УДК 004.7(045)

В.В.Єрмошин, Я.В. Невойт

АНАЛІЗ І ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ БАНКІВСЬКИХ ТА КОМЕРЦІЙНИХ СИСТЕМ

Відповідно до вимог стандартів з управління інформаційною безпекою вимоги безпеки ідентифікуються систематичною оцінкою ризиків безпеки, а результати оцінки ризику допомагатимуть підприємству яке розробило та впровадило систему управління інформаційною безпекою спрямувати і визначити відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки і впровадити відповідні заходи безпеки, вибрані для захисту від цих ризиків.

В роботі автори поділяться своїм багаторічним практичним досвідом проведення оцінки ризиків інформаційної безпеки для банківських та комерційних систем шляхом розгляду способів реалізації завдань, які виникають під час проведення цих робіт.

Ключові слова: оцінка ризиків, загроза, вразливість

Вступ

Представлена в статті інформація є продовженням статті, перша частина якої було опубліковано в попередньому випуску журналу [1].

Основна частина

Одним із актуальних, важливих, складних і ресурсномістких етапів в процесі оцінки ризиків інформаційної безпеки є складання і підтримка переліку вразливостей [2,3,4,5,6,7].

Як показав проведений аналіз:

- вразливістю є умови, які можуть призвести до реалізації загрози;
- формулювання вразливості повинно відповідати на питання «за рахунок чого?»;
- передумовами виникнення вразливості є не виконання будь яких вимог (законодавчих, нормативних правил, рекомендацій розробників);
- вразливість повинна бути сформульована таким чином щоб при її аналізі та оцінці експерт повинен був відповісти на питання одним з варіантів відповіді «так» чи «ні». Інакше отримати зіставний та відтворюваний результат просто неможливо.

За своєю суттю всі вразливості можна розділити на чотири типи:

- вразливості зумовлені відсутністю передбачених моделлю керування керуючих документів (наприклад: відсутність методики оцінки ризиків (вимога СОУ Н НБУ 65.1 СУІБ 2.0:2010, п.4.1));
- вразливості зумовлені відсутністю передбачених моделлю керування керуючих процесів в випадку коли не виконуються передбачені моделлю керування керуючі дії (наприклад: не доведення до відома найманого персоналу, постачальників / провайдерів / партнерів політики інформаційної безпеки (вимога СОУ Н НБУ 65.1 СУІБ 2.0:2010, п. 5.1.1, 8.2.1.));
- вразливості зумовлені відсутністю передбачених моделлю керування технічних рішень (наприклад: повинно бути введено процедуру сканування носіїв і комунікацій, що виходять за межі організації на можливість витоку конфіденційної інформації (у тому числі прихованої). Процедура повинна надавати можливість визначити задіяний у витоку інформації персонал та системи - відсутність засобів контролю витоку інформації (наприклад DLP-систем) (вимога СОУ Н НБУ 65.1 СУІБ 2.0:2010, п. 12.5.4))
- вразливості пов'язані з конкретним програмним забезпеченням та / або пристроєм.

Докладний аналіз інформації щодо виявлених різними організація вразливостей пов'язаних з конкретним програмним забезпеченням та / або пристроєм показав що

варіантом їх усунення є своєчасна установка оновлень які випускає виробник цього програмного забезпечення та / або пристроїв.

Підтвердженням цього факту є інформація представлена на рис. 1 та 2.

Джерело http: // www.pcweek.ua/themes/detail.php?ID=144870

Рис.1. Рекомендації щодо необхідності встановлення оновлень

Цитата з ресурсу: *Щоб уникнути негативних наслідків, які можуть виникнути в результаті шкідливої атаки за допомогою експлойтів в Java, експерти «Лабораторії Касперського» радять* ***своєчасно встановлювати оновлення Java,*** *а також вибирати захисні рішення, здатні боротися з кібератаками, що використовують експлойти.*

