УДК 336.71+004.78+65.001.3

Андрушків І.П.,
к.е.н., доцент кафедри фінансово-економічної
безпеки та банківського бізнесу,
Мушинський Б.М.*,
аспірант кафедри фінансово-економічної безпеки
та банківського бізнесу,
Львівський торговельно-економічний університет

ВПЛИВ ІТ ТА КІБЕР-РИЗИКІВ НА БАНКІВСЬКУ ДІЯЛЬНІСТЬ

Постановка проблеми. На сучасному етапі банківські установи повинні брати до уваги ще донедавна специфічні ризики, а саме ІТ та кібер-ризики, Оскільки з розвитком технологій, цей вид ризику стає все актуальнішим.

За статистикою, кожен день все нові організації стають жертвою кібер-атак. Зазвичай це втрата корпоративних даних, інтелектуальної власності або даних клієнтів, фінансові деталі - чи в гіршому випадку іноді все перелічене. Тому необхідно зрозуміти, де існують основні кібер-ризики, як їх виявити і як захистити себе від цієї зростаючої загрози, зберігаючи адекватний рівень затрат. Як наслідок вище зазначеного, зростає актуальність питань, які стосуються кібер-безпеки банку, яка охоплює все те, що захищає від умисних атак, порушень, ІТ інцидентів та їх наслідків.

Аналіз останніх досліджень і публікацій. Вплив ІТ та кібер-ризиків на діяльність банків досліджували у своїх працях такі науковці, як: В. Н. Вяткін, І. В. Вяткін, В. А. Гамза, А. О. Недосєкін, К. Е. Павлов, З. І. Абдулаева, О. Яновський, A. Allison, C. Williams, A. Chatzilia, M. Willsher, R. Anderson, P. Hopkins, W. Holt, J. Duffer та ін. Водночас необхідно зазначити, що недостатньо висвітленими є питання управління кібер-рииками та пріоритетів розвитку ризик-менеджменту в частині кібер-ризиків.

Постановка завдання. Мета дослідження – обґрунтувати вплив ІТ та кібер-ризиків на діяльність банків та окреслити основні тенденції розвитку кібер-безпеки; вивчити міжнародну практику застосування превентивних засобів захисту від кібер-ризику та запропонувати основні кроки у побудові кібер-захисту на основі міжнародних рекомендацій.

Виклад основного матеріалу дослідження. Під ІТ та кібер-ризиком мається на увазі будь-який ризик, що призводить до фінансових втрат, знищення або погіршення репутації банку у результаті виходу з ладу ІТ систем, систем інформаційної безпеки. Такий ризик може матеріалізуватися наступними способами:

– навмисне та несанкціоноване порушення безпеки, для отримання доступу до інформаційних систем з ціллю шпигунства, вимагання або нанесення репутаційної шкоди;

– ненавмисне або випадкове порушення безпеки, яке тим не менш, може призвести до певних матеріальних та нематеріальних втрат;

– операційні ІТ-ризики за рахунок низької цілісності системи або інших факторів.

Банки повинні не тільки реагувати на інциденти, які відбувається з ними безпосередньо, але й враховувати вплив ключових компаній в їхньому ланцюзі поставок.

Як зазначають вчені [6], невпинно зростає частка постачальників аутсорсингових сервісів, зокрема «хмарні» рішення. Використовуючи ці сервіси, профіль ризику банку не зменшується і не збільшується; ефективно контрольоване середовище, мігруючи у хмару, буде, при незмінних елементах і системі контролів, як і раніше ефективно контрольоване, в той час як недостатньо контрольоване середовище мати низку ІТ ризиків і загроз незалежно від вибору своєї інфраструктури.

Нові способи роботи приносять нові можливості, але в той же час нові ризики. Бізнес переваги, які надаються корпораціям за допомогою хмарних обчислень, BYOD (bring your own device), соціальних медіа та "інтернету речей" несуть в собі ряд нових ризиків, а також в результаті чого існуючі ризики аналогічно розвиваються. Відстеження цього факту у швидко розвиваючому світі, зберігаючи при цьому гнучкість реагування, є непростим завданням для сучасних банків. Ризик-менеджмент повинен проводитись з часткою креативності, потрібно знаходити баланс між побажаннями користувачів та вимогами самого банку.

