НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»
В.о. завідувача кафедри

_____ М.В.Грайворонський
(підпис)

“____”_____2019 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.040301 «Прикладна математика»

на тему: Рефлексивні моделі ризику

Виконав (-ла): студент (-ка) 4 курсу, групи ФІ-51
(шифр групи)

Нгуен Дик Мань

Керівник д.т.н., проф. Архипов Олександр Євгенійович

Консультант_____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 року

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Рефлексивні моделі ризику» містить 72 сторінок, 16 рисунків, 4 таблиць, список літератури з 15 найменувань.

Мета: формалізація методу аналізу високорівневих ризиків для визначення рівня інвестиції в СЗІ.

Об’єкт дослідження: Інформаційні ризики організацій

Предмет дослідження: Типізація інформаційних ризиків виходячи з мотиваційно-економічних можливостей атакуючої сторони.

В результаті виконання завдання роботи було проаналізовано поведінку економіко-вартісної моделі оцінки та аналізу ризиків. Ознайомлені з поведінкою рефлексивних моделей атакуючої сторони

РЕФЕРАТ

Пояснительная записка к дипломной работе «Рефлексивные модели риска» содержит 72 страниц, 16 рисунков, 4 таблиц, список литературы из 15 наименований.

Цель: формализация метода анализа высокоуровневых рисков для определения уровня инвестиции в СЗИ.

Объект исследования: Информационные риски организаций

Предмет исследования: Стандартизация информационных рисков исходя из мотивационно-экономических возможностей атакующей стороны.

В результате выполнения задачи работы были проанализированы поведение экономико-стоимостной модели оценки и анализа рисков. Ознакомлены с поведением рефлексивных моделей атакующей стороны.

ABSTRACT

Explanatory note to the thesis "Reflexive risk models" contains 72 pages, 16 figures, 4 tables, a bibliography of 15 titles.

Objective: formalization of the method of analysis of high-level risks to determine the level of investment in GIS.

Object of research: Information risks of organizations

Subject of research: Typization of information risks based on the motivational and economic capabilities of the attacking party.

As a result of the task, the behavior of the economics and value model of risk assessment and analysis was analyzed. Familiar with the behavior of the reflexive models of the attacking side

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ФІПЗІР – функція імовірності порушення захищеності інформаційного ресурсу.

ІБ – інформаційна безпека.

ОАР – оцінка та аналіз ризиків.

НСД – несанкціонований доступ.

ISO – International Organization for Standardization.

EBIS – Очікуваний прибуток від інвестицій в інформаційну безпеку

РОП – Ризик-орієнтований підхід

СЗІ – Системи Захисту Інформації

ВСТУП

На поточний момент необхідність захисту інформації, а відтак необхідність інвестування коштів в її безпеку, не викликає сумнівів. Однак наразі актуальним залишається питання про обсяги цих інвестицій. У даної проблеми є два основні аспекти: перший – оцінка вартості безпосередньо самих активів, для яких здійснюватиметься розгортання КСЗІ, і другий – визначення розмірів витрат на здійснення заходів спрямованих на реалізацію безпеки інформації. Як ціна самого об'єкта, що охороняється, так і сума інвестицій у захист зазвичай присутні в якості параметрів в моделях, які описують оцінку та аналіз ризиків. Таким чином є сенс використовувати для вирішення вище поставлених питань саме методи ОАР.

Актуальність роботи. Так як серед існуючих моделей для оцінки та аналізу ризиків досі немає переконливого лідера, а компанії, які зацікавлені у вирішенні даного питання не здатні самостійно оцінити необхідні метрики, для винесення рішень щодо інвестування коштів в захист інформації, актуальною залишається задача дослідження методів ОАР, а також вдосконалення та допрацювання вже існуючих, для отримання більш адекватних результатів, а значить і точнішого визначення ефективного рівня витрат на захист.

Мета і завдання дослідження: формалізація методу аналізу високорівневих ризиків для визначення рівня інвестицій у СЗІ.

