ГЛАВА 5
ОЦІНКА РИЗИКІВ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

Підходи до оцінки захищеності банківських систем

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

В теперішній час, інформаційна безпека як галузь науки, знаходиться на етапі теоретико-концептуального підходу, який в даний момент є перспективним і таким, що розвивається. 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. Приміром, 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.

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 (таблиця 5.1).

Таблиця 5.1

Етапи 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

Продовження табл.5.1

	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. 7. 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.

Як видно з таблиці, 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 уразливостей, які не можуть бути усунені за короткий проміжок часу;

– перевірити правильність усунень уразливостей;

– 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.

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.

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 усієї 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 інформаційної безпеки;

– синтез контрзаходів і обґрунтування їх ефективності.

Спираючись на вищевикладене, можна зробити висновок, що 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. В якості початкових даних використовуються знання експертів або статистичні данні появи тих або інших загроз. Значення кінцевих оцінок залежать не лише від коректності початкових даних, але від вибраної методики і, відповідно, від використовуваної моделі. Зважаючи на описи відкритих систем, приведених в першому розділі, можна сформулювати загальні вимоги до методики оцінки ризиків таких 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 проектується на розроблену 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.

Зупинимося детальніше на принципах побудови моделей визначення поточних і очікуваних значень показників уразливостей. Для цього скористаємося поняттям аналізу ризиків інформаційної безпеки.

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

Опубліковані документи не містять важливих деталей, приміром, критеріїв вибору шкал оцінювання застосованих для оцінки моделі і т.д., які потрібно обов'язково конкретизувати при розробці використовуваних на практиці методик. Таким чином, неможливо запропонувати яку-небудь

єдину, прийнятну для різних типів систем, універсальну методику, яка відповідає відповідній концепції управління ризиками. Проте, 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 оцінка ризиків можна отримати наступним виразом

$$Risk = P_i \times Cl \qquad (5.1)$$

де

P_i - вірогідність події;

Cl - ціна втрати.

При цьому розрізняють трьох факторний підхід, при якому вірогідність події замінюється добутком вірогідності появи загрози на вірогідність використання уразливості.

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 5.1 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 роботи.

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. Зупинимося на них детальніше.

Розглянемо методологію оцінки уразливості інформації. Як правило вона складається з трьох компонентів:

– показники уразливостей;

– загрози інформації;

– моделі визначення поточних і очікуваних значень показників уразливостей.

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

Існує ряд робіт [21, 30] в яких розглянутий підхід оцінки рівня захисту, що використовує структуризацію чинників що впливають на рівень оцінки, а також оцінок цих чинників, визначуваних експертним шляхом. У такому підході проблема визначення вимог до захисту інформації має комплексний характер і повинна розглядатися в двох напрямах: організаційному і 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.

Іншим, 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, необхідне для конкретного типу системи захисту. Причому основою забезпечення безпеки інформаційних технологій є рішення трьох фундаментальних завдань: забезпечення конфіденційності, забезпечення цілісності і забезпечення доступності. Цей підхід закладений в стандартах, що стосуються забезпечення інформаційної безпеки, більшості країн. Він також відбитий в керівних українських документах, ці документи були створені в результаті

дотримань і практичною, діяльності в цій області різних організацій та міністерств 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». Даний підхід створює досить надійну нормативну базу для вирішення практичних завдань в області захисту інформації, визначає вимоги до захисту інформації і закріплює їх в офіційних документах. Проте, з точки зору комплексності, ці документи є недостатніми, оскільки у використаних підходах враховуються далеко не усі чинники, що роблять істотний вплив на уразливість інформації.

Існує досить багато методик визначення, потрібного рівням захисту інформації. Приміром, одна з них 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, якою 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.

Існує також методика, що використовує класифікацію показників інформації залежно від цілей захисту, отримана 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 безлічі цих чинників і адекватніше визначення міри їх впливу на необхідний рівень захисту, що являється на сучасному етапі однієї з найбільш вирішальних завдань. Для досягнення цих цілей використовуються неформально евристичні методи, засновані на знаннях, досвіді і інтуїції спеціалістів захисту інформації [30].

Зважаючи на те, що системи захисту інформації зачисляються до систем з високим рівнем стохастичності, для вищеописаних цілей використовують методи нечітких великих кількостей, лінгвістичних змінних.

Для опису систем застосовуються методи теорії нечітких великих кількостей, де елементи належать тим або іншим множинам лише з деякою

ймовірністю. До таких елементів, наприклад, відносяться ті або інші канали несанкціонованого отримання інформації, засоби захисту і т. п. Вказані елементи належать відповідним множинам лише з деякою вірогідністю, а це призводить до укладення про можливість використання для опису процесів захисту інформації теорії нечітких множин.

Методи теорії лінгвістичних змінних використовуються, для побудови моделей великих систем. Вони ґрунтуються на неформальних судженнях, і висновках експерта-аналітика які формуються виходячи з накопленого досвіду і рішення аналогічних проблем; Основою для теорії служить сукупність трьох посилок.

