольов В.Ю., Литвинова С.Г., Кондратьєв А.А. та інші.

Формулювання мети статті. Метою даної статті є аналіз перспективних напрямів захисту від загроз безпеки ІТ, що дозволить здійснити впровадження хмарних технологій для банківських інформаційних систем (надалі – ІС), для скорочення ви-

трат та підвищення ефективності підтримки ІТ для бізнес-процесів банку.

Виклад основного матеріалу

В рамках цієї статті розглянуті основні вимоги щодо безпеки ІТ банківських ІС, які регламентовані нормативно-правовими актами НБУ та Європейських регуляторів. Складено модель загроз безпеки ІТ щодо архітектури банку на основі хмарних технологій. Запропоновані механізми захисту від загроз із застосуванням передових технологій та рішень ІТ від постачальників, лідерів ринку ІТ для забезпечення конфіденційності, цілісності та доступності даних.

Конфіденційність означає, що лише уповноважені сторони або системи можуть мати доступ до захищених даних.

Цілісність означає, що активи можуть бути змінені тільки уповноваженими сторонами в дозволений спосіб, що стосується даних, програмного та апаратного забезпечення.

Доступність означає властивість системи забезпечувати вхід авторизованого користувача та функціональність згідно його потреб.

Вимоги щодо безпеки банківських ІТ на основі хмарних технологій. Основні вимоги та підходи до побудови Системи управління інформаційною безпекою визначені у стандартах ISO 27000, 27001, 27002, 27005. НБУ адаптував ці вимоги у проекті «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» (надалі – Положення), яке набуває чинності з 01 березня 2018 року.

Зокрема для захисту «сеансового рівня» взаємодії відкритих інформаційних систем НБУ регламентовано використання криптографічного протоколу захисту на транспортному рівні версії 1.2 (Trasport Layer Security, надалі TLS) для забезпечення контролю цілісності та конфіденційності інформації. На рівні програмного додатку мають застосовуватись механізми захисту для забезпечення сильної автентифікації 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.

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.

Одною з основних вимог НБУ щодо безпеки ІТ банківських ІС є забезпечення цілісності фінансових транзакцій. Згідно вимог «Положення про застосування електронного підпису в банківській системі України» (надалі положення) для забезпечення цілісності банки мають застосовувати електронний цифровий підпис (надалі – ЕЦП) для платіжних документів на всіх етапах їхньої обробки. Згідно вимог Положення обов'язковим є використання послуг електронного цифрового підпису від центрів сертифікації ключів, які акредитовані в Засвідчувальному центрі НБУ.

Нажаль Положення не регламентує порядок застосування хмарних технологій в архітектурі ІТ банку, не містить вимог до безпеки таких технологій та базується на перемитровій концепції захисту, яка не може бути застосована до хмарних технологій.

Законодавство ЄС містить ряд технічних вимог до банківських установ, які вимагають застосування передових технологій для можливості побудови ефективних процесів. Існує висока ймовірність того, що органи законодавчої та виконавчої влади, включаючи НБУ, ратифікують ці вимоги в рамках стратегії Євроінтеграції. Зокрема, наступні вимоги:

- впровадження стандартів Оновленої директиви [10] щодо платіжних сервісів (англ. Revised Payment Service Directive, надалі – PSD2);
- впровадження стандартів Уніфікованого положення [11] щодо захисту даних (англ. General Data Protection Regulation, надалі GDPR);
- впровадження стандарту [9] безпеки даних індустрії платіжних карток (англ. Payment Card Industry Data Security Standard, надалі PCI DSS);
- впровадження PSD2 передбачає надання відкритого доступу до автоматизованих банківських систем, для використання третіми сторонами в якості платіжної інфраструктури, через відкриті програмні інтерфейси додатків (англ. Application Programming Interface, надалі API);
- стандарт GDPR регламентує вимоги щодо захисту персональних даних та забезпечення можливості їх видалення з усіх систем банку на вимогу клієнта, в першу чергу, не резидента.