Об'єкт дослідження: дослідження інформаційних ризиків організації для системи «атака-захист»

Предмет дослідження: Типізація інформаційних ризиків виходячи з мотиваційно-економічних можливостей атакуючої сторони.

Методи дослідження.В даній роботі були застосовані наступні методи

1) Метод систематизації – для вибору необхідних джерел

2) Системний підхід – для систематизації обраних джерел, та фокусування на головних аспектах.

3) Метод аналізу, синтезу і порівнянь – для аналізу проблеми і розробки шляхів її вирішення.

4) Метод логічності і історичності – для знаходження об'єктів дослідження

Наукова новизна одержаних результатів. Отримані рефлексивні моделі отримані в даній роботі мають свої недоліки, але вони дозволяють отримати уяву про загальну необюхідність інвестицій в СЗІ.

Практичне значення одержаних результатів. Досліждення рефлексивних моделей ризику отриманих Ризик-орієнтованим підходом внесе вагомий внесок у вирішення задачі оцінки оптимального рівня інвестицій в захист інформації.

1 ПІДХОДИ ДО АНАЛІЗУ РИЗИКІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ ЗАГРОЗ

1.1 Модель Гордона-Лоєба

В розділі оглядається модель Гордона-Лоєба оцінки оптимального об'єму інвестицій в інформаційну безпеку, даються практичні рекомендації по застосуванню моделі, а також як здійснюється вибір діапазону вразливостей, на якому слід зосередити фінансові ресурси, та характеризуються слабкі сторони моделі.

Гордон і Лоєб запропонували економічну модель [1], яка визначає оптимальний об'єм інвестицій в ІБ для захисту заданого інформаційного ресурсу. Модель розглядає те, як вразливість інформації і потенційні втрати внаслідок такої вразливості впливають на оптимальний об'єм ресурсів, котрі повинні бути вкладені в захист інформації нейтральною до ризику організацією. Ризики в даній моделі вважаються незалежними.

Інформаційний ресурс характеризується такими параметрами:

λ – потенційні збитки від витоку інформації;

t – імовірність нападу, $t \in [0,1]$;

v – уразливість інформації, під котрою розуміють імовірність того, що при відсутності інвестицій атака буде успішною, що завдасть збитки λ; $0 \le v \le 1$;

Хоча λ залежить від використання інформації (самою організацією, конкурентами, хакерами) і змінюється в часі, в моделі розглядається, що λ – фіксоване значення, скінченне і менше деякого дуже великого числа М. таким чином, модель не призначена для випадків захисту національних (державних) активів чи будь-яких інших, де втрати можуть бути катастрофічними. Для катастрофічної втрати λ≥М припущення про нейтральність до ризику організації стає нереалістичним.

Для заданого інформаційного ресурсу імовірність втрати дорівнює vt, а очікувана втрата, обумовлена відсутністю інвестицій в ІБ, дорівнює $vt\lambda$. Таким чином, для будь-якої позитивної імовірності загрози (t > 0) очікувана втрата зростає зі зростанням вразливості.

Для даної моделі робиться спрощення, що організація може інвестувати в зменшення вразливості, але не може впливати на зменшення загроз. Тому імовірність загроз $t > 0$ фіксується, і далі можна сфокусуватись на виборі об'єму інвестицій в цілях зменшення вразливості. Так як $t = const$, визначається значення $L = t\lambda$ – втрати чи потенційні втрати, пов'язані з інформаційним ресурсом.

Вводиться позначення $z > 0$ – це грошові інвестиції в безпеку для захисту даного інформаційного ресурсу, z вимірюється в тих же одиницях, що і потенційні втрати L. Ціллю інвестиції z є зниження імовірності порушення захищеності інформаційного ресурсу. Вводиться $S(z, v)$ – функція імовірності порушення захищеності інформаційного ресурсу (ФІПЗІР) з вразливістю v, при тому, що організація інвестувала z в безпеку цього ресурсу. Будемо називати імовірністю порушення захищеності значення функції $S(z, v)$ при заданих z і v.