– в якості міри характеристик систем, що вивчаються, замість числових змінних (чи доповнення до них) використовуються лінгвістичні змінні;

– прості стосунки між змінними в лінгвістичному вимірі описуються за допомогою нечітких висловлювань;

– складні стосунки між змінними в лінгвістичному вимірі описуються нечіткими алгоритмами;

Метод лінгвістичних змінних застосовний, коли строгий опис систем їх функціонування неможливий в силу самого характеру вирішуваної задачі, де відсутні необхідні, дані, як для строгого визначення уразливості інформації, так і для оцінки ефективності вживаних, засобів методів її захисту.

Описані вище нестрогі алгоритми доцільно використати, коли реалізація строгого алгоритму є трудомісткою, а час отримання такого алгоритму обмежене. У зв'язку з тим, що методи нечітких множин або лінгвістичних змінних значною мірою використовують евристичну складову, ефективне рішення з їх допомогою тих або інших проблем може бути забезпечене тільки раціональними діями людей (експертів-аналітиків).

До переваг розглянутих методів можна віднести наступні показники: можливість їх використання для широкого класу об'єктів дослідження, відносну простоту і невимогливість до якості початкової інформації, Експерт, будучи досвідченим фахівцем, в конкретній предметній області має в розпорядженні персональний унікальний фонд інформації, що акумулює не лише його власний, але і увесь відомий йому досвід з цієї проблеми. Він широко використовує в роботі не лише прості логічні будови, висновки, але також інтуїтивні представлення, і творчий підхід.

В той же час методи експертних оцінок володіють, відомими недоліками. В їх числі – суб'єктивність оцінок, заснованих на інтуїтивній

думці експертів; важка порівнянність думок – зважаючи на переважно якісний характер оцінок; необхідність постійного залучення групи висококваліфікованих фахівців. З організаційної точки зору процес прогнозування, досить трудомісткий: він важко піддається формалізації і подальшій автоматизації. До того ж серед безлічі методів експертних оцінок основною є, проблема конкретного визначення і обліку компетентності експерта, як з позиції його професійної придатності до оцінки і прогнозування, так і з позиції його індивідуальної здібності висловлювати конкретні, переконливі судження про поточний і майбутній стан об'єкту дослідження.

Незважаючи на ці недоліки, іноді експертні оцінки є єдиним можливим джерелом інформації про досліджувану систему. Отже, застосування експертних оцінок є обов'язковим, а частенько основним критерієм.

Частково уникнути властивого експертному прогнозуванню суб'єктивізму суджень, допомагає застосування методів колективної експертної оцінки з різними процедурами і методів обробки думок експертів, а також використання на додаток до експертної оцінки методів математичного і імітаційного моделювання. Це судження ще раз доводить самостійність комплексного підходу. При цьому поняття оцінки ризиків, інформаційній безпеці дозволить об'єднати математичні моделі досліджуваної відкритої системи і думки експертів.

Програмні засоби аналізу ризиків банківських систем

Розглянемо існуючі програмні продукти, розроблені для оцінки ризиків різних систем, засновані на різних підходах до аналізу ризиків. Серед них можна виділити Risk Watch, CRAMM, КОНДОР. Ці програмні продукти базуються на різних підходах до аналізу ризиків і рішення різних аудиторських завдань.

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. Потрібно також відмітити, що в цьому продукті ризики у сфері інформаційної і фізичної безпеки комп'ютерної мережі банка розглядаються спільно. 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 уразливості 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.

CRAMM - інструментальний засіб 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.

Завданням першого етапу є визначення достатності: для захисту системи застосування засобів базового рівня реалізовуючи традиційні, функції безпеки, а також необхідність проведення детальнішого аналізу. По суті, завдання першого етапу – відповідь на питання: чи «Досить для захисту системи засобів базового рівня, що реалізовують традиційні функції безпеки, або потрібний детальніший аналіз»?.

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.

Недоліком цього програмного продукту є наступні:

– 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.

Програмний продукт КОНКОР дозволяє фахівцям (IT-менеджерам, офіцерам безпеки) 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 відповідності 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.

Розглянуті методики дозволяють оцінити або переоцінити рівень поточного стану безпеки банківської системи понизити потенційні втрати шляхом підвищення стійкості функціонування корпоративної мережі розробити концепцію і політику безпеки банківської системи, а також запропонувати плани захисту від виявлених загроз і уразливих місць.

Аналізуючи програмні продукти, можна відмітити, що для дослідження вони є «чорними ящиками», міжкомпонентна взаємодія яких прихована від користувача, що не розголошується. Такі програми є комерційними продуктами, ціна яких досить велика.