Загрози безпеки банківських ІТ на основі хмарних технологій. Розглянемо модель загроз безпеки ІТ для банківських ІС. Загроза компрометації даних збільшується у хмарі, внаслідок збільшення числа сторін, пристроїв та програм, що призводить до збільшення кількості точок доступу до єдиного розподіленого ресурсу. Делегування контролю доступу до даних власнику хмарної інфраструктури, призводить до збільшення ризику компрометації даних, оскільки дані стають доступними для великої кількість учасників [3]. Порушників режиму безпеки ІТ банківських ІС можна умовно поділити на зовнішніх та внутрішніх. До зовнішніх можна віднести користувачів мережі Інтернет без привілейованого доступу до мережевих ресурсів, користувачів з обмеженим доступом до безпровідних мереж, користувачів с доступом до внутрішньої мережі з використанням віртуальної

приватної мережі (від англ. Virtual Private Network, надалі – VPN), користувачів з доступом до апаратної інфраструктури. До внутрішніх можна віднести користувачів операційних систем банку без привілеїв адміністраторів, користувачів з доступом адміністраторів, користувачів з доступом до серверної інфраструктури на апаратному та програмному рівні (адміністратори серверів, комутаційного обладнання, баз даних, систем управління базами даних та додатків).

Управління хмарною інфраструктурою на основі попиту на апаратні ресурси від користувачів, породжує високу залежність від постійної доступності мереж. Апаратне забезпечення та цілісність мережі є додатковим питанням, яке потребує вирішення постачальником хмарних сервісів, оскільки він повинен захистити обладнання, яке забезпечує надання хмарних сервісів від крадіжки, модифікації або підробки. З метою уніфікації підходів для подальшого аналізу використані класифікації (табл. 1) загроз OWASP [7] (абревіатура англ. Open Web Application Security Project) топ 10, 2017 року, співставленні з відповідними видами атак (табл. 2) згідно класифікації CAPEC [8] (абревіатура англ. Common Attack Pattern Enumeration and Classification).

Таблиця 1

Класифікація та технічні наслідки кібератак

№ OWASP топ 10	№ CAPEC	Назва атаки	Контекст атаки	Технічні наслідки
A1:2017-ін'єкція	CAPEC-66.	SQL ін'єкція	Конфіденційність, Контроль доступу, авторизація, цілісність	Зчитування даних, модифікація даних, виконання недозволеного коду, команд, отримання привілеїв доступу, підробка облікових даних, модифікація даних програмного додатку
A2:2017-порушена автентифікація	CAPEC-90:	Атака відображення в протоколі автентифікації маніпуляція протоколом	Конфіденційність, контроль доступу, авторизація	Отримання привілеїв доступу / підробка облікових даних, обхід механізмів захисту
A3:2017-розкриття конфіденційної інформації	CAPEC-54:	Запит ІС на інформацію	Конфіденційність	Зчитування даних програмного додатку, зчитування даних пам'яті
A4:2017-XML зовнішні сутності	CAPEC-197:	XML розширення сутностей	Доступність	Перевищення лімітів, споживання ресурсів (ЦПП), споживання ресурсів (пам'ять), споживання ресурсів (інше)
A5:2017-порушення контролю доступу	CAPEC-74	Маніпуляція ідентифікатором привілеїв користувача	Конфіденційність, контроль доступу, авторизація, цілісність	Отримання привілеїв доступу, підробка облікових даних, модифікація даних програмного додатку
A6:2017-неправильне налаштування ІБ	CAPEC-25	Циклічне блокування декількох паралельних процесів, завершення яких залежить від попередника	Доступність	Відмова роботи ІС через вичерпання доступних ресурсів
A7:2017-між. сайт. скриптниг	CAPEC-63:	Між сайтовий скриптниг (XSS)	Конфіденційність, цілісність, доступність	Виконання несанкціонованого коду, команд, модифікація даних програмного додатку, зчитування даних програмного додатку
A8:2017- небезп. десеріалізація	CAPEC-250:	XML ін'єкція	Конфіденційність, контроль доступу, авторизація	Отримання привілеїв доступу / підробка облікових даних, зчитування даних програмного додатку
A9:2017- використання компонентів з відомими вразливостями	CAPEC-111:	JSON злам (JavaScript злам)	Конфіденційність	Зчитування даних програмного додатку
A10:2017-недостат. логування та моніторинг	CAPEC-75:	Маніпуляція. не захищеним від запису конфігураційним файлом	Конфіденційність, контроль. доступу, авторизація	Отримання привілеїв доступу / підробка облікових даних