Через те, що ризики пов'язані з кібер-діяльністю, зокрема використання інтернет, є відносно новими – багато вітчизняних банків не мають досвіду у розумінні або боротьбі з ними. Але базуючись

* *Наук. керівник: Андрушків І.П. - к.е.н., доц.*

на сучасному досвіді та повідомленнях урядових служб та спеціальних організацій з захисту інформації – ніхто не застрахований перед цими ризиками [8].

Важливо також відмітити, що цілком неправильно вважати ніби маленькі банки мають імунітет до кібер-ризиків – існує зростаюча статистика випадків таких атак, саме через слабку захищеність перед зловмисниками.

Одним із варіантів управління IT ризиками є передача цього виду ризику страховим компаніям. Проте це також не є панацеєю, оскільки страхові не покривають цей ризик повністю.

На думку Richarda Andersona [1], з якою варто погодитись, страхове відшкодування може включати в себе витрати на:

– проведення експертизи для визначення тяжкості і обсягу порушення;
– повідомлення осіб, які постраждали від порушення;
– робота фахівця колл-центру для врегулювання запитів від постраждалих осіб;
– робота PR-компанії для надання професійних консультацій;
– юридичні витрати, виплати по відшкодуванню збитків та урегулюванню суперечок.

Відповідно, банк все ж буде нести витрати через репутаційний збиток, втрату клієнтів, девальвацію акцій, витрати на заходи щодо виправлення становища, IT-витрати на модернізацію. Таким чином накопичені витрати можуть перевищити застраховані втрати у кілька десятків разів.

Отже, страхування відіграє важливу роль, але не покриває реального збитку від кібер-загроз. Послідовна та розширена програма аналізу ризиків, для ідентифікації та вжиття необхідних заходів, призначена зберегти значну суму витрат, спровокованих кібер-ризиком.

Що стосується регулювання кібер-ризиків, то у банківській сфері даний ризик регулюється вимогами до достатності капіталу під операційний ризик, так як IT та кібер-ризики є частиною операційних [3]. Відповідними категоріями, які несуть в собі ці ризики, є зовнішнє шахрайство (інколи внутрішнє), порушення у роботі сервісів та системні збої. Зважаючи на неспішне впровадження в Україні вимог Базелю II та III, вимог до капіталу, які б включали частину капіталу під кібер-ризики, – вітчизняні банки не захищені від даного ризику, допоки з власної ініціативи не будуть відповідати даним вимогам.

Згідно дослідження GCHQ (Центр урядового зв'язку Великобританії), близько 80% кібер-атак на сьогодні можна було б зупинити базовими принципами управління інформаційної безпеки. З точки зору практичного застосування, виділено 10 основних кроків, які повинна прийняти організація для впровадження ефективного управління інформаційною безпекою, а саме:

Крок 1. Створення режиму управління інформаційною безпекою. Банк повинен мати чітке бачення управління, повинно бути призначено кваліфікованих фахівців, розроблено документарне забезпечення інформаційної безпеки, впроваджено міжнародні стандарти та найкращі світові практики, структура звітування, популяризовано культуру інформаційної безпеки на рівні вищого керівництва.

Крок 2. Безпечні конфігурації/ налаштування. Банк повинен слідкувати за використанням останніх версій ПЗ, повинна бути створена система управління оновленнями, завжди мати додаткові (запасні) засоби hardware і software, обмежити коло дозволених засобів записування/зчитування, обмежити права користувачів на адміністрування та внесення змін, створити закрите коло мережі (з використанням власних серверів, роутерів та інших мережевих засобів), виконувати регулярні сканування на наявність недоліків (vulnerability scans), створити білий список програмного забезпечення і обмежити використання ПЗ, яке напряму не потрібне для бізнесу.

Крок 3. Безпека мережі. Необхідні дії: впровадження політик роботи внутрішньої та зовнішньої мереж, використання антивірусів/антиспам систем/ malware-protection систем, інвентаризація усіх мережевих активів, використання шифрованих каналів зв'язку для зовнішніх з'єднань, захист внутрішніх IP адрес від стороннього використання, захист або обмеження Wi-Fi мережі, моніторинг використання мережі, проведення регулярних тестувань на проникнення.

Крок 4. Управління правами доступу. Для управління правами доступу, в банку, як мінімум, повинно бути наступне: розроблено ефективний процес аккаунт-менеджменту, обмежено кількість користувачів з привілейованими правами, моніторинг всіх користувачів, розроблено політику та стандарти доступу та ідентифікації, обмежено доступ до матеріалів аудиту та логів інформаційних систем, розвиток обізнаності в інформаційній безпеці.