Джерело http: // www.securitylab.ru/vulnerability/447543.php

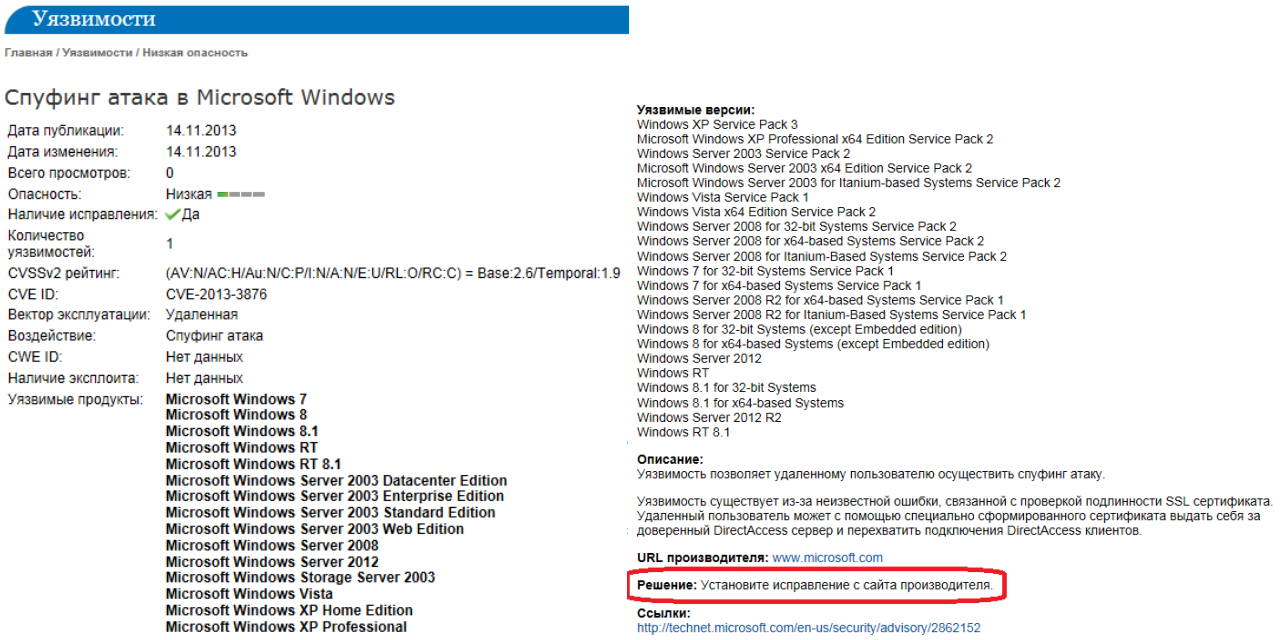

Рис.2. Рекомендації щодо необхідності встановлення оновлень

Це висновок очевидний, тому що в переважній більшості випадків у кінцевого користувача немає можливості самостійно усунути виявлену вразливість в зв'язку з відсутністю у нього доступу до похідного коду цього програмного забезпечення, а також в слідстві відсутності необхідного рівня кваліфікації.

Таким чином можна зробити висновок що розглядати вразливості пов'язані з конкретним програмним забезпеченням та / або пристроєм в разі якщо цей продукт стороннього розробника і цей продукт знаходиться в стадії активної підтримки сенсу немає. Досить щоб це програмне забезпечення або пристрій регулярно з визначеною виробником періодичністю оновлювалося.

У разі якщо програмне забезпечення є власною розробкою організації то аналіз на властиві цьому програмному забезпеченню вразливості розглядати потрібно.

В цьому випадку вразливості можна виявити застосуванням різних типів спеціалізованих сканерів або аналізаторів вихідного коду.

Джерелом переліку можливих вразливостей для банківських систем може бути невиконання вимогнаступних документів [8]:

1. СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD) та СОУ Н НБУ 65.1 СУІБ 2.0:2010 "Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою" (ISO/IES 27002:2005, MOD).
2. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України введених в дію листом НБУ від 03.03.2011 N 24-112/365.
3. Інструкція про безготівкові розрахунки в Україні в національної валюті, затверджена постановою Правління Національного банку України від 21.01.2004 № 22 (зі змінами), зареєстрована в Міністерстві юстиції України 05.05.2005 за № 469/10749.
4. Інструкція про міжбанківський переказ коштів в Україні в національній валюті, затверджена постановою Правління Національного банку України від 16.08.2006 № 320, зареєстрована в Міністерстві юстиції України 06.09.2006 за № 1035/12909.
5. Положення про організацію операційної діяльності в банках України, затверджене постановою Правління Національного банку України від 18.06.2003 № 254, зареєстроване в Міністерстві юстиції України 08.07.2003 за № 559/7880 (зі змінами).
6. Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України, затверджене постановою Правління Національного банку України від 17.06.2004 № 265.
7. Перелік документів, що утворюються в діяльності Національного банку та банків України із зазначенням строків зберігання, затверджений постановою Правління Національного банку України від 08.12.2004 № 601.
8. Положення про порядок формування, зберігання та знищення електронних архівів у Національному банку України і банках України, затверджене постановою Правління Національного банку України від 12.09.2006 № 357, зареєстроване в Міністерстві юстиції України 03.10.2006 за № 1089/12963.
9. Правила зберігання, захисту, використання та розкриття банківської таємниці, затверджені постановою Правління Національного банку України від 14.07.2006 № 267, зареєстровані в Міністерстві юстиції України 03.08. 2006 за № 935/12809.
10. Положення про здійснення банками фінансового моніторингу, затверджене постановою Правління Національного банку України від14.05.2003 №189, зареєстроване в Міністерстві юстиції України 19.11.2004 за № 1062/8383 (зі змінами).
11. Положення про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем, затверджене постановою Правління Національного банку України від 25.09.2007 № 348, зареєстроване в Міністерстві юстиції України 15.10. 2007 за № 1173/14440 (зі змінами).
12. Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затверджені постановою Правління Національного банку України від 02.04.2007, № 112, зареєстровані в Міністерстві юстиції України 24.04.07 за № 419/13686.
13. Правила технічного захисту приміщень банків, у яких обробляються електронні банківські документи, затверджені постановою Правління Національного банку України від 04.07.2007 № 243, зареєстровані в Міністерстві юстиції України 17.08.2007 за № 955/14222.
14. Постанова Правління Національного банку України "Про затвердження нормативно-правових актів з питань функціонування електронного цифрового підпису в банківській системі України" від 04.06.2010 № 284, зареєстрована в Міністерстві юстиції України 04.11.2010 за № 1034/18329.

15. Правила реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків України в Засвідчувальному центрі Національного банку України, зареєстровані в Міністерстві юстиції України 04.11.2010 за № 1035/18330.

16. Правила оформлення Регламенту роботи центрів сертифікації ключів банків України, зареєстровані в Міністерстві юстиції України 04.11.2010 за № 1036/18331.

Слід зазначити, що цей перелік вимог стосується виключно банківських систем, не є вичерпним та повинен підтримуватися власником СУІБ шляхом його періодичного перегляду та актуалізації за визначеною процедурою.

Розрахунок ризиків інформаційної безпеки відповідно до вимог Національного банку України повинен проводитися по відношенню до кожного критичного бізнес-процесу та лише за тим вразливостям, які є актуальними для певного бізнес-процесу[9]. При цьому відповідно до п.5.2 Методичних рекомендацій НБУ слід мати на увазі, що ряд вразливостей будуть однакові для усіх бізнес процесів[9].

В подальшому, кожній вразливості з актуального переліку вразливостей співвідноситься загроза, умовами реалізації якої може бути ця вразливість.

Наприклад: для критичного бізнес-процесу, в якому фігурують персональні дані (бізнес-процес управління персоналом), будуть актуальними всі вразливості, які стосуються захисту персональних даних, та утворені від них пари загроза/вразливість. При цьому для інших критичних бізнес-процесів ці загрози і як наслідок пари є неактуальними, якщо в них не обробляються персональні дані.

В подальшому відповідно до вимог НБУ за кожною визначеною парою необхідно провести оцінку ймовірність її виникнення, плив на конфіденційність, цілісність, доступність та спостережність[9].

При цьому доцільно дотримуватися наступних визначень:

Оцінка ймовірності – умовне число, яке визначає ймовірну частоту реалізації пари загроза/вразливість;

Конфіденційність - властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;

Цілісність - властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом. Цілісність системи - властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки;

Доступність - властивість ресурсу системи, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;

Спостережність - властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Після визначення пар за прийнятими в рамках банку системою оцінок проводиться оцінка впливу реалізації цієї пари на цілісність, конфіденційність, доступність та спостережність, а також ймовірність реалізації цієї пари[9].