Для побудови економічної моделі Гордон і Лоєб припускаються, що функція $S(z, v)$ двічі неперервно диференційована. Природа вразливості і захищеності інформації дозволяє зробити наступні припущення стосовно функції $S(z, v)^2$;

Аксіома 1. $S(z, v) = 0$ для будь-яких z. Якщо інформаційний ресурс абсолютно невразливий, то він буде залишатись ідеально захищеним для будь-якої кількості інвестицій z, включаючи нульові.

Аксіома 2. $S(z, v) = 0$ для будь-яких v. При відсутності інвестицій в інформаційну безпеку, імовірність порушення захищеності інформаційного ресурсу, обумовлена реалізацією загрози, є наслідуваною від ресурсу вразливістю v.

Аксіома 3. Для будь-яких $v \in (0; 1)$ і для будь-яких z, $S_z(z, v) < 0$ і $S_{zz}(z, v) < 0$, де S_z – часткова похідна по z, а S_{zz} – часткова похідна S_z по z. Більше того, згідно з

моделлю Гордона-Лоєба, вважається, що для будь-яких $v\epsilon$ (0; 1), $limS_z(z, v) \rightarrow 0$ при $z \rightarrow \infty$. Таким чином, при достатньому інвестуванні в інформаційну безпеку імовірність порушення захищеності інформаційного ресурсу можна як завгодно наблизити до нуля.

Далі вважається, що ФІПЗІР задовольняє припущенням всіх трьох аксіом. З ціллю визначення кількості грошових засобів для інвестування в захищеність інформації, організація порівнює очікуваний прибуток від інвестицій з вартістю інвестицій. Очікуваний прибуток від інвестицій в інформаційну безпеку, позначений через *EBIS*, дорівнює зменшенню очікуваних втрат організації, обумовленому додатковим захистом:

$$EBIS(z) = [v - S(z, v)]L. \quad (1.1)$$

Очікуваний чистий прибуток від інвестицій в інформаційну безпеку, позначена через *ENBIS*, дорівнює різниці *EBIS* і вартості інвестицій:

$$ENBIS(z) = [v - S(z, v)]L - z. \quad (1.2)$$

Позначимо оптимальні інвестиції через $z^*(v)$.

Із аксіоми 3 слідує, що $S_z(z, v)$строго випукла як функція від змінної z, а значить,*ENBIS*строго ввігнута як функція від змінної z.

Для визначення оптимального рівня інвестицій в ІБ вирішується задача пошуку максимуму функції:

$$ENBIS^*(z) = ENBIS(z^*) = max_z[v - S(z, v)]L - z. \quad (1.3)$$

Звідси максимум $z^*(v) > 0$ знаходиться з умови рівності нулю першої похідної:

$$-S_z(z^*, v)L = 1, \quad (1.4)$$

де ліва частина представляє собою граничний прибуток від інвестицій, а права – граничну вартість інвестицій. Необхідно інвестувати в безпеку тільки до тієї точки, де граничний прибуток від інвестицій дорівнює граничній вартості інвестицій.

Для заданого рівня вразливості оптимальний об'єм інвестицій в інформаційну безпеку z^* зростає зі зростанням загрози t або втрат λ.

Оптимальний об'єм інвестицій в ІБ проілюстрований в рис. 1. Із рівності (1) та аксіом 1 і 2 слідує, що прибуток від інвестицій $ENBIS(z)$ починається в нулі і досягає vL зі зростанням інвестицій. Вартість інвестицій z показана за допомогою прямої, що складає кут 45° з віссю z. Оптимальний об'єм інвестицій z^* знаходиться там, де різниця між прибутком і затратами максимальна. В цій точці дотична до $ENBIS(z^*)$ має тангенс кута нахилу, що дорівнює 1, а це свідчить про те, що граничний прибуток дорівнює граничній вартості.