Таблиця 2

Числові значення факторів ризику кібератак

№ CAPEC	Імовірність	Складість реалізації	Застосовність	доступність ресурсів	Імовірність настання ризику	Вплив конфіденційність	Вплив цілісність	Вплив доступність	Потенційна шкода	Масштаб збитків
C-66	0,2	0,2	0,2	0,2	0,8	3	3	3	3	12
C-90	0,2	0,15	0,2	0,15	0,7	3	3	1	2	9
C-54	0,2	0,15	0,2	0,2	0,75	2	2	1	1	6
C-197	0,2	0,2	0,15	0,2	0,75	1	1	3	2	7
C-74	0,15	0,15	0,2	0,15	0,65	3	3	2	3	11
C-25	0,1	0,1	0,2	0,1	0,5	1	1	3	3	8
C-63	0,2	0,1	0,15	0,2	0,65	3	3	3	3	12
C-250	0,2	0,2	0,15	0,2	0,75	3	3	2	2	10
C-111	0,2	0,15	0,15	0,2	0,7	3	1	1	3	8
C-75	0,2	0,15	0,2	0,1	0,65	3	3	2	3	11

Багатокористувацьке розподілене середовище хмари містить унікальні виклики безпеки, в залежності від рівня, на якому працює користувач: програмний додаток, віртуальна або фізична інфраструктура.

Внаслідок порушення цілісності, конфіденційності, доступності ІС для банківської діяльності банк може понести репутаційні, регуляторні збитки, господарські збитки, або припинити діяльність у випадку позбавлення ліцензії. Порушення конфіденційності, зокрема, призводить до розголошення банківської таємниці; порушення цілісності може призвести до незаконного привласнення клієнтських коштів, порушення доступності до зупинки банківських процесів з обслуговування клієнтів.

Наведена оцінка ризиків базується на якісній оцінці кібератак (рис. 1.).

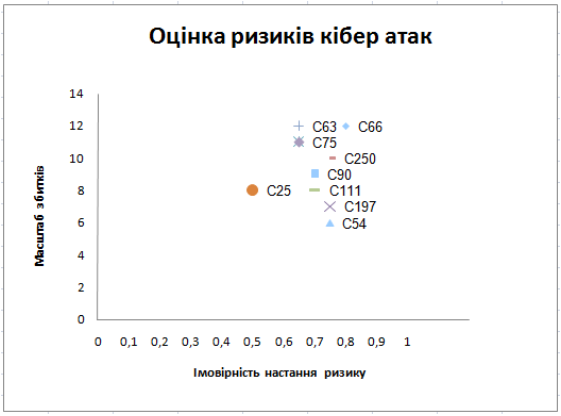

Рис. 1. Оцінка ризиків кібератак

Для класифікації кібератак застосовуються стандарти корпорації MITRE. По осі Y розміщена шкала масштаб збитків, по осі X шкала вірогідність настання ризику. Значення для цих параметрів розраховуються для кожної із загроз. Кожна з загроз входить до однієї з категорій OWASP top 10. Для зручності візуалізації всі значення на діаграмі помножені на 10.

Для розрахунку імовірності настання ризику використовуються наступні фактори, згідно з даними ресурсу MITRE:

- імовірність;
- складність реалізації;
- застосовність;
- доступність ресурсів.

Під імовірністю розуміється числова характеристика можливості того, що кібератака відбудеться в умовах, які можуть бути відтворені необмежену кількість разів.

Під складністю реалізації розуміється необхідність наявності у порушника режиму ІБ певного рівня спеціальних знань та вмінь для здійснення кібератаки.

Під застосовністю розуміється можливість застосовувати кібератаку на рівні різних архітектур, фреймворків, операційних систем, мов програмування.

Під доступністю ресурсів та засобів реалізації розуміється можливість отримання порушником режиму ІБ легкого доступу до необхідних ресурсів.

Числове значення параметру «ймовірність» визначається на основі класифікації ресурсу MITRE: unlikely = 0,1, likely = 0,15, very likely = 0,2.

Числове значення параметру «складність реалізації» визначається на основі класифікації ресурсу MITRE: knowledge and skill required low = 0,1, medium = 0,15, high = 0,2.

Числове значення параметру «застосовність» визначається на основі класифікації ресурсу MITRE: якщо атака застосовуватися до всіх типів архітектур, фреймворків, платформ, мов програмування, то значення параметру дорівнює 0,2, якщо атака може застосовуватися до певних, широко розповсюджених типів архітектур, фреймворків, платформ (наприклад «клієнт-сервер», J2EE, Java), то значення параметру становить 0,15, якщо атака може застосовуватися до окремих менш розповсюджених чи застарілих типів архітектур, фреймворків, платформ (наприклад файловий обмін, Novel Netware, MS DOS, Cobol), то значення параметру приймають за 0,1.