Під час першої оцінки за відсутності у банку статистики щодо зареєстрованих інцидентів та їх впливу на зазначені вище категорії доцільно уникати кількісне (числове) співвідношення впливу та ймовірності, а використовувати їх умовну інтуїтивно зрозумілу оцінку. Після накоплення між двома процесами оцінки певної статистики, доцільно переходити на кількісну оцінку впливу та ймовірності реалізації пари загроза/вразливість запропоновану Методичними рекомендаціями НБУ.

Так для оцінки вплив наслідків реалізації загрози на цілісність при першій оцінці доцільно використовувати наступну шкалу оцінки:

Таблиця 1

Оцінка рівня наслідків	Опис
1	Інформація, що несанкціоноване модифікована, виявляється автоматично і не обробляється в подальшому
2	Інформація, що несанкціоноване модифікована, виявляється автоматично, але потребує незначного часу (не більше 1/10 від максимально допустимого часу простою для цього бізнес-процесу/банківського продукту) на її відновлення та має незначний вплив на репутацію банку
3	Інформація, що несанкціоноване модифікована, виявляється автоматично, але потребує середнього часу(не більше 1/2 від максимально допустимого часу простою для цього бізнес-процесу/банківського продукту) на її відновлення та має значний вплив на репутацію банку
4	Інформація, що несанкціоноване модифікована, не виявляється автоматично, потребує значного часу (до максимально допустимого часу простою для цього бізнес-процесу/банківського продукту та більше) на її відновлення, має значний вплив на репутацію банку і може призвести до зупинки роботи бізнес-процесу/банківського продукту
5	Інформація, що несанкціоноване модифікована, не виявляється автоматично, не може бути відновлена, призводить до зупинки бізнес-процесу/банківського продукту і порушує законодавство України

При проведенні банком повторного оцінювання ризиків інформаційної безпеки при визначені рівня наслідків реалізації загрози у вигляді впливу на цілісність по можливості повинна використовуватися шкала оцінки запропонована Методичними рекомендаціями НБУ (зв'язок цілісності з фінансовими втратами), а саме [9]:

Таблиця 2

Оцінка рівня наслідків	Опис
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансових втрат та має незначний вплив на репутацію банку
3	Призводить до значних фінансових втрат та має значний вплив на репутацію банку
4	Призводить до великих фінансових втрат, має значний вплив на репутацію банку і може призвести до зупинки роботи бізнес-процесу/банківського продукту
5	Призводить до зупинки бізнес-процесу/банківського продукту і порушує законодавство України

При цьому повинна бути врахована статистика зареєстрованих (на момент оцінки) фактичних інцидентів інформаційної безпеки (якщо такі інциденти було банком зареєстровано), а саме фактичне числове значення втрат. Саме на основі цієї статистики банк самостійно визначає які суми фінансових втрат будуть розглядатися як незначні, значні та великі фінансові втрати.

В якості прикладу шкали фінансових втрат можна надати таке:

Під незначними фінансовими втратами розуміються втрати до 999 грн.; під значними фінансовими втратами розуміються втрати від 1 000 грн. до 9 999 грн.; під великими фінансовими втратами розуміються втрати від 10 000 грн. до 99 999 грн. Тобто, кількісне

значення фінансових втрат застосовується при оцінці для вже зареєстрованих Банком інцидентів (інцидентів, за яким зареєстрована певна статистика). Для інших інцидентів використовується якісна оцінка (представлена в Таблиці 5.1), рішення щодо якої (рівень) визначає експерт, який проводить таку оцінку. При цьому необхідно мати на у вазі, що при зміні експерта, який проводить оцінку, є загроза, що результат проведеної в цьому випадку оцінки може не відповідати критеріям «відтворюваний» та «зіставний» (за рахунок неможливості чіткого співвідношення опису впливу на цілісність з їх числовим розміром для випадків які в діяльності Банку не відбувалися/не зареєстровані).

Для запобігання такому випадку та підвищення рівня відтворюваності можна долучати декількох експертів для проведення оцінки з наступним усередненням їх результатів.

