ФІНАНСИ, ПОДАТКОВА СИСТЕМА ТА ІНВЕСТИЦІЙНА ДІЯЛЬНІСТЬ

УДК 336.71:004.056:34

ЕЛЕМЕНТИ КІБЕРЗАГРОЗ БАНКІВ В РАМКАХ СИСТЕМИ ФІЛЬТРАЦІЇ ТА ОЧИЩЕННЯ ЗОВНІШНЬОГО СЕРЕДОВИЩА

Богославський М.Ю.
Національна академії управління

В статті розглянуто складові та пріоритети процесу організації кібервтручання в комерційний банк, які з позиції зовнішнього середовища поділено на структурні елементи та напрями процесу кібератаки.

Розподіл послідовності процесів фільтрації вхідної загрози методом очищення інформаційного середовища на нашу думку є найбільш ефективним в рамках забезпечення фінансової безпеки банку. Для внутрішньої обробки системи фільтрації загроз банку пропонується класифікувати інциденти в залежності від порушених операційних і технологічних процесів, скорегованих на обсяги потенціальних наслідків.

Уточнено технологічні складові кіберзагроз на вітчизняному ринку та інструментів для їхньої протидії з позиції нормативно-технічного та програмного забезпечення банку. Віднесено зловживання повноваженнями персоналу як процесом неконтрольованим за рахунок технологічної фільтрація, причому припущено що ефективний аналіз можливо отримати лише на базі біхевіористичного аналізу персоналу банку.

Ключові слова: фільтрація загроз банку, забезпечення фінансової безпеки банку, пентестер, структурні елементи кібератаки, напрями, розподіл послідовності процесів, класифікація інцидентів

UDC 336.71:004.056:34

BANKS' CYBERATTACK STRUCTURE IN THE SYSTEM OF FILTRATION AND CLEARANCE OF THE EXTERNAL ENVIRONMENT

Bogoslavskij N.
National academy of management

The article researches the components and priorities of the process of organizing cyber intervention in a commercial bank, which is divided into the structural elements and directions of the cyber-attack process. The sequence distribution of filtering incoming threats by the method of cleaning the information environment is the most effective in our opinion while ensuring the financial security of the bank. In order of internal bank's filtration system processing it was proposed to classify incidents depending on the disturbed operating and technological processes corrected for the scope of potential consequences.

© **Богославський М.Ю., 2017**

The technological components of cyber threats on the domestic market and the tools for their counteraction from the position of normative and technical software of the bank are specified. Uncontrollable process created by the staff through technological filtration wasn't assumed, but for an effective analysis may be obtained only on the basis of behavioral analysis of the bank's staff.

***Keywords*:** filtration of bank threats, financial security of the bank, pentester, structural elements of cyberattacks, directions, distribution of sequence of processes, classification of incidents.

Актуальність проблеми. В процесі удосконалення систем протидії кіберзагрозам комерційному банку важливо зосередитися на аналізі середовища де виникають такі небезпеки. Інформаційний розвиток банків окрім маркетингових та комунікаційних активностей має долучати оповіщення загальних, прецедентних та специфікованих загроз, які породжують додаткові заходи з хеджування ризиків у контексті забезпечення фінансової безпеки банку. Розробка заходів та прийняття дієвих рішень керівництвом служби безпеки банку та топ-менеджменту є неможливим без спрямованих на стратегії забезпечення фінансової безпеки банку як в короткостроковому, так і в довгостроковому періодах, відповідно дані аспекти потребують подальшого удосконалення.

Аналіз останніх наукових досліджень. Розробки фінансистів за даною тематико є здебільше теоретичними та малозастосованими через інклюзивність кожного окремого випадку кібратаки, проте обчислення та прогнозування фінансових втрат, організація діяльності фінансової установи, відповідний макроекономічний аналіз середовища небезпек та проведення фінансового контролінгу за напрямами порушень фінансової безпеки є набором тих інструментів, при вчасній реакції на які може підвищитись загальна ефективність роботи комерційного банку. Серед вітчизняних вчених які досліджували поточну проблематику можемо відзначити В. Ткаченко, С. Хвалінського, В. Хорошко, А. Піскозуб А. Войціховського, С. Семенова, В. Домушев, С. Барановського, В. Домарєва, Т. Чернадчук, проте виходячи із активного розвитку технологій вивчення структури адаптованих кіберзагроз та методів їх блокування потребують нових удосконалень. Процес очищення інформаційного середовища банку буде значно ефективнішим в разу детермінації структурних елементів та напрямів безпосереднього процесу кібератаки.