Крок 5. Навчання та обізнаність користувачів. Найуразливішою частиною банку, з точки зору кібер-атак, є персональна складова, в той же час – персонал є найважливішим активом кожної компанії. Саме тому необхідно розробити процес обізнаності нового персоналу, процес проведення нагадувальних навчань, підтримка розвитку IT спеціалістів з використання міжнародних сертифікатів по інформаційній безпеці, забезпечити систему звернень та відгуків, запровадити формальний процес дисциплінарних покарань.

Крок 6. Управління інцидентами. Профіль ризику банку визначатиме тип і характер можливих інцидентів. Сама система управління повинна включати такі компоненти: побудова відповідної структури відповідальності та обізнаності на рівні вищого керівництва, розробка процедури реагування на інциденти та можливості аварійного відновлення, навчання для команди відновлення роботи,

впровадження програм безперервності ведення бізнесу, визначення чітких ролей залучених спеціалістів та кризових менеджерів, розробка можливості відновлення критичних даних, тестування планів відновлення, аналіз результатів тестування.

Крок 7. Захист від шкідливого програмного забезпечення (malware prevention). Банк повинен забезпечити наявність наступних компонентів попередження інцидентів: розробка та публікація політик, які передбачають використання довірених програмних засобів та процедуру аналізу нового ПЗ, використання anti-malware клієнтів, регулярне сканування на шкідливе ПЗ, управління всіма вхідними та вихідними потоками інформації, навчання та підняття обізнаності для користувачів ПЗ.

Крок 8. Моніторинг. Цей крок дозволяє реагувати на ранні трігери інциденту та забезпечує превентивну функцію. Компанія повинна забезпечити такі засоби моніторингу: розробка моніторингової стратегії, моніторинг всіх ICT систем (NIDS/HIDS, системи попередження), моніторинг мережевого трафіку, моніторинг всієї активності користувачів, забезпечення достатнього об'єму пам'яті, навчання для працівників з інформаційної безпеки, процедура регулярного перегляду нормативних вимог банку щодо системи управління інформаційною безпекою.

Крок 9. Контроль та управління з'ємними пристроями. Найпершим пунктом цього етапу можна назвати формування політики та загального підходу до використання та передавання інформації на зовні. Відповідно до визначених орієнтирів також необхідно обмежити кількість використання з'ємних пристроїв до мінімуму, сканувати з'ємні пристрої на наявність шкідливого ПЗ та вірусів, проводити регулярну інвентаризацію цих пристроїв, шифрувати інформацію, яка зберігається на з'ємному пристрої, блокувати за замовчуванням доступ до таких пристроїв, моніторити систему на використання несанкціонованих з'ємних пристроїв, управління повторним використанням утилізованих пристроїв (re-usage).

Крок 10. Робота з дому та використання мобільних пристроїв. Використання цього кроку включає такі компоненти, як: оцінка ризиків та створення політики використання мобільних пристроїв, перед наданням дозволу використання мобільних пристроїв проводити навчання з обізнаності у питаннях інформаційної безпеки, шифрування каналу передачі даних (VPN), обмеження об'єму та типу передачі даних на мобільні пристрої (storage limit), шифрування даних на мобільному пристрої, регулярний перегляд планів реагування на інциденти [7].

Цей перелік необхідних кроків є обов'язковим для впровадження у банківських установах, так як саме вони піддаються кібер-ризикам в найбільшій мірі. Шахраї можуть порушити систему кібер-безпеки банку з різними цілями: крадіжка коштів клієнтів, доступ до конфіденційної інформації з метою продажу, доступ до комерційної таємниці банку, крадіжка персональних даних з метою шантажу і вимагання, задоволення власних амбіцій, політичні чи релігійні переконання та ін. Реагувати на порушення системи кібер-безпеки банку є вкрай важко та витратно, тому необхідно вживати максимум превентивних заходів, для упередження кібер-атак.

В Україні існують власні вимоги до банків щодо системи управління інформаційною безпекою (СУІБ), які включають вимоги до менеджменту та працівників банку щодо прав доступу, регулярних оцінок та тестувань інформаційних активів. В межах перевірок НБУ банки повинні підтверджувати виконання вимог СУІБ та вживати всіх необхідних заходів для упередження збоїв та порушень системи інформаційної безпеки установи [2].