Можна відмітити, що ці програмні продукти є, потужні засоби опитуванням як експертів інформаційної безпеки так і менеджерів організації, в якій проводиться оцінка ризиків. У гетерогенному середовищі використати такий підхід не ефективно із-за різнорідності складових системи – як в організаційному, так і в програмно-технічному аспектах. В цьому випадку є два варіанти вирішення проблеми неефективності розглянутих програмних продуктів. Використати комплексний підхід оцінками ризиків на основі вже існуючих методик або розробити методику, яка дозволила б врахувати різнорідність середовища досліджуваної системи.

У першому випадку виникає проблема трудомісткості і сумісності отриманих оцінок як наслідок складності отримання, точних, і ефективних висновків.

Другий підхід є привабливішим, оскільки дозволить створити оптимальну методику для оцінки захищеності в гетерогенному середовищі відкритих систем і ефективно використати її надалі. Оптимальність в другому підході може бути досягнута сукупністю розробки комплексу моделей, що описують відкриту систему для її подальшої оцінки думками експертів по відношенню до досліджуваної системи.

Системний підхід щодо оцінки захищеності банківських систем

Розглянемо підхід, який використовується при аналізі 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. При цьому усі засоби, методи і заходи, використовувані для захисту інформації, об'єднуються в цілісний механізм - систему захисту. 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, певний результат, що відбувається усередині системи і має:

– стан – положення системи відносно інших її положень. Таким чином, 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 має ряд властивостей, серед яких можна виділити :

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

– ієрархічність будови, тобто наявність безлічі (принаймні, двох) елементів, розташованих на основі підпорядкування елементів нижчого рівня,

– елементам вищого рівня. Реалізація цього принципу добре видно на прикладі будь-якого конкретного банку. Як відомо, будь-який банк є взаємодія двох підсистем: та, що управляє і та, яка керує, де одна підкоряється іншій;

– структуризація, що дозволяє аналізувати елементи системи і їх взаємозв'язку у рамках конкретного банку структури. 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.

Приведені вище постулати і властивості не можна розглядати догматично. Специфіка будь-якої системи полягає в тому що, її цілі, для яких сукупність об'єктів розглядається як окрема система (чи підсистема), можуть бути не властиві основним цілям системи. Також слід зазначити, що іноді підсистему інформаційної безпеки складно виділити в окремо дану систему зважаючи на щільну взаємодію з іншими підсистемами. В цьому випадку вона буде неповною і (чи) невизначеною, що у свою чергу може негативно відбитися на оцінці захищеності системи. Ще одним недоліком можна

вважати спосіб аналізу, який визначається не лише метою аналізу, але і суб'єктивною думкою аналітика.

Іншим, актуальним підходом до аналізу систем, у тому числі і систем інформаційної безпеки, є процесний підхід. Він 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 – 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.

Такий підхід базується на наступних ключових поняттях:

– безліч входів. Ними можуть бути різні вимоги ресурси для виконання процесу;

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

– діяльність. Дії для досягнення поставлених вимог і результатів.

При цьому ефективність процесу визначається порівнянням між досягнутими результатами і використаними ресурсами.

На практиці процесний підхід знайшов застосування в таких методах 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;

– IDEF 2 - застосовується при реалізації динамічної моделі, характерними моментами якої є зміна в часі поведінка функцій інформації і ресурсів системи.

Слід зазначити, що найбільше поширенням отримали, методології IDEF0 і IDEF1. 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.

Використовуючи процесний підхід в області ІБ, дії в системі можуть бути представлені, у вигляді процесів, що дозволяє виділити основні і допоміжні процеси. Як відомо, механізми ІБ, а також будь-які дії, що виконуються в банківській системі процесами, і представлення моделі у вигляді взаємодії процесів, задасть контекст високого рівня, який дозволить розглянути управлінські, інформаційні і інші ресурси у рамках забезпечення інформаційної безпеки цієї системи. Такий підхід дасть початковий рівень формалізації на етапі дослідження інформаційної системи.

Існує безліч різних методик, використаних для оцінки захищеності банків і банківських систем. До переваг розглянутих методів і моделей можна віднести достатню універсальність, яка використовується для великої кількості об'єктів дослідження. Проведений аналіз дозволяє виконати постановку завдання для подальшої роботи.

Можна припустити, що для підвищення якості прогнозування і оцінки рівня захищеності потрібне використання комплексності методів шляхом доповнення експертних оцінок і застосуванням методів математичного і імітаційного моделювання. Це дасть своєрідний синтез деякої людино-машинної системи, що формалізує знання експерта (у тому числі і інтуїтивні) в конкретній предметній області шляхом проведення обчислювального експерименту з комплексом математичних моделей. Також слід зазначити, що відкриті системи - це сукупність різнорідних елементів, частин, що

взаємодіють між собою у рамках цілей функціонування. Застосування методів експертних оцінок буде украй ускладнено із-за необхідності використання великих знань в різних областях інформаційних технологій. Цей факт ще раз підкреслює вибір комплексного підходу до оцінки захищеності банківських відкритих систем.