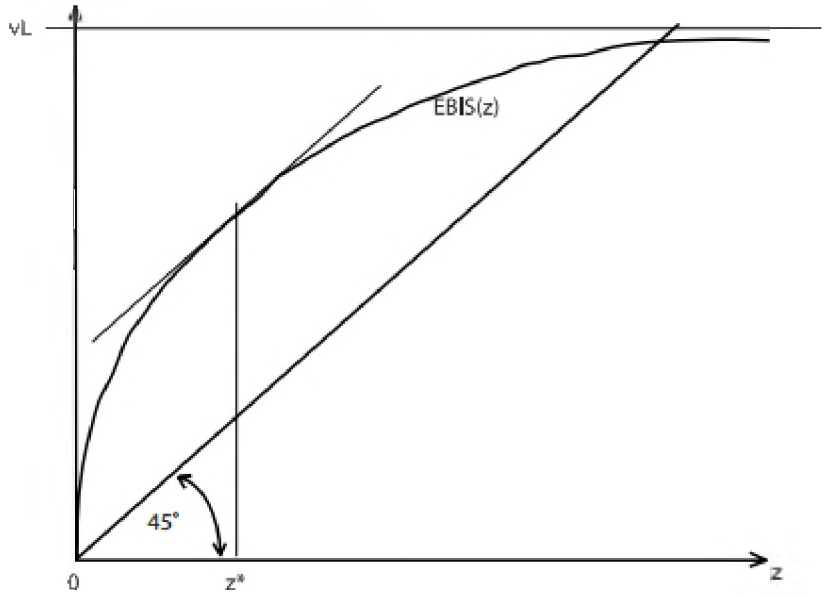

Рисунок 1.1 – Прибуток і вартість інвестицій в інформаційну безпеку

Оптимальний об'єм інвестицій в ІБ дорівнює нулю, якщо граничний прибуток при $z = 0$ менший чи дорівнює граничній вартості такої інвестиції. Ця умова може бути записана у вигляді:

$$L \leq \frac{1}{-S_z(0,v)}. \qquad (1.5)$$

Досліджуються два широких класи функцій $S(z, v)$.

Перший клас, позначений через $S^I(z, v)$, задається як

$$S^I(z,v) = \frac{v}{(\alpha z+1)^\beta}, \qquad (1.6)$$

де параметри $\alpha > 0$, $\beta \geq 1$ – міри ефективності ІБ. ФІПЗІР цього класу лінійні по вразливості. Рисунок 2 показує, як зростання інвестицій в ІБ, *z*, зменшує очікувану втрату від порушення захищеності інформаційного ресурсу. Різниця між значеннями, котрі приймають лінійні функції вигляду *S(z, v)L* в точці *v*, і представляють собою *ENBIS*.

Вираз для оптимального рівня інвестицій в ІБ для $S^I(z, v)$має вигляд:

$$z^{I^*}(v) = ((v\beta\alpha L)^{\frac{1}{\beta+1}} - 1)/\alpha). \qquad (1.7)$$