Метою роботи є визначення структурних елементів та напрямів процесу кібератаки на банк з метою підвищення ефективності фільтрації вхідних загроз за рахунок очищення інформаційного середовища.

Викладення основного матеріалу дослідження. Ефективне забезпечення фінансової безпеки(ФБ) банків у контексті протидії кібератакам та несанкціонованим видам втручання третіх сторін передбачає дослідження структурних елементів та напрямів потенційного враження при паралельній ідентифікації ризиків і пов'язаних з ними похідних видів небезпек; детермінацію поточного супротиву ризикам та порогових значень індикаторів ФБ банку; реалізація заходів з відбору та відсіювання потенційних загроз при паралельних актуарних розрахунках щодо втрат банку[1,2].

Також слід зазначити, що розповсюдження спектра фінансових послуг, які надаються банками, залежить від відсутності у міжнародних банків контрольного пакета акцій державних банків. Зазначимо структурні елементи та напрями активної реалізації кібератак під час фінансово-господарської діяльності банків на рис. 1.

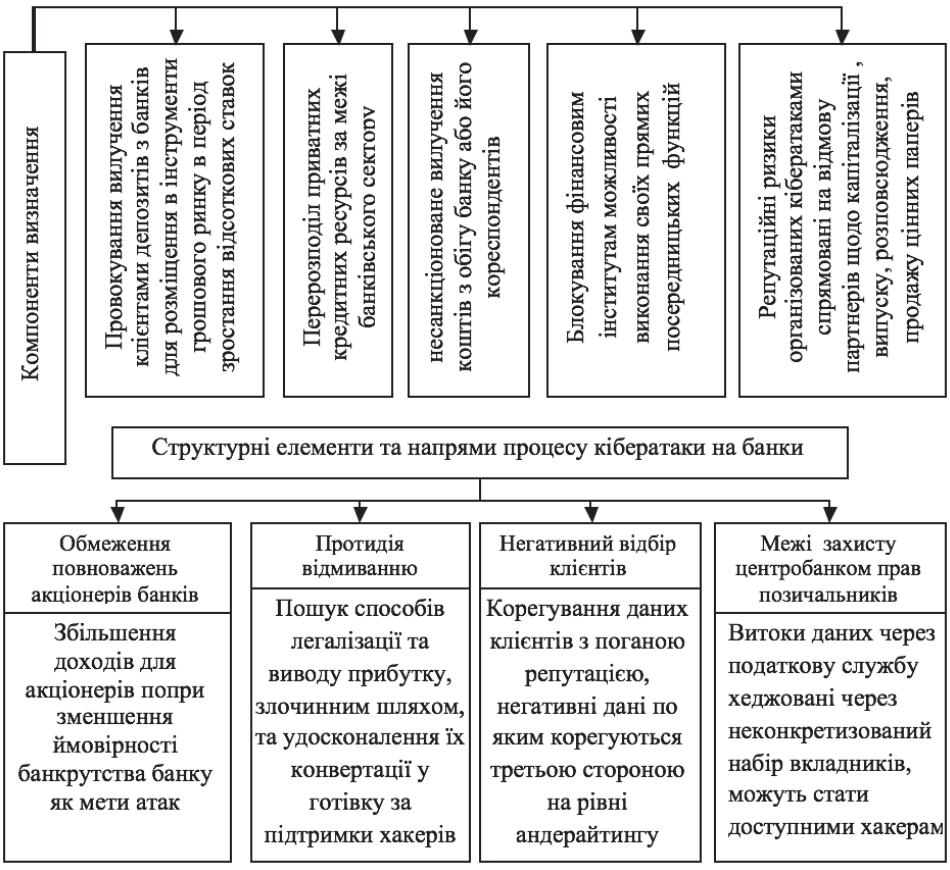

***Рис. 1**. Структурні елементи та напрями процесу кібератаки*
Складено автором на основі [3,4]

Стандартне провадження контролю по запланованим заходам є недостатнім, оскільки структура і форми кіберзагроз весь час видозмінюються, потребуючи колегіального дослідження та моніторингу з боку груп реагування – профільних служб банку. Корегування проникнення загроз у фінансовому сенсі проходить за рахунок списання коштів на відшкодування за напрямами втрат, збільшуючи чистий збиток банку. Тому превентивізація у даному сенсі полягає при ідентифікації загроз банку і корегування індикаторів залежно від зміни структурних елементів кібергазроз та видозмінених технічних умов роботи банку з урахуванням волатильності зовнішнього середовища[6].

Проведемо розподіл послідовності процесів фільтрації вхідної загрози методом очищення інформаційним середовищем в рамках ФБ банку, який зображено на рис. 2.

