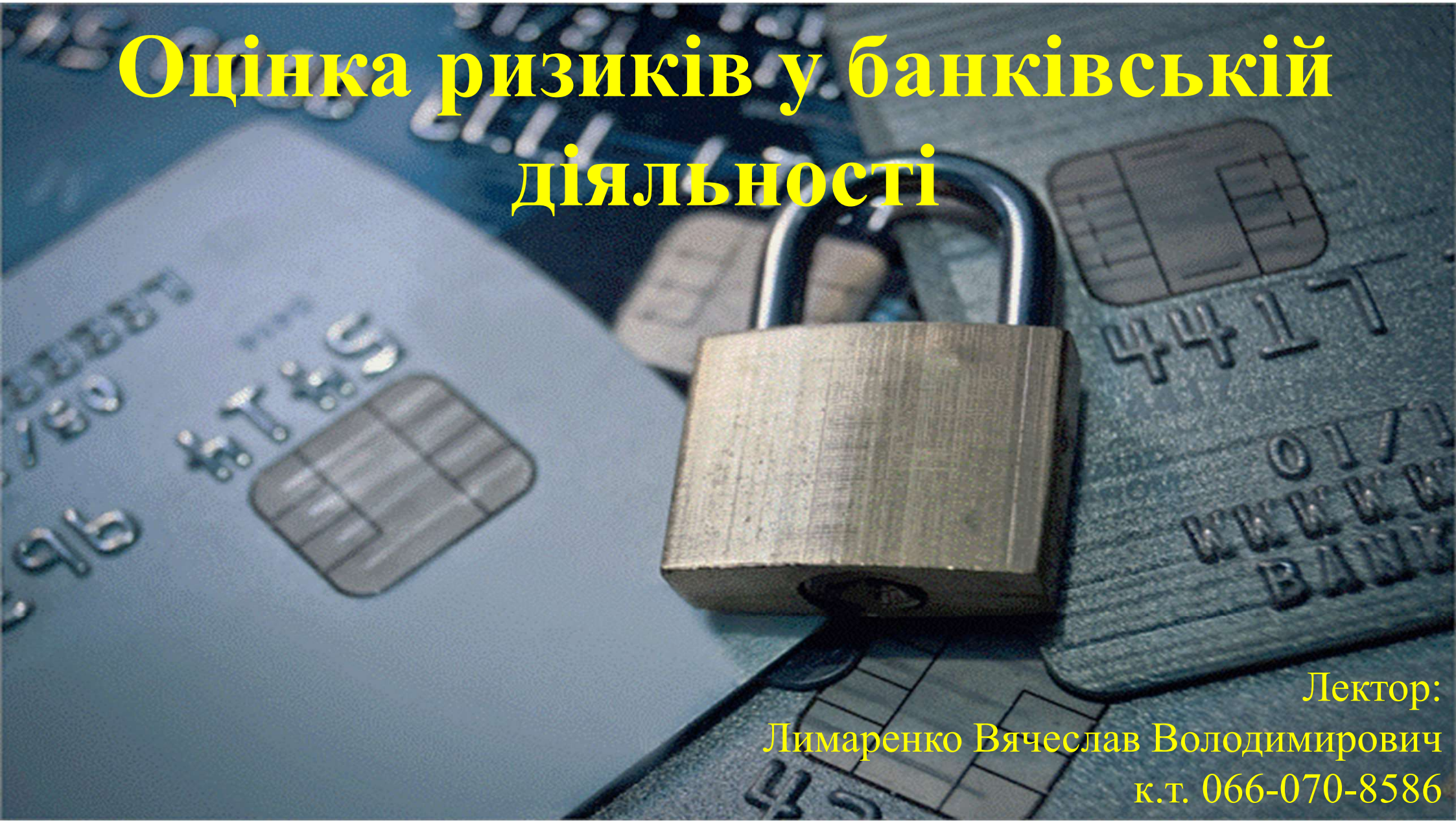
Оцінка ризиків у банківській діяльності



Лектор:
Лимаренко Вячеслав Володимирович
к.т. 066-070-8586

Підходи до оцінки захищеності банківських систем

Безпека банківських систем в загальних аспектах інформаційних систем розглядається як *здатність системи протистояти руйнівній дії зовнішніх і внутрішніх загроз*. В цілому, безпеку банківської системи можна представити як протистояння дестабілізуючим діям зовнішніх і внутрішніх загроз, тобто збереження структури і її функціонування від дії дестабілізуючих чинників, або впливу загроз для елементів системи від зовнішнього середовища.