Для оцінки величини наслідків реалізації загрози: вплив на конфіденційність при першій оцінці доцільно використовувати наступну шкалу:

Таблиця 3

Оцінка рівня наслідків	Опис
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до «банківської таємниці», «комерційної таємниці», персональних даних
3	Призводить до розкриття окремих документів, які відносяться до «банківської таємниці», «комерційної таємниці», персональних даних
4	Призводить до розкриття документів, які відносяться до «банківської таємниці», «комерційної таємниці», персональних даних і має значний вплив на репутацію банку і може призвести до зупинки роботи бізнес-процесу
5	Призводить до зупинки бізнес-процесу і порушує законодавство України

При проведенні банком повторного оцінювання ризиків інформаційної безпеки при визначені рівня наслідків реалізації загрози у вигляді впливу на конфіденційність по можливості повинна використовуватися шкала оцінки запропонована Методичними рекомендаціями НБУ (зв'язок конфіденційності з фінансовими втратами), а саме[9]:

Таблиця 4

Оцінка рівня наслідків	Опис
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до «банківської таємниці», «комерційної таємниці», персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до «банківської таємниці», «комерційної таємниці», персональних даних і призводить до незначних фінансових втрат
4	Призводить до розкриття документів, які відносяться до «банківської таємниці», «комерційної таємниці», персональних даних і призводить до значних фінансових втрат, має значний вплив на репутацію банку і може призвести до зупинки роботи бізнес-процесу/банківського продукту
5	Призводить до зупинки бізнес-процесу/банківського продукту і порушує законодавство України

При проведенні Банком повторного оцінювання ризиків інформаційної безпеки при визначені рівня наслідків реалізації загрози у вигляді впливу на конфіденційність, повинна бути врахована статистика зареєстрованих (на момент оцінки) фактичних інцидентів

інформаційної безпеки (якщо такі інциденти було Банком зареєстровано), а саме фактичне числове значення втрат, яке визначається аналогічно наведеному вище для оцінки впливу на цілісність.

Тобто, кількісне значення фінансових втрат застосовується при оцінці для вже зареєстрованих Банком інциденті (інцидентів, за яким зареєстрована певна статистика). Для інших інцидентів використовується якісна оцінка, рішення щодо якої (рівень) визначає експерт який проводить таку оцінку. При цьому необхідно мати на увазі, що при зміні експерта, який проводить оцінку, є загроза, що результат проведеної в цьому випадку оцінки може не відповідати критеріям «відтворюваний» та «зіставний» (за рахунок неможливості чіткого співвідношення опису фінансових втрат з їх числовим розміром для випадків які в діяльності Банку не відбувалися/не зареєстровані).

Для запобігання такому випадку та підвищення рівня відтворюваності можна долучати декількох експертів для проведення оцінки з наступним усередненням їх результатів.

Для оцінки величини наслідків реалізації загрози: вплив на доступність при першій оцінці доцільно використовувати наступну шкалу:

Таблиця 5

Оцінка рівня наслідків	Опис
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше 1/10 від максимально допустимого часу простою для цього бізнес-процесу/банківського продукту)
3	Вплив на доступність середній (не більше 1/2 від максимально допустимого часу простою для цього бізнес-процесу/банківського продукту)
4	Вплив на доступність значний (до максимально допустимого часу простою для цього бізнес-процесу/банківського продукту)
5	Призводить до зупинки бізнес-процесу/банківського продукту на тривалий час, який перевищує максимально допустимий час простою

Для величини наслідків реалізації загрози: вплив на спостережність:

Таблиця 6

Оцінка рівня наслідків	Опис
1	Практично не впливає
2	Вплив незначний
3	Призводить до неможливості відстежити частину дій виконавців бізнес-процесу/банківського продукту
4	Призводить до неможливості відстежити дії виконавців і адміністраторів бізнес-процесу/банківського продукту/ програмно-технічного комплексу
5	Призводить до неможливості відстежити дії виконавців і адміністраторів бізнес-процесу/банківського продукту/ програмно-технічного комплексу, може призвести до зупинки бізнес-процесу/банківського продукту, має вплив на репутацію банку і порушує законодавство України

В випадку розгляду вразливостей, які є однаковими для усіх бізнес-процесів, в якості суми фінансових втрат для оцінки впливу на цілісність та конфіденційність приймається максимальна сума втрат з усіх розглянутих бізнес-процесів. В якості максимального часу простою бізнес-процесу для оцінки впливу на доступність приймається мінімальний час простою з усіх розглянутих бізнес-процесів.