Числове значення параметру «доступність ресурсів та засобів реалізації» визначається на основі класифікації ресурсу MITRE: відсутність необхідності в спеціальних ресурсах, програмному забезпеченні, програмне забезпечення з відкритим програмним кодом, у вільному доступі – значення параметру дорівнює 0,2; ліцензоване програмне забезпечення, необхідність у спеціалізованому апаратному забезпеченні – значення параметру дорівнює 0,15; необхідність у значних програмних/апаратних ресурсів, суперкомп'ютерів значення параметру дорівнює 0,1.

Загальне значення імовірності настання ризику розраховується як сума зазначених вище параметрів, та відображається по осі X.

Для розрахунку масштабу збитків використовуються наступні фактори (табл. 2), згідно з даними ресурсу MITRE:

- вплив на конфіденційність;
- вплив на цілісність;
- вплив на доступність;
- потенційна шкода.

Під впливом на конфіденційність розуміється ступінь впливу на конфіденційність, внаслідок успішної кібератаки, що призводить до порушення конфіденційності.

Під впливом на цілісність розуміється ступінь впливу на цілісність, внаслідок успішної кібератаки, що призводить до порушення цілісності.

Під впливом на доступність розуміється ступінь впливу на доступність, внаслідок успішної кібератаки, що призводить до порушення доступності.

Під потенційною шкодою розуміється тяжкість технічних наслідків кібератаки і складність виконання заходів щодо відновлення ІС без втрат даних.

Числове значення параметру «вплив на конфіденційність» визначається на основі класифікації ресурсу MITRE: low = 1, medium = 2, high = 3.

Числове значення параметру «вплив на цілісність» визначається на основі класифікації ресурсу MITRE: low = 1, medium = 2, high = 3.

Числове значення параметру «вплив на доступність» визначається на основі класифікації ресурсу MITRE: low = 1, medium = 2, high = 3.

Числове значення параметру «потенційна шкода» визначається на основі класифікації ресурсу MITRE: medium = 1, high = 2, very high = 3.

Загальне значення параметру «масштаб збитків» розраховується як сума зазначених вище параметрів, та відображається по осі Y.

Як видно з діаграми найбільш критичним щодо ймовірності настання і масштабу потенційного збитку є атаки з класифікації OWASP A1, яка відповідає атаці CAPEC-66, – SQL ін'єкція, що призводить до таких критичних технічних наслідків як виконання недозволеного коду, команд, отримання привілеїв доступу, підробка облікових даних, модифікація даних програмного додатку тощо.

Механізми захисту від загроз безпеки банківських ІТ на основі хмарних технологій. Комбінуючи різні види атак, зловмисник може заволодіти даними, що становлять банківську таємницю та вимагати винагороди за нерозголошення, зашифрувати дані в базі даних, порушити безперервність банківських процесів, здійснити несанкціоноване перерахування коштів та завдати інших збитків.

Завданнями безпеки [1] в межах архітектури банківської ІС на основі хмарних технологій, у відповідності до контролів регламентованих стандартом ISO 270001, є:

• забезпечити доступність інформації, що передається між інтегрованими системами або зберігається в межах цих систем;

• зберегти цілісність інформації, що передається між ними або зберігається в межах систем, тобто запобігання втрати або зміни інформації через несанкціонований доступ, несправність компонентів або іншої помилки;

• зберегти цілісність наданих послуг, тобто конфіденційність і правильну роботу ІС;

• забезпечити контроль за рівнем доступу до сервісів або їх компонентів, щоб користувачі могли використовувати тільки ті сервіси, для яких вони є авторизованими;

• забезпечити ідентифікацію сторін, що взаємодіють, нерозголошення джерел походження даних та їх передачі;

• забезпечити безпечну взаємодію з системами обмеженого доступу;

• забезпечити конфіденційність інформації, що зберігається в системі, яка інтегрується;

• чітко розділити дані і процеси на віртуальному рівні хмари, забезпечуючи повну відсутність витоку даних при взаємодії між різними програмними додатками;

• зберегти той самий рівень безпеки при додаванні чи вилученні ресурсів на фізичному рівні.