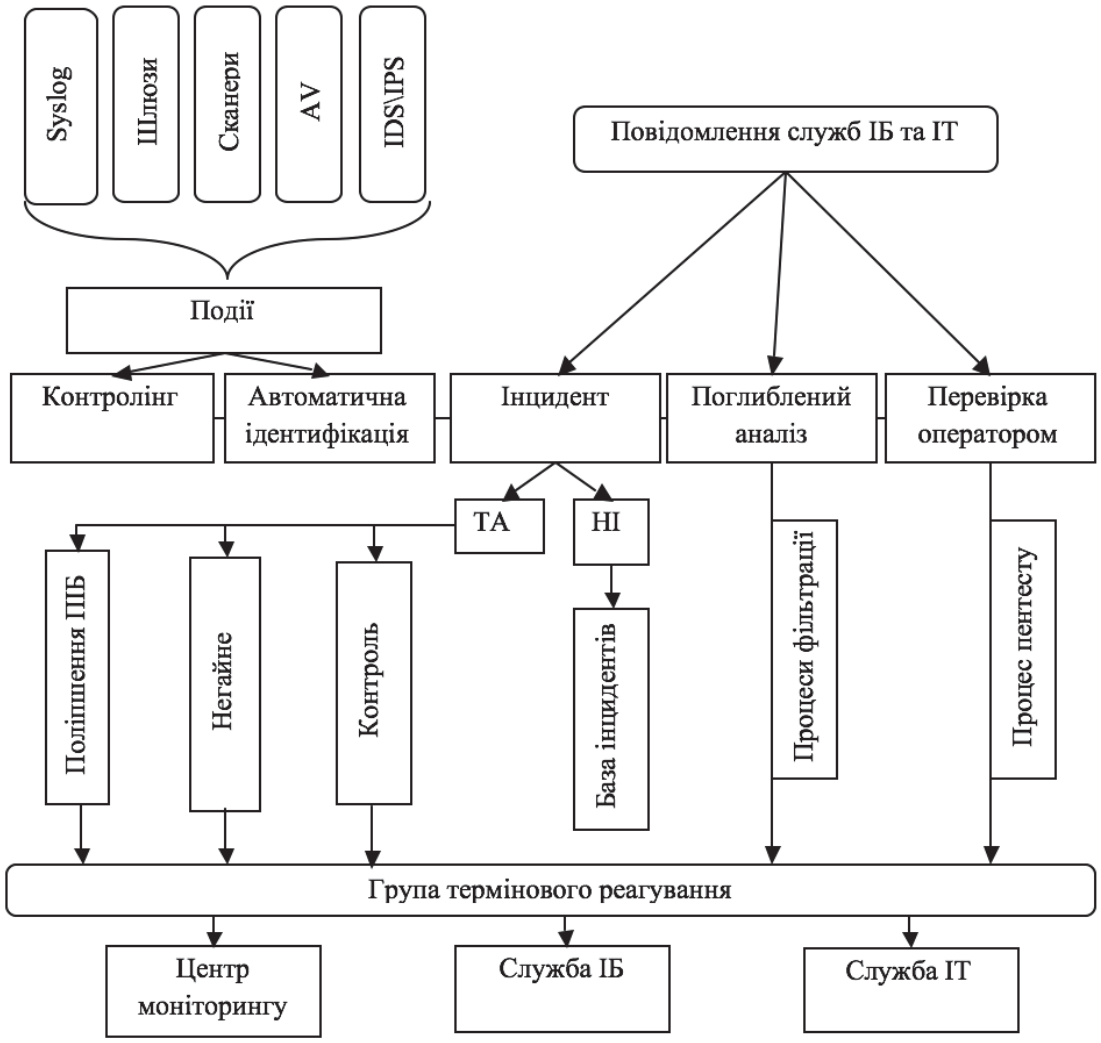

Рис. 2. *Розподіл послідовності процесів фільтрації вхідної загрози методом очищення інформаційним середовищем в рамках ФБ банку*
Джерело: [5]

У системі управління інцидентами головною сутністю є картка інциденту, в якій збирається вся пов'язана з інцидентом інформація і з якою працюють співробітники центра моніторингу та співробітники групи реагування на стороні замовника.

Чергова зміна центра моніторингу отримує оповіщення про виявлений інцидент в реальному часі в інтерфейсі Системи управління інцидентами. Відповідальний персонал комерційних банків, інформаційні системи яких підключені до центру моніторингу, отримують оповіщення по пошті, через смс або телефону згідно рольової моделі [2].

На фазі фільтрації загроз та імплементації пентестів операторами служби ІТ, андерайтингом, службою безпеки та фінансового моніторингу, представники яких входять до групи термінового реагування, формується режим та пріоритетність реагування з відповідною підбіркою інструментів протидії.

В рамках розподілу послідовності процесів фільтрації вхідної загрози методом очищення інформаційним середовищем в рамках ФБ банку, можна зазначити події та інциденти інформаційної безпеки(ІБ).