Наприклад: для пари загроза/вразливість компрометація інформації в наслідок несанкціонованого фізичного доступу/відсутності контролю за носіями інформації визначним параметром впливу є конфіденційність. Для неї вибирається значення оцінки 5 або 4. Наступним за значенням впливу параметром для цієї пари є цілісність. Для неї вибирається значення оцінки 4 або 3. Доступність та спостережність за впливом для цієї пари є несуттєвими. Для них вибирається значення оцінки 2 або 1. Для параметрів (конфіденційність, цілісність, спостережність, доступність) які не мають відношення до пари вибирається значення оцінки 1. При цьому більша з оцінок обирається експертом для відомих йому випадків реалізації певної вразливості.

Оцінку ймовірності реалізації загрози з використанням вказаної вразливості доцільно проводити методом експертної оцінки по шкалі представленій нижче.

Таблиця 7

Оцінка ймовірності	Опис
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне
3	Виникнення інциденту ймовірне
4	Виникнення інциденту цілком ймовірне
5	Інцидент відбудеться

При виборі оцінки ймовірності доцільно використовувати наступну логіку: в разі, коли вразливість обумовлена відсутністю технічного рішення, в якості ймовірності доцільно обирати значення 5 або 4 – тобто в разі відсутності технічного рішення подія відбудеться; в разі, коли вразливість обумовлена відсутністю процесу керування, в якості ймовірності доцільно обирати значення 4 або 3 – тобто в разі відсутності процесу керування подія швидше відбудеться чим ні; в разі, коли вразливість обумовлена відсутністю певного регламентуючого процес документу, в якості ймовірності доцільно обирати значення 3 або 2 – тобто в разі відсутності регламентуючого процес документу подія ймовірно відбудеться. При цьому при виборі оцінки ймовірності значення 1 не використовується.

Наприклад: для вразливості «відсутність методики оцінки ризиків» ймовірності реалізації загрози з використанням вказаної вразливості дорівнює 3 або 2, для вразливості «відсутність задокументованих результатів декількох оцінок, які можна порівняти» ймовірності реалізації загрози з використанням вказаної вразливості дорівнює 4 або 3, для вразливості «відсутності засобів контролю витоку інформації (наприклад DLP-систем)» ймовірності реалізації загрози з використанням вказаної вразливості дорівнює 5 або 4.

При проведенні банком повторного оцінювання ризиків інформаційної безпеки при визначені ймовірності реалізації загрози з використанням вказаної вразливості, за можливістю повинна бути врахована статистика зареєстрованих (на момент оцінки) фактичних інцидентів інформаційної безпеки (якщо такі інциденти було банком зареєстровано), а саме фактичне числове значення кількості зареєстрованих інцидентів.

Під виникнення інциденту практично неможливо розуміється, що інцидент інформаційної безпеки виникає не частіше ніж 1 раз на 2 роки; під виникнення інциденту малоймовірне розуміється, що інцидент інформаційної безпеки виникає не частіше ніж 1 раз на 1 рік; під виникнення інциденту ймовірне розуміється, що інцидент інформаційної безпеки виникає не частіше ніж 1 раз на 3 місяці; під виникнення інциденту цілком ймовірне розуміється, що інцидент інформаційної безпеки виникає не частіше ніж 1 раз на тиждень; під інцидент відбудеться розуміється, що інцидент інформаційної безпеки виникає 1 раз на добу. На підставі статистичних даних кількісне вираження частоти появи інцидентів в Банку можуть бути змінені (збільшені або зменшені).

Тобто, кількісне значення частоти виникнення інциденту застосовується при оцінці для вже зареєстрованих банком інциденті (інцидентів, за яким зареєстрована певна статистика).

Для інших інцидентів використовується якісна оцінка, рішення щодо якої (рівень) визначає експерт, який проводить таку оцінку. При цьому необхідно мати на у вазі, що при зміні експерта, який проводить оцінку, є загроза, що результат проведеної в цьому випадку оцінки може не відповідати критеріям «відтворюваний» та «зіставний» (за рахунок неможливості чіткого співвідношення опису частоти виникнення інциденту з їх реальною кількістю зареєстрованою банком).

Для запобігання такому випадку та підвищення рівня відтворюваності можна залучати декількох експертів для проведення оцінки з наступним усередненням їх результатів.

Після визначення пар загроза/вразливість та їх оцінки проводиться розрахунок ризику.