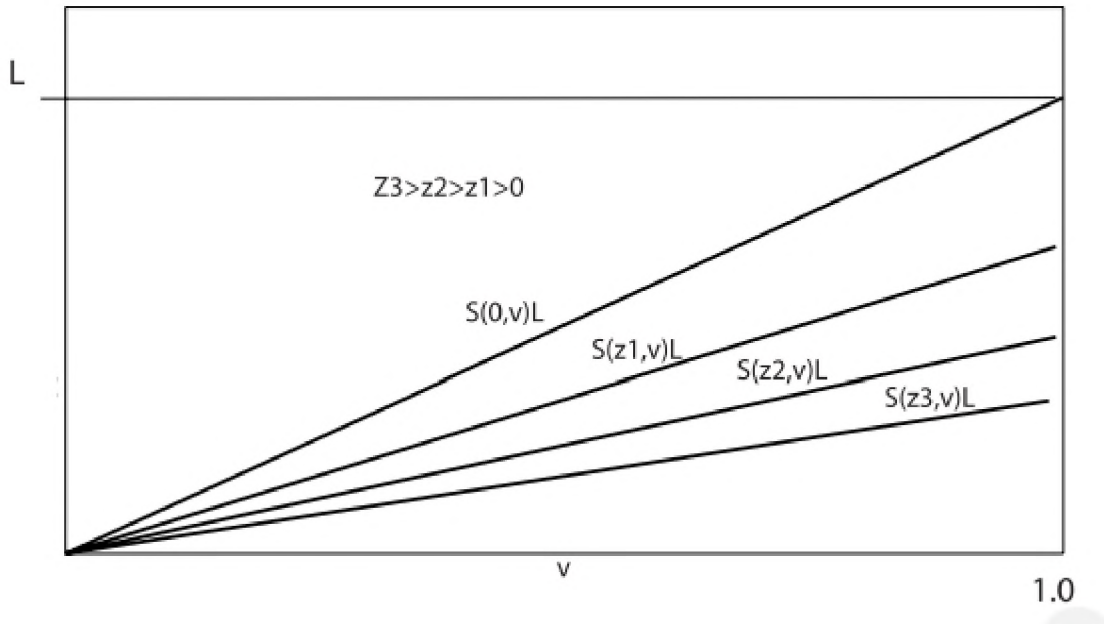

Рисунок 1.2 – Очікуваний об'єм втрат, *S(z, v)L*при збільшенні вразливості, а також при різних рівнях інвестицій в ІБ для першого класу ФІПЗІР

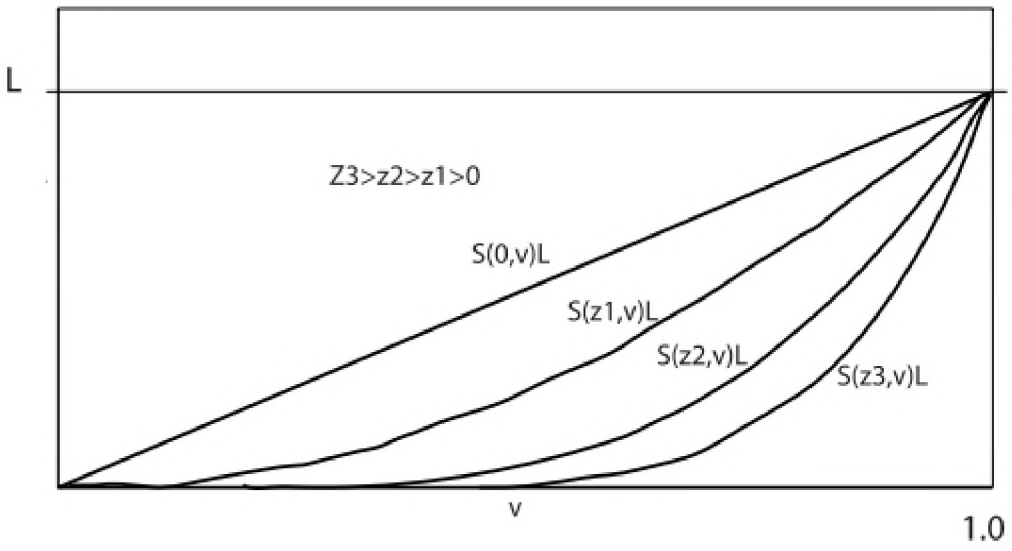

Рисунок 1.3 – Величина очікуваних втрат *S(z, v)L* при збільшенні вразливості, а також при різних рівнях інвестицій в ІБ для другого класу ФІПЗІР

Другий клас ФІПЗІР задається у вигляді $S^{II}(z,v) = v^{\propto z+1}$, де параметр α> 0 –міра ефективності ІБ. Кожна крива на рисунку 3 представляє собою функцію, що належить класу $S^{II}(z,v)$.