Підходи до оцінки захищеності банківських систем

В теперішній час, *інформаційна безпека* як галузь науки, знаходиться на етапі теоретико-концептуального підходу, який в даний момент є перспективним. Він ґрунтується на розробці цілісності теорії захисту інформації з використанням науково-методичної бази, яка повинна постійно поповнюватися, створюючи нові, гнучкіші і ефективніші інструментальні засоби.

У основу цього підходу лягло поняття «*комплексність*». Цей підхід припускає застосування усіх доступних способів, взаємозв'язаних між собою для досягнення кінцевої мети – забезпечення ефективного захисту банківської системи. Він виражається на всіх напрямках реалізації захисту. В організаційних аспектах комплексність має бути представлена через зацікавленість і взаємодію усіх учасників банківської системи. У технічному аспекті – це застосування усіх доступних програмно-апаратних засобів, їх взаємодія відповідно до вибраної політики реалізації інформаційної безпеки системи.

Етапи життєвого циклу

Для забезпечення захищеності будь-яких систем здійснюється ряд дій, які можна класифікувати відносно переліку завдань відповідно до їх часових і цільових рамок. Таку класифікацію можна побачити в етапах *життєвого циклу*

Життєвий цикл	Задачі, що вирішуються в галузі захисту
Аналіз	Виявлення і оцінка потенційно значимих дестабілізуючих факторів. 1.Оцінка показників уразливості інформації при різних вимогах і варіантах управління. 2.Оцінка рівня захищеності системи, а також у часу. 3.Виявлення найбільш небезпечних дестабілізуючих чинників і елементів системи. 4.Аналіз умов, при яких рівень уразливості може бути вищий допустимого. 5.Прогнозування рівня захищеності. 6.Аналіз впливу змін вимог до захисту
Синтез	1.Обґрунтування оптимального складу функцій захисту. 2.Обґрунтування оптимальної достатньої безлічі завдань з реалізації функцій захисту. 3.Обґрунтування і уточнення оптимального складу функцій, структури системи захисту і технології рішення завдань.
Управління	1. Обґрунтування оптимальної структури і алгоритмів планування захисту. 2. Відробіток алгоритмів оптимального реагування в нештатних ситуаціях. 3. Пошук оптимальних рішень в процесі планування захисту інформації.

Етапи життєвого циклу. Етап аналізу

Першим і важливим завданням, що вирішується для ефективного забезпечення інформаційної безпеки, є *етап аналізу* – саме він задає подальшу дію для досягнення кінцевої мети – створення захищеної банківської системи. Також, цей етап життєвого циклу допомагає ефективно використати ресурси, розробити і реалізувати захист, системи.

На основі результатів аналізу захищеності можна здійснити наступні дії:

- зробити коригування помилкових налаштувань і конфігурацій підсистем для банківських систем;
- провести заходи щодо зниження вірогідності застосувань вразливостей, які не можуть бути усунені за короткий проміжок часу;
- перевірити правильність усунень вразливостей;
- переглянути політику безпеки з урахуванням останніх змін;
- провести інші заходи спрямовані на підвищення захищеності систем;
- внести необхідні зміни, в архітектуру банківської системи з метою підвищення ефективності захисту;

Фактично *етап аналізу* можна оцінити як визначення рівня, захищеності системи.

Етапи життєвого циклу. Етап аналізу

Широке поширення отримав *аудит інформаційної безпеки*.

Під аудитом розуміється виконання заходів з перевірки відповідності використаних механізмів із забезпечення інформаційної безпеки банківської системи заданим вимогами. Аудит інформаційної безпеки спрямований на об'єктивну оцінку поточного стану інформаційної безпеки банку (системи), а також на її адекватність поставленим цілям і завданням бізнесу для збільшення ефективності і рентабельності економічної діяльності банку.

Можна виділити два варіанти аудиту:

- ✓ аудит банку;
- ✓ аудит тільки банківської системи.