Відповідно до вимог НБУ розрахунок ризику повинен проводиться відповідно до п.6.1 Методичних рекомендацій НБУ, а саме рівень ризику за окремою парою загроза/вразливість, яка може використовуватися для реалізації цієї загрози, визначається перемноженням загального рівня оцінки величини наслідків на оцінку ймовірності реалізації загрози. Загальний рівень оцінки величини наслідків реалізації кожної пари загроза/вразливість на сервіси безпеки визначається як максимальна величина з окремих оцінок впливу на цілісність, конфіденційність, доступність, спостережність[9].

Загальний рівень ризику для бізнес-процесу/банківського продукту дорівнює максимальної величині з усіх ризиків за кожною парою загроза/вразливість[9].

За результатами оцінки готується звіт, форма якого для банку представлена в Додатку 3 до Методичних рекомендацій НБУ.

Окрім звіту, по кожному бізнес процесу або категорії розгляду може бути підготовлена відповідна «хмара ризиків».

Хмара ризиків - кругова діаграма, діаметрами якої є рівні ризику (від 0 до 25), а радіусами цієї діограми є оцінені за парою загроза-вразливість ризики.

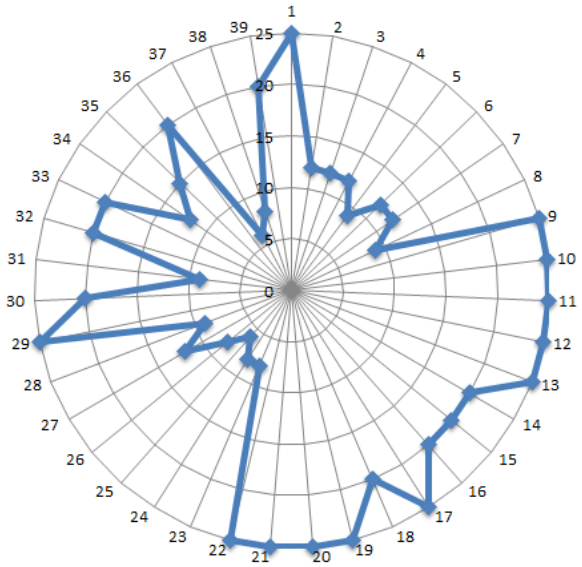

Рис. 3. Хмара ризиків

На підставі наявного у авторів досвіду з побудови систем управління інформаційної безпеки (12 успішно реалізованих проектів) доцільно надати наступну статистику:

- 13% всіх вразливостей пов'язані з відсутністю певних технічних рішень які їх усувають/блокують;
- 41% вразливостей пов'язані з відсутністю певного керуючого процесу;
- 46% вразливостей обумовлені відсутністю певного керуючого документа;

- максимальна вага ризику обумовленого вразливістю пов'язаною з відсутністю технічних рішень лежить в межах 20-25;
- максимальна вага ризику обумовленого вразливістю пов'язаною з відсутністю впровадженого керуючого процесу лежить в межах 15-20;
- максимальна вага ризику обумовленого вразливістю пов'язаною з відсутністю керуючого документа лежить в межах 10-15;
- реалізація проекту побудови СУІБ гарантовано усуває всі вразливості обумовлені відсутністю керуючих документів, при цьому за виконання певних умов можуть бути усунені і всі вразливості пов'язані з відсутністю керуючих процесів;
- відсутність впроваджених технічних рішення залишає в повному обсязі всі вразливості які обумовлені їх відсутністю. Загрози обумовлені відсутністю технічного рішення не можуть бути усунені шляхом впровадження документів та управляючих процесів;
- залишкова кількість вразливостей всіх типів в якісно реалізованому проекті по побудові СУІБ становить не більше 6%;
- залишкова кількість вразливостей всіх типів в разі формально впровадження моделі управління ІБ становить 27%. У самому негативному результаті може досягати 54%;
- задіяними в проект СУІБ без сертифікації є відповідальні за критичні бізнес-процеси, представники підрозділу безпека, IT, юристи, HR, ризиків, аудиту (мінімум 28 осіб);
- задіяними в проект при сертифікації СУІБ окрім вказаних вище додатково залучаються по одному представнику з кожного підрозділу (у тому числі регіонального - за їх наявності) - на практиці загальна кількість для банка першої та другої групи близько 90 осіб;
- хмари ризиків до та після впровадження проекту СУІБ представленні нижче.
-