З огляду на те, що встановлення фізичного периметру безпеки за умов розгортання банківської ІС на хмарній інфраструктурі неможливе, слід застосо-

вувати інші механізми захисту. За таких обставин необхідно визначити довірену третю сторону (надалі – ДТС) в межах хмари, а для забезпечення довіри та впровадити політики використання криптографії, для гарантування конфіденційності, цілісності та автентичність даних та зв'язків, щоб вирішити конкретні ризики та убезпечити вразливі місця безпеки [2].

Обсяг довіри до ДТС визначається забезпеченням надання сервісів безпеки які цілком охоплюють процеси служб безпеки, що масштабуються, працюють на основі стандартів та застосовних в різних доменах, географічних районах і враховують специфіку банківського сектора.

У криптографії ДТС є суб'єктом, який сприяє безпечній взаємодії між двома сторонами. Завданням ДТС в межах інформаційної системи є забезпечення повного циклу сервісів безпеки, які є масштабованими, базуються на стандартах та можуть бути застосовані в різних доменах, географічних середовищах та галузях спеціалізації. Введення ДТС може компенсувати втрату традиційного периметру безпеки створюючи надійні домени безпеки.

Ця інфраструктура використовує систему дистрибуції цифрових сертифікатів і механізм з в'язання цих сертифікатів з відомими джерелами походження та цільовими сайтами на кожному сервері-учаснику. ДТС оперативно пов'язані через ланцюжки довіри (зазвичай вони називаються шляхами сертифікатів), щоб забезпечити мережу довіри, яка формує поняття «Інфраструктура відкритого ключа» (PKI), надає технічно обґрунтовані та юридично прийнятні засоби для забезпечення:

- сильної перевірки автентичності: контроль автентичності, процесу ідентифікації сторін, що беруть участь у електронних операціях або обмінюються інформацією електронними засобами;
- авторизації: автентифікованого доступу до ресурсів, бази даних та інформаційних систем, відповідно до повноважень, прав та ролей користувача;
- конфіденційності даних: захисту інформації, що локально зберігається або передається, від несанкціонованого доступу;
- цілісності даних: захисту інформації, що локально зберігається або передається від несанкціонованої модифікації PKI в розподіленій інформаційній системі, виграє від з'єднання з каталогом.

Сертифікати, видані засобом PKI, можуть бути використані для забезпечення контролю доступу у веб-середовищі [6]. Прикладом є використання розширеного X.509 сертифікату, який містить інформацію про роль користувача. Ці сертифікати видаються сертифікаційним центром, який діє як довірчий центр у глобальному веб-середовищі. Атрибути сертифікатів містять пару атрибут-значення та принцип, як це застосовується. Вони підписані центрами атрибутів, що зазначені в сертифікаті. Контроль доступу на основі атрибутів забезпечує гнучкість і масштабованість, необхідні для великомасштабних розподілених систем на кшталт хмари.

Простий протокол доступу до каталогу або LDAP – це Інтернет стандарт доступу до служб каталогів, які відповідають стандартам моделі даних X.500. LDAP став найбільш розповсюдженим протоколом в підтримку PKI доступу до служб каталогів для сертифікатів та списків анулювання сертифікатів (CRLs) і часто використовується у веб-сервісах для цілей автентифікації. Каталог для поєднання з PKI може бути використаний для розповсюдження:

• сертифікатів для таких програм, як електронна пошта, в якій сертифікат кінцевого користувача повинен бути отриманий перед тим як зашифроване повідомлення буде відправлено;

• інформація про статус сертифіката, наприклад, списки анулювання сертифікатів (CRL);

• приватні ключі, коли необхідна портативність у середовищі, де користувачі не використовують одну і ту ж робочу станцію кожного дня.

Каталог зберігає зашифровані приватні ключі, які розшифровуються на віддаленій робочій станції, використовуючи пароль, наданий користувачем.

PKI що розгортається разом із механізмами єдиного входу в систему (від англ. Single sign on, надалі – SSO). SSO є ідеальним для розподілених середовищ на кшталт хмари [12]. У середовищі єдиного входу в систему користувачеві не потрібно повторно вводити паролі для доступу ресурси 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 машинах.

Механізми SSO на основі PKI є незамінними в середовищі хмари, оскільки вони забезпечують засоби сильної автентифікація на різних фізичних ресурсах.

Для забезпечення сильної автентифікації користувачів при SSO застосовуються механізми багатофакторної автентифікації.

Багатофакторна автентифікація – це метод автентифікації користувачів, який вимагає більше ніж один фактор верифікації користувача:

- щось, що відомо користувачу (наприклад пароль);
- щось, що належить користувачу (довірений пристрій, який не просто скопіювати, наприклад мобільний телефон, USB-накопичувач[5]);
- біометрія (наприклад відбиток пальця, візуальний образ обличчя, сітківка ока).