Етапи життєвого циклу. Етап аналізу

Основними діями аудиту банку є:

- ✓ перевірка в організації виробленої політики інформаційної безпеки, зокрема, перевірка наявності документованого підходу до оцінювання ризиків і управління ними у рамках усього банку;
- ✓ перевірка організаційної інфраструктури інформаційної безпеки на місцях, тобто перевірка розподілу обов'язків співробітників по забезпеченню безпеки;
- ✓ аналіз процесу обслуговування, і адміністрування банківської системи;
- ✓ перевірка підходів оцінювання ризиків і управління ними;
- ✓ дослідження документації за системою управління інформаційною безпекою;
- ✓ оцінювання ризиків банківської системи;
- ✓ вибір заходів для протидії виявленим ризикам.

Етапи життєвого циклу. Етап аналізу

Основними діями аудиту банку є:

- ✓ перевірка в організації виробленої політики інформаційної безпеки, зокрема, перевірка наявності документованого підходу до оцінювання ризиків і управління ними у рамках усього банку;
- ✓ перевірка організаційної інфраструктури інформаційної безпеки на місцях, тобто перевірка розподілу обов'язків співробітників по забезпеченню безпеки;
- ✓ аналіз процесу обслуговування, і адміністрування банківської системи;
- ✓ перевірка підходів оцінювання ризиків і управління ними;
- ✓ дослідження документації за системою управління інформаційною безпекою;
- ✓ оцінювання ризиків банківської системи;
- ✓ вибір заходів для протидії виявленим ризикам.

Для аудиту банківської системи виконуються наступні дії:

- ❑ дослідження політики інформаційної безпеки документації за системою управління інформаційної безпеки і відомостей відповідності, які відбивають реальний стан оцінюваної системи;
- ❑ аналіз документації проведеному оцінюванню ризиків;
- ❑ перевірка засобів управління інформаційною безпекою;
- ❑ синтез контрзаходів і обґрунтування їх ефективності.

Етапи життєвого циклу. Етап аналізу

Одним з основних завдань будь-якого аудиту є *отримання результату процесу оцінювання ризиків безпеки* банківської системи. Слід зазначити *відсутність єдиної методики* оцінки ризиків інформаційної безпеки. Проте, існують загальні критерії реалізації таких методик. Вони припускають використання деякої моделі або комплексу моделей, через які можна охарактеризувати досліджувану систему.

Початкові дані:

- ❑ знання експертів
- ❑ статистичні данні появи тих або інших загроз.

Значення кінцевих оцінок залежать не лише від коректності початкових даних, але і від вибраної методики і, відповідно, від використовуваної моделі.

Етапи життєвого циклу. Загальні вимоги до методики оцінки ризиків відкритих систем

По-перше, важливо, щоб обрана стратегія в методиці була достатньо гнучкою при нарощуванні системи і мала можливість швидкого отримання кінцевих оцінок ризиків відносно реалізованої системи.

По-друге, методика має бути універсальною, щоб вона дозволяла давати оцінки для різних по структурі систем, якими є відкриті системи. При цьому вона повинна мати достовірність і оцінювати систему не лише для групи життєво важливих елементів, але і розглядати усю систему в комплексі.

При оцінці захищеності банківських систем існує загальна інформація про можливі загрози і очікуваний збиток від реалізації тієї або іншої загрози. Ця інформація накладається на розроблювану або існуючу модель реальної оцінюваної системи. Основна вимога до такої моделі – це адекватне уявлення необхідної інформації про оригінал. Іноді застосовується додаткова інформація, наприклад, визначаються дії зловмисника, що називаються *моделлю зловмисника*.

Комплексний підхід щодо аналізу інформаційної безпеки банківських систем

Для ефективного захисту від атак потрібна оцінка рівня безпеки банківської системи. Саме для цих цілей застосовуються методики аналізу і оцінка ризиків. В результаті отриманої оцінки можна сформулювати набір вимог до системи, що забезпечує необхідний рівень захисту.

Побудова ефективної, системи управління ризиками IT-безпеки – це не разовий проект, а комплексний процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз.