Для банку необхідно чітко побудувати СУІБ та виділити достатню кількість спеціалістів з інформаційної безпеки, кібер-злочинництва, запобігання шахрайству та мережевих технологій. Основним методом боротьби з кібер-ризиком є створення превентивних бар'єрів для ймовірних атак, забезпечення надлишків потужностей (для надзвичайних подій), бекапування критичних даних, проведення стрес-тестування, регулярний аудит.

За даними ISACA (Асоціація Аудиту та Контролю Інформаційних Систем), 2016 рік нестиме 5 основних трендів розвитку кібер-ризиків та, відповідно, кібер-безпеки.

1. Кібер-вимагання, використовуючи ігрові системи, медичні системи, інтернет-речі.
2. Збільшення хакерських атак на хмарні сервіси.
3. Жорсткіші вимоги користувачів до безпеки персональних даних.
4. Шкідлива реклама та шкідливе програмне забезпечення для мобільних пристроїв досягне загрозливих масштабів.
5. Різниця між навиками спеціалістів у кібер-безпеці та зловмисниками [4].

Варто зазначити і те, що компанією Munich Re America було проведене опитування щодо страхового покриття кібер-ризиків, і 82% опитуваних вважають, що у 2016 році страхові поліси по покриттю кібер-ризиків є адекватними щодо ціни та покриття загроз, а 77% відповіли, що вже мають або забезпечать себе страховими полісами на наступні 12 місяців [5].

Зважаючи на стійкі тренди боротьби з кібер-ризиками, на українському ринку все ще мало розвинута культура ризик-менеджменту, особливо у банків з вітчизняним капіталом. Результатом цього може бути низка скандальних справ з компрометацією даних або й з викраденням коштів з клієнтських рахунків, що аж ніяк не додасть балів нашій банківській системі серед населення та у світі.

Висновки з проведеного дослідження. Зважаючи на стрімкий розвиток технологій, використання у роботі новітніх пристроїв обробки даних та мобільних пристроїв, – кібер-загрози постають проблемою і об'єм цієї проблеми змушує звернути на себе увагу. Багато банків вкладають кошти у технологію, а не у інвестиції зі зменшення ризику. Як результат, немає повного розуміння специфіки схильності до кібер-ризику, вартості витрат на врегулювання ризику та потенціал репутаційного збитку. При управлінні даним ризиком банк повинен відповісти на запитання: «яка пріоритетність цього ризику для нас та який розмір інвестицій ми готові вкласти у засоби попередження, виявлення та реагування?».

Для формування успішної системи управління інформаційною системою необхідно вкладати досить великі кошти у цей напрямок менеджменту. Для збереження активного реагування на новітні загрози та підтримку якісного управління необхідні також кваліфіковані працівники як з точки зору безпеки, так і з точки зору IT. Дана загроза не сприймається більшістю українських компаній серйозно, оскільки оцінити кібер-ризик кількісно є досить складно (так як і решту операційних ризиків), а якісна оцінка базується на попередньому досвіді та експертній оцінці. Відповідно, увага до кібер-атак та IT інцидентів привертається лише після вже реалізованих втрат, які для багатьох фінансових установ можуть бути катастрофічними і призвести до закриття бізнесу.

Підсумувавши вищевказане, можна стверджувати, що управління IT та кібер-ризиками чутливих інформаційних активів та систем є одним з найвищих пріоритетів для більшості компаній.

Бібліографічний список

1. Richard Anderson Cyber Risk Executive Summary // Institute of Risk Management [Електронний ресурс]. – Режим доступу : https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf

2. Вяткин В.Н. Риск-менеджмент / В.Н. Вяткин, И.В. Вяткин, В.А. Гамза. – М. : Издательско-торговая корпорация "Дашков и К", 2012 – 512 с.

3. Грабовой П.Г. Риски в современном бизнесе / П.Г. Грабовой. – М. : Аланс, 2014. – 240 с.

4. Joanne Duffer ISACA Identifies Five Cyber Risk Trends for 2016 [Електронний ресурс]. – Режим доступу : http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Identifies-Five-Cyber-Risk-Trends-for-2016.aspx

5. Adrian Ladbury Risk managers seek to buy more cyber cover finds // Commercial RiskEurope [Електронний ресурс]. – Режим доступу : http://www.commercialriskeurope.com/cre/3317/56/Risk-managers-seek-to-buy-more-cyber-cover-finds-Munich-Re-survey/

6. Недосекин А.О. Стратегический подход к управлению рисками корпорации / А.О. Недосекин, К.Е. Павлов, З.И. Абдулаева // Стратегический менеджмент. – 2008. – № 4. – С. 94-97.