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.

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».

Федерація – це група юридичних осіб, які поділяють набір узгоджених політик та правил доступу до онлайнових ресурсів, зокрема у відповідності до стандарту ISO 270001. Федерація забезпечує структуру та правову основу, яка дає змогу проводити автентифікацію та авторизацію в різних організаціях.

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. Федерація забезпечує основу та правову структуру, що дозволяє здійснювати автентифікацію і авторизацію в різних організаціях.

Кінцевий користувач зобов'язаний використовувати свій особистий цифровий сертифікат, щоб автентифікувати себе з хмарним сервісом і підтвердити права доступу до потрібного ресурсу. Цей сертифікат використовується у поєднанні з сертифікатом постачальника послуг (PaaS або IaaS), щоб створити безпечний TLS-зв'язок між ними для шифрування даних.

Висновки

Хмарні обчислення в своїй квінтесенції мають здатність вирішити проблеми, пов'язані з безпекою ІТ, та мінімізувати ряд недоліків традиційних архітектур завдяки своїм унікальним характеристикам, але прийняття цієї інноваційної архітектури може ввести ряд додаткових категорій загроз щодо таких основних якостей безпеки інформації:

- конфіденційність;
- цілісність;
- доступність.

Водночас хмарні реалізації дозволяють застосовувати передові технології забезпечення безпеки, які в основному доступні завдяки централізації даних і універсальним характеристикам архітектури. Однорідність та централізоване управління пулом ресурсів з боку провайдерів хмарних сервісів дозволяє їм сконцентрувати зусилля на забезпеченні безпеки архітектури ІТ. Переваги щодо безпеки включають в себе централізацію, сегментацію даних та процесів, резервування і високу доступність.

Повертаючись до вимог Європейських регуляторів, забезпечення яких важливе в контексті Євроінтеграційних прагнень України, варто також відмітити переваги хмарних технологій, що зазначені нижче:

Впровадження стандартів PCI DSS передбачає забезпечення конфіденційності щодо номерів та інших платіжних реквізитів карток, забезпечення цілісності та криптографічного захисту даних при міжсистемній передачі даних, хешування номерів платіжних карток при відображенні в інтерфейсах користувача. Впровадження комплексного рішення ІТ на основі хмарних технологій дозволить впровадити вимоги PCI DSS із забезпеченням високої ефективності задіяних хмарних сервісів.

Впровадження GDPR потребує значних апаратних ресурсів з огляду на збільшення кількості споживачів сервісів в геометричній прогресії, суттєвих інвестицій в апаратне забезпечення банку для масштабування потужностей в залежності від попиту. Для вирішення цієї проблеми і оптимізації ідеально підходить хмарна інфраструктура. Для використання захищеного транспорту з гарантованою доставкою повідомлень, забезпечення транзакційної цілісності та оптимізації процесу розробки, тестування та впровадження зовнішніх сервісів доцільно використовувати підхід сервісно-орієнтованої архітектури з інтеграцією через корпоративну шину даних (англ. Enterprise service bus) на основі хмарних технологій. Для забезпечення механізмів захисту цілісності та конфіденційності даних при міжсистемній взаємодії доцільно застосовувати TLS 1.2., який рекомендований НБУ.

Впровадження цих стандартів передбачає створення системи управління умовно-постійними даними (англ. Master Data Management). Система має бути в інтегрована в архітектурний ландшафт, стати першоджерелом даних клієнта з інтерфейсами до інших автоматизованих ІС банку для забезпечення дистрибуції оновлень даних клієнта в режимі он-лайн. Такі системи зазвичай працюють з високим навантаженням і потребують значних інвестицій в апаратну інфраструктуру. Для збільшення ефективності доцільно використовувати рішення на основі хмарних технологій. З точки зору безпеки ІТ, першочерговим завданням є забезпечення конфіденційності щодо клієнтських даних, які становлять банківську таємницю, та цілісності даних при міжсистемній взаємодії. Доцільно застосовувати механізми криптографічного захисту даних та захисту «сеансового рівня» взаємодії ІС на транспортному рівні TLS 1.2.