Існують загальні, базові етапи оцінки ризиків:

- Ідентифікація
- Оцінка
- Вимір
- Вибір контрзаходів

Вимір ризиків

Зазвичай вважається, що ризик тим більше, чим більше вірогідність події і тяжкість наслідків. Формально, в загальному виді оцінку ризиків можна отримати наступним виразом

$$Risk = P_i \cdot C_l$$

де

P_i – вірогідність події; C_l – ціна втрати.

При цьому розрізняють трьохфакторний підхід, при якому вірогідність події замінюється добутком вірогідності появи загрози на вірогідність використання вразливості.

При оцінці значень змінних існує два підходи *кількісний* і *якісний*. У першому випадку змінні представляються у вигляді чисельних величин, а ризик – це оцінка математичного очікування втрат. При *якісному підході* набуття значень змінних робиться згідно із встановленими критеріями, що складаються з трьох – семи значень. При цьому формула в явному виді не застосовується.

Вибір контрзаходів

Завдання оцінки ефективності контрзаходів не простіше, ніж оцінка ризиків. Це пояснюється тим, що оцінка ефективності комплексної підсистеми безпеки, що включає контрзаходи різних рівнів (адміністративні, організаційні, програмно-технічні) в конкретній, інформаційній системі – це окрема, методологічно надзвичайно складна задача. Дослідження цієї проблеми виходить за рамки курсу.

Незважаючи на різні підходи до оцінки ризиків, є загальні, базові етапи в отриманні кінцевих оцінок. Розглянуті етапи дозволять дотримуватися рамок в реалізації методики оцінки ризиків для відкритих систем. При цьому не буде виключенням застосування поняття комплексності до моделей оцінки, що розробляються. Комплексність можна представити у вигляді наступних тез:

– у першому випадку вона досягатиметься набором розроблених взаємопов’язаних моделей, що дозволяють ефективно провести дослідження системи;

– в другому – комплексність досягається застосуванням експертів по відношенню до досліджуваної системи через сукупність моделей відкритої системи.

Оцінка захищеності інформації у банківській діяльності

Існують різні види оцінок захищеності відмінні від оцінок ризиків. Розглянемо *методологію оцінки вразливості інформації*. Як правило вона складається з трьох компонентів:

1) показники вразливостей;

2) загрози інформації;

3) моделі визначення поточних і очікуваних значень показників вразливостей.

Практична реалізація такої методології стикається з рядом проблем пов'язаних з формуванням баз початкових даних необхідних для забезпечення моделей оцінки вразливості. Доведеність необхідного рівня захисту, на кожному конкретному об'єкті в умовах його функціонування, що змінюються, натрапляє на труднощі пов'язані з різними гетерогенними чинниками, які часто оцінюються якісними показниками.

Оцінка захищеності інформації у банківській діяльності

Проблема визначення вимог до захисту інформації має комплексний характер і повинна розглядатися в двох напрямах:

- Організаційному;
- Технічному.

У *технічному аспекті* виникають труднощі з огляду на те, що існує досить велика кількість каналів просочування інформації, які можуть бути перекриті спеціалізованими програмно-технічними засобами.

Організаційним, являється підхід, що базується на створенні і використанні системи стандартів в області захисту інформації. Виділяється деяка кількість типових, систем захисту, рекомендованих в тих або інших умовах і таких, що містять деяку кількість механізмів захисту, що необхідна для конкретного типу системи захисту.

Оцінка захищеності інформації у банківській діяльності

Основою забезпечення безпеки інформаційних технологій є рішення трьох фундаментальних завдань:

- ❑ забезпечення конфіденційності
- ❑ забезпечення цілісності
- ❑ забезпечення доступності.

Цей підхід закладений в стандартах, що стосуються забезпечення інформаційної безпеки, більшості країн. Він також відбитий в керівних українських документах.

Документи створені з урахуванням «Критеріїв оцінки довірених комп'ютерних систем», відомих під назвою «*Помаранчева книга*», які разом з Європейськими і Канадськими критеріями склали основу «*Загальних критеріїв*» – стандарту ISO «Критерії оцінки безпеки інформаційних технологій».