Подія ІБ передбачає фільтрацію як небажана загроза в оптимальному стані розвитку ФБ банку, причому становить собою ідентифіковану появу певного стану системи, сервісу або мережі, що вказує на можливе порушення політики ІБ, відмови захисних заходів, або виникнення невідомої раніше ситуації, яка сприймається захистом ФБ банку як інцидент ІБ, який є проявом одного або декількох небажаних чи раптових подій ІБ, з якими пов'язана значна ймовірність конфронтації бізнес-операцій і утворення негативних ефектів для платоспроможності банку.

Для внутрішньої обробки системи фільтрації загроз банку пропонується класифікувати інциденти в залежності від порушених ресурсів та обсягу потенціальних наслідків:

- Висока критичність: інциденти, котрі пов'язані з головними ресурсами серверного сегмента або з критичними ресурсами призначеного для користувача сегмента (ресурси, обробні критичну з точки зору бізнесу, фінансів або законодавства інформацію) [4].

- Середня критичність: інциденти, пов'язані з некритичними ресурсами серверного сегмента.

- Низька критичність: інциденти, пов'язані з некритичними ресурсами призначеного для користувача сегмента (рядовий користувач).

За останні роки абсолютно не новим явищем є проведення хакерами фінансових махінацій або масових кібератак на сервери великих світових компаній.

Під час ознайомлення з рядом інформаційних загроз української банківської системи, слід виділити технологічні складові загроз, які класифіковані на таблиці 1.