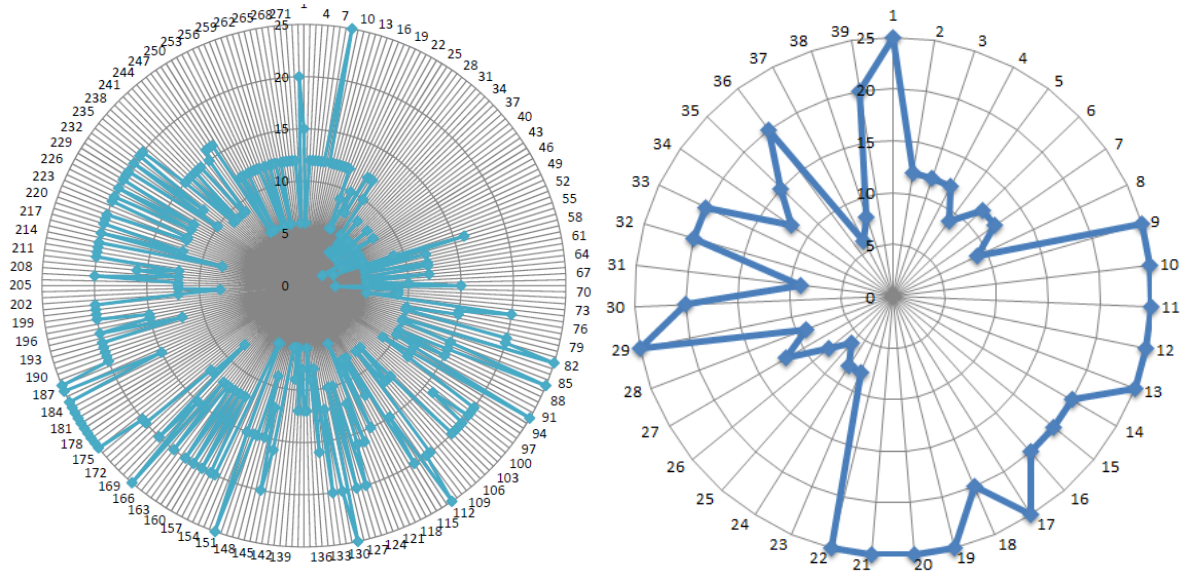

Рис. 4. Хмари ризиків до та після впровадження проекту СУІБ

Висновок

Таким чином банком чи підприємством буде вирішена друга частина задачі оцінки ризиків інформаційної безпеки - створено загальний перелік вразливостей та вирішена задача оцінки ризиків інформаційної безпеки в цілому.

Література

1. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем // Сучасний захист інформації. – 2014. – №3, С. 26-29.

2. Розорінов Г.М., Єрмошин В.В. Проблемні питання в реалізації оцінки ризиків інформаційної безпеки // Проблеми та перспективи розвитку науки / Матеріали XIV Міжнародної науково-практичної конференції 25-26 жовтня 2014 р. (Буковинська економічна фундація, Чернівці). – Т. 1. – Київ: Науково-видавничий центр «Лабораторія думки», 2014. – С.7.

3. Єрмошин В. Методологія оцінки ризиків у відповідності до вимог міжнародного стандарту ISO/IEC 27001 // Одиннадцатая Международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах", Тезисы докладов. –К: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ" . –2008. - С.63.

4. Ермошин В.В. Методика оценки информационных рисков предприятия // Захист інформації. – 2009. – №4(45), С. 80-88.

5. Єрмошин В.В., Хорошко В.О., Капустян М.В. Методика оцінки інформаційних ризиків системи управління інформаційною безпекою // Сучасний захист інформації. – 2010. – №3, С. 95-104.

6. Ермошин В.В. Методика оценки информационных рисков предприятия // Захист інформації. – 2009. – №4(45), С. 80-88.

7. Корченко А.Г., Архипов А.Е., Казмирчук С.В. Анализ и оценивание рисков информационной безопасности.– К: ООО «Лазурит-Полиграф», 2013 – С.275.

8. 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.

9. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України введених в дію листом НБУ від 03.03.2011 N 24-112/365.

Надійшла 29.10.2014 р. Рецензент: д.т.н., проф. Хорошко В.О.