Методики визначення потрібного рівня захисту

Перша базується на *напівевристичній процедурі*

- усі показники інформації діляться на три категорії: визначальні, істотні і другорядні, причому основним критерієм такого ділення повинна служити мета, для досягнення, якої здійснюється захист інформації;
- необхідний рівень захисту, визначається по значеннях визначальних показників інформації;
- вибраний рівень при необхідності може бути скорегований з урахуванням значення істотних показників. Значення другорядних показників при цьому можуть ігноруватися.

Методики визначення потрібного рівня захисту

Друга методика використовує класифікацію показників інформації залежно від цілей захисту, що отримані на основі експертних оцінок. В цьому випадку необхідний рівень захисту інформації в конкретних умовах залежить від обліку чинників, які впливають на захист.

Таким чином, можливе формування повнішого визначення множини цих чинників і адекватніше визначення міри їх впливу на необхідний рівень захисту, що являється на сучасному етапі однім з найбільш вирішальних завдань. Для досягнення цих цілей використовуються *неформально евристичні методи*, засновані на знаннях, досвіді і інтуїції спеціалістів захисту інформації

Програмні засоби аналізу ризиків банківських систем

Розглянемо існуючі програмні продукти, розроблені для оцінки ризиків різних систем, засновані на різних підходах до аналізу ризиків.

- ✓ Risk Watch;
- ✓ CRAMM;
- ✓ КОНДОР.

Ці програмні продукти базуються на різних підходах до аналізу ризиків і рішення різних аудиторських завдань.

Програмні засоби аналізу ризиків банківських систем. Risk Watch

Risk Watch є потужним засобом аналізу і управління ризиками, більше орієнтованим на точну, кількісну, оцінку співвідношення витрат від загроз безпеці і витрат на створення системи захисту. В продукті ризики у сфері інформаційної і фізичної безпеки комп'ютерної мережі банка розглядаються спільно.

Програмні засоби аналізу ризиків банківських систем. Risk Watch

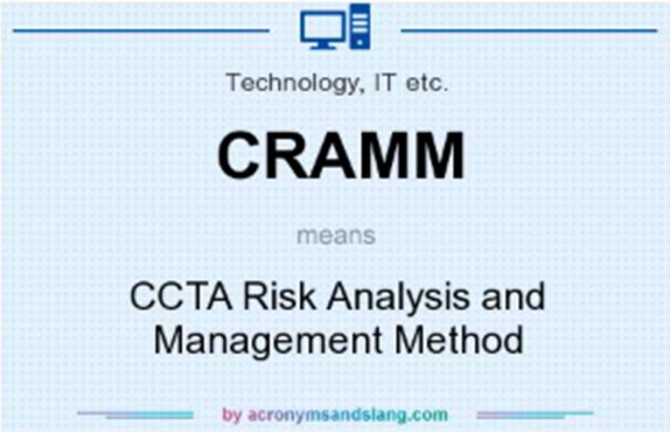
В основу Risk Watch покладена методика аналізу ризиків, яка складається з чотирьох етапів:

- *перший* – визначення предмета дослідження. Тут описуються такі параметри, як тип банка, склад досліджуваної системи, базові вимоги в області безпеки;
- *другий* – введення даних, що характеризують основні параметри системи. На цьому етапі детально описуються ресурси, втрати і класи інцидентів. Останні виводяться шляхом зіставлення категорії втрат і категорії ресурсів. Крім того, задаються частота виникнення кожної з виділених загроз, міра вразливості і цінність ресурсів. Усе це використовується надалі для розрахунку ефекту від впровадження засобів захисту;
- *третій* – кількісна оцінка. На цьому етапі розраховується профіль ризиків, вибираються заходи забезпечення безпеки. Фактично ризик оцінюється за допомогою математичного очікування втрат за рік. Ефект від впровадження засобів захисту кількісно описується за допомогою показника ROI (Return on Invtstment – віддача від інвестицій), який показує віддачу від вкладених інвестицій за певний період часу;
- *четвертий* – генерація звітів.

Недоліком цього програмного продукту є те, що такий метод не підходить, якщо вимагається провести аналіз ризиків на програмно-технічному рівні захисту, без урахування організаційних і адміністративних чинників. Отримані оцінки ризику (математичне очікування втрат) далеко не вичерпують розуміння ризику з системних позицій. Також метод не враховує комплексний підхід до інформаційної безпеки.