7. Reducing the Cyber Risk in 10 Critical Areas [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf

8. 2014 ISACA Annual Report [Електронний ресурс]. – Режим доступу : http://www.isaca.org/About-ISACA/annual-report/Pages/default.aspx.

References

1. Anderson, Richard (2015), "Cyber Risk Executive Summary", available at: https://www.theirm.org/media/883443/Final_IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf (access date May 10, 2016).

2. Viatkin, V.N., Viatkin, I.V. and Gamza, V.A. (2012), *Risk-menedzhment* [Risk-management], Izdatelsko-torgovaia korporatsiia "Dashkov i K", Moscow, Russia, 512 p.

3. Grabovoy, P.G. (2014), *Riski v sovremennom biznese* [Risks are in modern business], Alans, Moscow, Russia, 240 p.

4. Duffer, Joanne (2016), "ISACA Identifies Five Cyber Risk Trends for 2016", available at: http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Identifies-Five-Cyber-Risk-Trends-for-2016.aspx (access date May 11, 2016).

5. Ladbury, Adrian (2016), "Risk managers seek to buy more cyber cover finds", available at: http://www.commercialriskeurope.com/cre/3317/56/Risk-managers-seek-to-buy-more-cyber-cover-finds-Munich-Re-survey/ (access date May 10, 2016).

6. Nedosekin, A.O., Pavlov, K.E and Abdulaeva, Z.I. (2008), "A strategic approach to corporate risk management", *Strategicheskiy menedzhment*, no. 4, p. 94-97.

7. Reducing the Cyber Risk in 10 Critical Areas (2016), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf (access date May 10, 2016).

8. 2014 ISACA Annual Report, (2015), available at: http://www.isaca.org/About-ISACA/annual-report/Pages/default.aspx (access date May 10, 2016).

Андрушків І.П., Мошинський Б.М. ВПЛИВ ІТ ТА КІБЕР-РИЗИКІВ НА БАНКІВСЬКУ ДІЯЛЬНІСТЬ

Мета – обґрунтувати вплив ІТ та кібер-ризиків на діяльність банків та окреслити основні тенденції розвитку кібер-безпеки; вивчити міжнародну практику застосування превентивних засобів захисту від кібер-ризику та запропонувати основні кроки у побудові кібер-захисту на основі міжнародних рекомендацій.

Методика дослідження. В основу досліджень роботи покладені як загальнонаукові (аналіз, спостереження), так і спеціальні методи пізнання. Методи аналізу і спостереження використані для дослідження основних тенденцій розвитку кібер-безпеки. Методи пізнання використані для обґрунтування впливу ІТ та кібер-ризиків на діяльність банків.

Результати. Доведено, що питання, які стосуються кібер-безпеки банку, яка охоплює все те, що захищає від умисних атак, порушень, ІТ інцидентів та їх наслідків та напрямів їх вдосконалення, на сучасному етапі набувають особливої актуальності.

Обґрунтовано, що банки повинні не тільки реагувати на інциденти, які відбуваються з ними безпосередньо, але й враховувати вплив ключових компаній в їхньому ланцюзі поставок.

Встановлено, що одним із варіантів управління ІТ ризиками є передача цього виду ризику страховим компаніям. Встановлено, що страхування відіграє важливу роль, але не покриває реального збитку від кібер-загроз. Послідовна та розширена програма аналізу ризиків, для ідентифікації та вжиття необхідних заходів, призначена зберегти значну суму витрат, спровокованих кібер-ризиком.

Зроблено висновок, що зважаючи на неспішне впровадження в Україні вимог Базелю ІІ та ІІІ, вимог до капіталу, які б включали частину капіталу під кібер-ризики, – вітчизняні банки не захищені від даного ризику, допоки з власної ініціативи не будуть відповідати даним вимогам.

З точки зору практичного застосування, виділено 10 основних кроків, які повинна здійснити організація для впровадження ефективного управління інформаційною безпекою, які є обов'язковим для впровадження у банківських установах, так як саме вони піддаються кібер-ризикам в найбільшій мірі.

Наукова новизна. Обґрунтовано на основі методів пізнання вплив ІТ та кібер-ризиків на діяльність банків та окреслено основні тенденції розвитку кібер-безпеки.

Практична значущість. Результати дослідження можуть бути запропоновані для впровадження у діяльності банків, що сприятиме ефективному управлінню інформаційною безпекою.