Найбільшої ефективності процесів та механізмів захисту можна досягти, поєднавши хмарні технології з SSO. Для забезпечення SSO на ринку існують багато рішень від лідерів ІТ індустрії, зокрема Microsoft, IBM, Oracle та інших. Але вибір конкретного рішення зале-

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

В будь-якому випадку кожне конкретне впровадження в банківській установі має супроводжуватись підтвердженням відповідності вимог ІБ, зокрема щодо відсутності вразливостей в результаті тестування на проникнення (англ. penetration test), проведеного зовнішньою сертифікованою організацію. Крім того, відсутність вразливостей має бути підтверджена в результаті статичного аналізу вихідного коду (англ. Static Code Review), виконаного зовнішньою спеціалізованою компанією.

Нажаль НБУ не регламентує використання хмарних технологій в банківській діяльності, а останні нормативні документи щодо безпеки IT передбачають виключно периметрові методи захисту, шляхом встановлення мережевих екранів на власному серверному обладнанні, не може бути застосовним щодо хмарних технологій.

З іншого боку, в нормативній документації згадується про створення та ліцензування Центрів Сертифікації Ключів, які виступатимуть в ролі ДТС. Це вірний крок щодо делегування довіри із застосуванням кращих світових практик. Наступним кроком має стати створення Центру сертифікації постачальників хмарних сервісів для банківської діяльності, адже великі американські системні банки, такі як Capital One, вже працюють на хмарних сервісах для забезпечення основних процесів. Сильна автентифікація, забезпечення конфіденційності та цілісності із застосуванням хмарних технологій IdaaS, федерації, SSO з багатофакторною автентифікацією мають стати пріоритетними напрями розвитку безпеки IT для хмарних технологій у банківській діяльності.

Список літератури

1. Зіссіс Д. Адресуючи проблеми безпеки хмарних обчислень / Д. Зіссіс, Д. Леккас // Комп'ютерні системи майбутнього покоління. – 2012. – № 28. – С. 583-592.

2. Андрощук О.С. Багатокритеріальна модель вибору архітектури системи нечіткого логічного висновку для аналізу ризиків безпеки інформації в хмарних обчислювальних та інших складних системах / О.С. Андрощук, А.М. Кудін // Искусств. интеллект. – 2012. – № 4. – С. 529-534.

3. Бобиль В.В. Управління ризиками «хмарних» технологій в системі ризик-менеджменту банку/ В.В. Бобиль // Збірник наукових праць Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна. Проблеми економіки транспорту. – 2014. – Вип. 7. – С. 29-36.

4. Бобиль В.В. "Хмарні" технології як фактор збільшення операційного ризику банку / В.В. Бобиль, М.А. Дронь // Банківська справа. – 2014. – № 11/12. – С. 47-62.

5. Корольов В.Ю. Захист інформації в корпоративних USB-флеш накопичувачах для хмарних обчислень / В.Ю. Корольов // Мат. машини і системи. – 2012. – № 2. – С. 60-69.

6. Кондратьев А.А. Разработка распределенной системы защиты облачных вычислений / А.А. Кондратьев, И.П. Тищенко, В.П. Фраленко // Программные системы: Теория и приложения. – 2011. – № 4(8).

7. OWASP (2018), Open Web Application Security Project website [Електронний ресурс]. – Режим доступу до ресурсу: www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (accessed 17 February 2018).

8. Common Attack Pattern Enumeration and Classification (2018), MITRE corporation website [Електронний ресурс]. – Режим доступу до ресурсу: capec.mitre.org (accessed 17 February 2018).

9. PCI DSS Security standards (2018), PCI DSS Security standards council website [Електронний ресурс]. – Режим доступу до ресурсу: www.pcisecuritystandards.org (accessed 17 February 2018).

10. Payment Service Directive (2018), European Union PSD official website [Електронний ресурс]. – Режим доступу до ресурсу: ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services_en (accessed 17 February 2018).

11. General Data Protection Regulation (2018), European Union Law official website [Електронний ресурс]. – Режим доступу до ресурсу: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (accessed 17 February 2018).

12. Set up Single Sign-On (SSO) (2018), Google corporation website [Електронний ресурс]. – Режим доступу до ресурсу: support.google.com/a/answer/60224?hl=en&ref_topic=6348126&visit_id=1-636156016113854457-157298457&rd=1 (accessed 17 February 2018).

References

1. Zissis, D. and Lekkas, D. (2012), Addressing cloud computing security issues, *Future Generation Computer Systems*, No. 28, pp. 583-592.