Формат загрози	Класифікація впливу
Вірусне ПО	Зараження заключної системи, розповсюдження вірусу по локальній мережі, відключення / блокування служб, що заважають розповсюдженню вірусу, спроби проведення інших атак всередині мережі для отримання критичної інформації та передачі на командні сервери.
Перебір паролів	Намагання підбору аутентифікаційної інформації для доступу до сервісів та ресурсів контрольованих організацій - RDP, SSH, SMB, DB, Web.
Порушення політик ІБ	Дане ПО може бути використано зловмисником для атаки шляхом експлуатації уразливості. Також використання ресурсів компанії для отримання власної вигоди (майнінг bitcoin / ethereum).
Рекламне ПО	Зараження кінцевої системи, передача на командний сервер інформації про користувача, показ таргетованої реклами.
Deface WEB-ресурсів	Хакерська атака, при якій сторінки і важлива інформація замінюються на інші, як правило викликає виду (реклама, попередження, загроза, пропаганда) Найчастіше, доступ до всього іншого сайту блокується, або ж колишній уміст видаляється.
Спроби експлуатації вразливостей	Використання недоліків в системі для порушення цілісності і порушення правильної роботи системи. Уразливість може бути результатом помилок програмування, недоліків, допущених при проектуванні системи, ненадійних паролів, вірусів і інших шкідливих програм, скриптових і SQL-ін'єкцій. Деякі уразливості відомі тільки теоретично, інші ж активно використовуються і мають відомі експлойти.

Складено автором на основі [3,5]

Поступовий розвиток банківської сфери стає прямим чинником до виникнення різного виду порушень з боку злочинців, що у свою чергу впливає на ефективне функціонування банку.

Під час розгляду ІБ українських банків можна зазначити, що управління інцидентами є один з найважливіших процесів управління інформаційною безпекою. Банкам важливо правильно і своєчасно відстежувати обробку інцидентів: прогнозувати, ідентифікувати,

класифікувати, інформувати, стримувати, розслідувати і усувати наслідки.

Користувачам ViPNet TIAS доступна глибока інтеграція з Системою управління інцидентами «превентивного моніторингу», в яку передаються ознаки інцидентів для спільного розбору і реагування. Аналітик банку може прямо з технологічного комплексу запросити необхідні дані про пов'язаних з інцидентом події з ViPNet TIAS, доповнити її вручну, оповістити конкретних співробітників служби безпеки, моніторингу і IT-служб, переадресувавши рекомендації щодо реагування до відома згідно компетенції [9].

Пентест визначається, як показник наскільки легко зловмисникові здійснити проникнення в банківську інформаційну систему. В ході тестування на проникнення «Перспективний моніторинг» моделює дії зловмисника і дає оцінку, скільки ресурсів і часу буде потрібно для успішної кібератаки на замовника. Ми виявляємо ймовірні напрямки розвитку атак і даємо рекомендації, як усунути слабкі місця в захисті і підвищити рівень ІБ. Тест на проникнення зображує, як буде діяти потенційний зловмисник під час кібератаки комерційної структури. Знання векторів атак дає можливість підготуватися до них і знизити негативні наслідки[1].

Пентестер є складовою фільтраційної функції ФБ, який знаходить і експлуатує уразливість в мережевому обладнанні, способах охорони інформації, серверному, системному, прикладному ПО, дізнається, наскільки актуальні знання персоналу установи на яку йде атака. «Перспективний моніторинг» дає замовникам повні рекомендації, як можна скоротити виявлені вразливості або прийняти компенсаційні заходи, і, якщо необхідно, допомагає це зробити[4].

Банківський персонал, або підрозділи ФБ банків мусять підсліджувати потенційні загрози за для усунення можливих інформаційних втрат тому, що далеко не кожний банк може власноруч забезпечити захист інформації. До найбільш невідпрацьованих загрозам, від яких важко захищатися, можна віднести зловживання повноваженнями, технологічна фільтрація від таких факторів безсильною, а ефективний аналіз можливо отримати лише на базі біхевіористичного аналізу персонал у банку.

В ході отримання до банком вхідного масиву даних, вся інформація поділяється на профільну та службову. Службова інформація (наприклад,

паролі користувачів) не відноситься до певної профільної області, в інформаційній системі вона грає технічну роль, але її розкриття є неприпустимою, оскільки воно загрожує отриманням несанкціонованого доступу до всієї інформації, в тому числі предметної [7].