Ключові слова: кібер-ризик, ІТ-ризик, ризик-менеджмент, кібер-безпека, інформаційні системи, програмне забезпечення, антивірус, інциденти.

Andrushkiv I.P., Mushynskyi B.M. INFLUENCE OF IT AND CYBERBUCK – RISKS ON BANK ACTIVITY

Purpose is to influence of the IT and cyber risk in the banks and outline the major trends in cyber security; study the international practice of proactive protection against cyber-risk and offer basic steps in building a cyber-defense based on international guidelines.

Methodology of research. The basis of the research work assigned as general (analysis, observation) and special methods of cognition. Methods of analysis and observation used to study the basic trends of cyber-security. Methods of knowledge used to study the impact of IT and cyber risks for banks.

Findings. Proved that issues relating to cyber-security bank that covers all that protects against intentional attacks, breaches, IT incidents and their consequences, and areas of improvement at this stage is particularly important.

Proved that the banks must not only respond to incidents that happen to them directly, but also consider the impact of key companies in their supply chain.

One of the options for management of IT risk management is to transfer this type of risk insurance companies. Found that insurance plays an important role, but does not cover the real damage from cyber threats. Consistent and expanded application of risk analysis to identify and take necessary measures, designed to save a substantial amount of costs provoked by cyber risk.

It was concluded that despite the leisurely introduction in Ukraine of Basel II and III, capital requirements, which would include part of the capital in cyber risks - domestic banks are not immune from this risk, unless their own initiative will not meet these requirements.

In terms of practical application, selected 10 key steps that should take the organization to implement effective information security management that is required for implementation in banking institutions, as they are exposed to cyber risks to the greatest extent.

Originality. Grounded based methods of learning impact of IT and cyber risk in the banks and outlines the major trends in cyber security.

Practical value. Research results can be offered for introduction in activity of banks, which will be instrumental in an effective management informative safety.

Key words: Cyber risk, IT risk, risk management, cyber security, information systems, software, antivirus incidents.

Андрушкив И.П., Мушинский Б.М. ВЛИЯНИЕ IT И КИБЕР-РИСКОВ НА БАНКОВСКУЮ ДЕЯТЕЛЬНОСТЬ

Цель – обосновать влияние ИТ и кибер-рисков на деятельность банков и определить основные тенденции развития кибер-безопасности; изучить международную практику применения превентивных мер защиты от кибер-риска и предложить основные шаги в построении кибер-защиты на основе международных рекомендаций.

Методика исследования. В основу исследований работы положены как общенаучные (анализ, наблюдение), так и специальные методы познания. Методы анализа и наблюдения использованы для исследования основных тенденций развития кибер-безопасности. Методы познания использованы для обоснования влияния IT и кибер-рисков на деятельность банков.

Результаты. Доказано, что вопросы, касающиеся кибер-безопасности банка, которая охватывает все то, что защищает от умышленных атак, нарушений, IT инцидентов и их последствий и направлений их совершенствования на современном этапе приобретают особую актуальность.

Обосновано, что банки должны не только реагировать на инциденты, которые происходят с ними непосредственно, но и учитывать влияние ключевых компаний в их цепи поставок.

Одним из вариантов управления IT рисками является передача этого вида риска страховым компаниям. Установлено, что страхование играет важную роль, но не покрывает реального ущерба от кибер-угроз. Последовательная и расширенная программа анализа рисков, для идентификации и принятия необходимых мер, предназначена сохранить значительную сумму расходов, спровоцированных кибер-риском.

Сделан вывод, что несмотря на медленное внедрение в Украине требований Базеля II и III, требований к капиталу, которые включали часть капитала под кибер-риски, – отечественные банки не защищены от данного риска, пока по собственной инициативе не будут соответствовать данным требованиям.

С точки зрения практического применения, выделено 10 основных шагов, которые должна осуществить организация для внедрения эффективного управления информационной безопасностью, которые являются обязательным для внедрения в банковских учреждениях, так как они подвергаются кибер-рисков в наибольшей степени.

Научная новизна. Обоснованно на основе методов познания влияние IT и кибер-рисков на деятельность банков и очерчено основные тенденции развития кибер-безопасности.

Практическая значимость. Результаты исследования могут быть предложены для внедрения в деятельность банков, которая будет способствовать эффективному управлению информационной безопасностью.

Ключевые слова: кибер-риск, IT-риск, риск-менеджмент, кибер-безопасность, информационные системы, программное обеспечение, антивирус, инциденты.