2. Androshchuk, O.S. (2012), "Bahatokryterialna model vyboru arkhitektury systemy nechitkoho lohichnoho vysnovku dlia analizu ryzykiv bezpeky informatsii v khmarnykh obchysliuvalnykh ta inshykh skladnykh systemakh" [Multicriteria model of fuzzy logic system architecture selection for analysis of information security risks in cloud computing and other complex systems], *Artificial intelligence*, No. 4, pp. 529-534.

3. 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.

4. 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.

5. 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.

6. 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).

7. OWASP (2018), *Open Web Application Security Project website*, www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (accessed 17 February 2018).

8. Common Attack Pattern Enumeration and Classification (2018), *MITRE corporation website*, www.capec.mitre.org (accessed 17 February 2018).

9. PCI DSS Security standards (2018), *PCI DSS Security standards council website*, www.pcisecuritystandards.org (accessed 17 February 2018).

10. Payment Service Directive (2018), *European Union PSD official website*, www.ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services_en (accessed 17 February 2018).

11. General Data Protection Regulation (2018), *European Union Law official website*, www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (accessed 17 February 2018).

12. Set up Single Sign-On (SSO) (2018), *Google corporation website*, www.support.google.com/a/answer/60224?hl=en&ref_topic=6348126&visit_id=1-636156016113854457-157298457&rd=1 (accessed 17 February 2018).

Надійшла до редколегії 13.02.2018
Схвалена до друку 20.03.2018

Відомості про автора:

Баглай Роман Олегович
аспірант Київського національного
торговельно-економічного університету,
Київ, Україна
https://orcid.org/0000-0002-4067-4929
e-mail: romanbaglai@gmail.com

Information about the author:

Roman Baglai
Doctoral Student of Kyiv National University
of Trade and Economics,
Kyiv, Ukraine
https://orcid.org/0000-0002-4067-4929
e-mail:romanbaglai@gmail.com

УГРОЗЫ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ БАНКОВ

Р.О. Баглай

Проведен анализ угроз безопасности информационных технологий при внедрении облачных вычислений для обеспечения бесперебойной и эффективной деятельности банковских учреждений и предложены меры по минимизации этих угроз. Рассмотрены проблемы и преимущества облачных технологий на различных уровнях архитектурного ландшафта банка для обеспечения конфиденциальности, целостности, подлинности и доступности данных. Результаты исследования могут быть имплементированы путем внедрения соответствующих проектов, обусловленных вызовами и тенденциями банковской сферы, рыночными и регуляторными изменениями.

***Ключевые слова**: ИТ архитектура банка, облачные технологии, проект OWASP, классификация CAPEC, стандарт PCI DSS, директива PSD2, нормативные требования GDPR, стандарт TLS, стандарт SAML, технология SSO, электронная цифровая подпись.*

CLOUD TECHNOLOGY IT SECURITY THREATS FOR BANKS

R. Baglai

Relevance of the subject. Implementation of cloud technology allows to increase efficiency of banking IT by enabling cost saving and improved customer experience. Despite all the benefits there are issues which prevent full scale migration to cloud for banking entities in Ukraine. NBU and legislation limitations, absence of certified trusted cloud service provides and systematic approaches to data and interfaces integrity protection, is not the full list of problems in this area. Banks as entities which store, possess and process personal information subject to banking secrecy are obliged to comply with applicable European, international and national legislation. Considering Euro integration strategic roadmap Ukraine has to adopt European and international requirements as PCI DSS, PSD2, GDPR which is a heavy burden for traditional IT architecture of the bank unless innovative cloud technology is applied. Cloud infrastructure also triggers number of regulatory issues related to confidentiality of client data, as data is physically stored in remote geographical locations out of direct control of respective bank. Such peculiarity is in conflict with the principle that the bank should be in control of customer data in real time. Purpose of the article is to define feasible measures to mitigate the risks related to IT security defined by special features of cloud architecture considering national and European requirements for Banks. Methodological basis of research is modern theoretical methods and systematic approach to design, build, integration and support of cloud service oriented architecture, as well as OWASP and CAPEC standard approaches to cyber attack classification. To address the issues raised it is necessary to ensure strong authentification establish domains of trust, delegate trust to verified third parties and protect the communication channels with modern cryptography means.

***Keywords:** IT architecture of a Bank, cloud technology, OWASP project, CAPEC classification, PCI DSS standard, PSD2 directive, GDPR regulation, TLS standard, SAML standard, SSO technology, Eelectronic digital signature.*