У випадках якщо інформація зберігається на зовнішніх серверах або паперових носіях, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер, при тому що порушення ФБ приходить з боку персоналу і не може бути враховано технічними засобами. До неприємних загроз, з якими наразі банкам складно оперувати, можна віднести зловживання повноваженнями та попередньо підготовленими корисними діями персоналу банку. Для багатьох типів систем привілейований користувачів існують різні доступи (наприклад системний адміністратор) здатний прочитати будь-який (незашифрований) файл, отримати доступ до пошти будь-якого користувача і т.д. Інший приклад - нанесення збитку при сервісному обслуговуванні. Зазвичай сервісний інженер отримує необмежений доступ до обладнання та має можливість діяти в обхід програмних захисних механізмів.

Конфіденційну інформацію можна розділити на предметну і службову. Службова інформація (наприклад, паролі користувачів) не відноситься до певної предметної області, в інформаційній системі вона грає технічну роль, але її розкриття особливо небезпечно, оскільки воно загрожує отриманням несанкціонованого доступу до всієї інформації, в тому числі предметної. Навіть якщо інформація зберігається в комп'ютері або призначена для комп'ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер[3,8].

Висновки. Було розглянуто складові та пріоритети процесу організації кібервтручання в комерційний банк, які з позиції зовнішнього середовища поділено на структурні елементи та напрями процесу кібератаки. Встановлено, що розподіл послідовності процесів фільтрації вхідної загрози методом очищення інформаційного середовища є найбільш ефективним в рамках забезпечення фінансової безпеки банку, а окреме застосування пентестів та елементів штучних пасток дозволяє превентивно запобігати загрозам.

Для внутрішньої обробки системи фільтрації загроз банку пропонується класифікувати інциденти в залежності від порушених

операційних і технологічних процесів, скорегованих на обсяги потенціальних наслідків. Уточнено технологічні складові кіберзагроз на вітчизняному ринку та інструментів для їхньої протидії з позиції нормативно-технічного та програмного забезпечення банку. Акцентовано увагу на тому, що до найбільш невідпрацьованих загрозам, від яких важко захищатися, можна віднести зловживання повноваженнями персоналу, технологічна фільтрація від таких факторів є безсильною, а ефективний аналіз можливо отримати лише на базі біхевіористичного аналізу персоналу банку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Войціховський, А. В. Міжнародне співробітництво у боротьбі з кіберзлочинністю [Електронний ресурс] // Національна бібліотека імені В. І. Вернадського. – Режим доступу: http://www.archive.nbuv.gov.ua/portal/.../ PB-4_26.pdf. – Заголовок з контейнера, доступ вільний, 28.06.2013.
2. Піскозуб А.З. Використання тестування на проникнення в комп'ютерні мережі та системи для підняття їх рівня захищеності // Матеріали третьої міжнародної науково-практичної конференції FOSS Lviv 2013,. – Львів,2013.
3. Семенов С.Г. Исследование методов идентификации програмного обеспечения и их характеристик /С.Г.Семенов // Системи обробки інформації. – Х.: ХУ ПС, 2015. – Вип. 12(137). – С. 148-150.
4. Ткаченко В. Требования к тесту на проникновение [Електронний ресурс] / В. Ткаченко. – Режим доступу: http://auditagency.com.ua/ blog/ Pentest%20requirements.pdf
5. Хвалінський С.О. Основні індикатори-предвісники банківських криз в транзитивних економіках / С.О. Хвалінський // Формування ринкової економіки: збірник наукових праць. Спеціальний випуск: Державне антикризове управління національною економікою: світовий досвід та проблеми в Україні. – К.: КНЕУ, 2010. – С. 283-287.
6. Хорошко В.О. Банківська безпека: Підручник / Корченко А.О., Скачек Л.М, Хорошко В.О. /За заг. ред. докт. техн. наук, проф. О.В.Хорошка. – К.: ПВП «Задруга», 2014 – с.185.
7. Kennedy D., O'Gorman J. Metasploit. The penetration tester's guide. – No starch press, San Francisco, 2011.
8. Category:OWASP Top Ten Project / [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/ OWASP_Top_Ten_Project.
9. OWASP Guide Project / [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/OWASP_Guide_Project