Програмні засоби аналізу ризиків банківських систем. CRAMM

CRAMM – інструментальний засіб, що реалізовує однойменну методику, яка була розроблена компанією BIS Applied Systems Limited за замовленням британського уряду. У основі CRAMM лежить комплексний підхід до оцінки ризиків що поєднує кількісні і якісні методи аналізу. Метод універсальний може застосовуватися для великих і малих банків, як державних, так і комерційних. Ця методика спирається на оцінки якісного характеру, що отримуються від експертів, і на їх базі будує кількісну оцінку. У методиці CRAMM уся процедура аналізу розділена на три послідовні етапи.



Програмні засоби аналізу ризиків банківських систем. CRAMM

На першому етапі виконується завдання визначення достатності для захисту системи застосування засобів базового рівня, що реалізовують традиційні функції безпеки, а також необхідність проведення детальнішого аналізу.

На другому етапі робиться ідентифікація ризиків і оцінюється їх величина.

На третьому етапі вирішується питання про вибір адекватних контрзаходів.

Для кожного етапу визначають набір початкових даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки і набір звітних документів.

Програмні засоби аналізу ризиків банківських систем. CRAMM

Недоліком програмного продукту є:

- ✓ використання методу CRAMM вимагає від аудитора спеціальної підготовки і високої кваліфікації;
- ✓ CRAMM підходить для аудиту вже існуючих банківських систем, що знаходяться на стадії експлуатації, але не для ІС в розробці;
- ✓ аудит по методу CRAMM – процес досить трудомісткий і може зажадати декілька місяців безперервної роботи аудитора;
- ✓ програмний інструментарій CRAMM генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці;
- ✓ можливість внесення доповнень у базу знань CRAMM не доступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретного банку.

Програмні засоби аналізу ризиків банківських систем. КОНКОР

КОНКОР дозволяє фахівцям проводити політику інформаційної безпеки банка на відповідність вимогам ISO 17799. КОНКОР включає більше 200 питань, відповівши на які, фахівець отримує звіт про стан існуючої політики безпеки, а також модуль оцінки рівня ризиків відповідно вимогам ISO 17799. Ця система також реалізує метод якісної оцінки ризиків за трирівневою шкалою:

- ❑ Високий
- ❑ Середній
- ❑ Низький.

Недоліком продукту є:

– відсутність можливості установки користувачем ваги на кожну вимогу;

– відсутність можливості внесення користувачем коментарів.

Системний підхід щодо оцінки захищеності банківських систем

Найбільш сталим є *системний підхід*. Незважаючи на його довге існування, немає єдиних методик синтезу і аналізу систем, які можна використати в різних галузях життєдіяльності людини. У поняття «Системний підхід» вкладається наступний зміст:

– точне формулювання вимог, що пред'являються до рішення задачі;

– наявність математичного апарату для її дослідження і набору критеріїв для оцінки можливих рішень.

У простому випадку застосування системного підходу до завдання не зобов'язує до детального знання фізичних елементів, необхідних для реалізації знайденого рішення. Поняття системності полягає не просто в створенні відповідних механізмів захисту, а є регулярним процесом, здійснюваним на усіх етапах життєвого циклу ІС. Усі засоби, методи і заходи, використовувані для захисту інформації, об'єднуються в цілісний механізм – систему захисту.

Системний підхід щодо оцінки захищеності банківських систем

Системний підхід базується на наступних поняттях:

– *система* – сукупність елементів і зв'язків між ними;

– *структура* – стійка картина взаємовідносин між елементами (картина зв'язків і їх стабільна/динамічна зміна системи у часі).

– *функція* – процес, що відбувається усередині системи і має *стан* – положення системи відносно інших її положень.

Системний підхід можна описати як підхід, при якому будь-яка система (об'єкт) розглядається як сукупність взаємозв'язаних елементів (компонентів):

– вихід (мета);

– вхід (ресурси);

– зв'язок із зовнішнім середовищем;

– зворотний зв'язок.

Системний підхід щодо оцінки захищеності банківських систем

Системний підхід має ряд властивостей:

– цілісність, що дозволяє розглядати одночасно систему як єдине ціле і в той же час як підсистему для вище розташованих рівнів;

– ієрархічність будови, тобто наявність множини (принаймні, двох) елементів, розташованих на основі підпорядкування елементів нижчого рівня, елементам вищого рівня;

– структуризація, що дозволяє аналізувати елементи системи і їх взаємозв'язки у рамках структури конкретного банку. Як правило, процес функціонування системи обумовлений не стільки властивостями її окремих елементів, скільки властивостями самої структури;

– множина, що дозволяє використати безліч економічних і математичних моделей для опису окремих елементів і системи в цілому.

Процесний підхід щодо оцінки захищеності банківських систем

Процесний підхід синтезований з ідеї функціонування системи і є переродженням системного підходу. Передбачається, що система, маючи конкретні поставлені цілі або не маючи їх, буде постійно функціонувати. У першому випадку система функціонуватиме для досягнення поставлених цілей, а в другому для підтримки, номінальності її існування. У обох випадках система, здійснює певні види, діяльності або іншими словами виконує процес.

Процесний підхід щодо оцінки захищеності банківських систем

Процесний підхід – це представлення діяльності із забезпечення інформаційної безпеки у вигляді системи процесів в межах організації разом з ідентифікацією, взаємодіями і їх координацією і управлінням. Можна, припустити, що процесний підхід є доповненням системного підходу, який дозволяє розглядати динамічну сторону системи, отримуючи нову інформацію для глибшого дослідження.

Підхід базується на наступних ключових поняттях:

– множина входів. Ними можуть бути різні вимоги ресурсів для виконання процесу;

– множина виходів. Задоволені вимоги, результати процесу. При цьому виходи можуть бути входами для інших процесів;

– діяльність. Дії для досягнення поставлених вимог і результатів.

Ефективність процесу визначається порівнянням між досягнутими результатами і використаними ресурсами.

Процесний підхід щодо оцінки захищеності банківських систем. IDEF

Процесний підхід знайшов застосування в такому методі моделювання, як IDEF. Методологія IDEF складається з трьох методологій:

– IDEF0 – використовується для створення функціональної моделі, яка відображає структуру і функції системи, а також потоки інформації матеріальних об'єктів;

– IDEF1 – застосовується при розробці і побудові інформаційної моделі, яка характеризується структурою і змістом інформаційних потоків, необхідних для підтримки функцій системи;

– IDEF2 – застосовується при реалізації динамічної моделі, характерними моментами якої є зміна в часі поведінка функцій інформації і ресурсів системи.

Процесний підхід щодо оцінки захищеності банківських систем. IDEF0

У своїй основі методологія *IDEF0* використовує наступні, визначення:

– модель – штучний об'єкт, що є повним або частковим відображенням реальної системи і її компонентів. Вона описує, що відбувається в системі, як нею управляють, які засоби використовує для свого функціонування, які сутності вона перетворить, що отримує на виході;

– блочне моделювання і графічне представлення. Описана методологія представляє систему у вигляді набору взаємодіючих і взаємозв'язаних блоків, що відбивають процеси операції дії;

– лаконічність і точність. Застосована в методології графічна мова дозволяє однозначно і точно показати усі елементи системи;

– суворість і формалізм. Незважаючи на свою гнучкість, IDEF0 вимагає дотримання ряду правил, що забезпечують переваги методології відносно однозначності, точності і цілісності складних багаторівневих моделей.

Процесний підхід щодо оцінки захищеності банківських систем. IDEF0

У своїй основі методологія *IDEF0* використовує наступні, визначення:

– модель – штучний об'єкт, що є повним або частковим відображенням реальної системи і її компонентів. Вона описує, що відбувається в системі, як нею управляють, які засоби використовує для свого функціонування, які сутності вона перетворить, що отримує на виході;

– блочне моделювання і графічне представлення. Описана методологія представляє систему у вигляді набору взаємодіючих і взаємозв'язаних блоків, що відбивають процеси операції дії;

– лаконічність і точність. Застосована в методології графічна мова дозволяє однозначно і точно показати усі елементи системи;

– суворість і формалізм. Незважаючи на свою гнучкість, IDEF0 вимагає дотримання ряду правил, що забезпечують переваги методології відносно однозначності, точності і цілісності складних багаторівневих моделей.


Дякую за увагу
Лекцію закінчено