Вираз для оптимального рівня інвестицій в ІБ має вигляд:

$$z^{II^*} = \ln\left(\frac{1}{-\propto vL(\ln v)}\right)/\propto \ln v. \qquad (1.8)$$

Гордон і Лоєб доказують, що для ФІПЗІР, які належать до першого і другого класів, оптимальний рівень інвестицій ніколи не перевищує величини 1/e = 36,79% від очікуваних втрат. Для широкого кола функцій, що належать до першого і другого класів, оптимальний об'єм інвестицій в ІБ значно менше максимуму 36,79%.

Для першого класу ФІПЗІР оптимальний рівень інвестицій в ІБ зростає зі збільшенням вразливості ресурсу, а для другого класу ФІПЗІР оптимальний рівень інвестицій в ІБ спочатку зростає зі збільшенням вразливості ресурсу, а потім спадає. Таким чином, другий клас ФІПЗІР показує, що менеджерам слід концентрувати фінансові ресурси на захисті інформації в діапазоні середньої вразливості.

1.2 Розширення моделі Гордона-Лоєба

У вихідне формулювання моделі Гордона-Лоєба можна внести уточнення і розширити її.

Наприклад, ДженВільємсон (JanWillemson) в своїй роботі показує, що аксіома 3 виконується не завжди: із рівності S_z (z, v) < 0 слідує, що якщо спочатку вважалось v = 0, то неможливо зменшити імовірність атаки строго до нуля незалежно від того, наскільки великий об'єм інвестицій вкладається в ІБ. Хоча це і може служити хорошим наближенням для багатьох реальних ситуацій, але цілком точно існують загрози, які можуть бути повністю усунені достатнім інвестуванням в заходи ІБ. Він приводить уточнення цієї аксіоми і формулює аксіому 3': Функція S(z, v) двічі неперервно диференційовна і

$$S_z(z, v) \leq 0 \text{ і } S_{zz}(z, v) \geq 0, \qquad (1.9)$$

А також для будь-яких *v*, $lim\ S(z, v) \rightarrow 0$ при $z \rightarrow \infty$.

Далі шляхом конструювання спеціального класу функцій, що задовольняють аксіомам 1, 2, 3', Вільємсон показує, що оптимальний об'єм інвестицій досягає 50% очікуваних втрат при відсутності інвестицій в ІБ (на відміну від 36,79 в моделі Гордона-Лоєба). Також Вільємсон показав, що якщо прибрати умову неперервності другої похідної ФІПЗІР, то можна отримати рівень оптимальних інвестицій в ІБ, близький до 100% від очікуваних втрат. Можливість прибрати цю умову він обґрунтовує тим, що неперервність першої похідної необхідна для існування другої похідної, але по суті немає причин для другої похідної бути неперервною.

1.3 Підсумки по моделі Гордона-Лоєба та її недоліки

Модель Гордона-Лоєба призначена для оцінки оптимального об'єму інвестицій в ІБ у випадку незалежних ризиків. У випадку застосування даної моделі об'єм інвестицій в ІБ не перевищує 36,97% від очікуваних втрат. При

виборі цієї моделі перш за все слід вирішити, чи можливо знехтувати взаємо зв'язаністю ризиків в даному конкретному випадку. Для цього необхідно дослідити взаємодію даної організації з іншими, а також її положення на ринку. Якщо позитивні і/або негативні зовнішні ефекти суттєві, то застосування даної моделі недоцільне. Позитивні зовнішні ефекти суттєві, коли декілька організацій пов'язані, скажімо, комп'ютерною мережею. В цьому випадку інвестування однієї з організацій в інформаційну безпеку спричинить зменшення вразливості і другої організації. Негативні зовнішні ефекти суттєві, коли велика імовірність того, що збільшення захищеності однієї організації перенаправить атаки зловмисників на дану.

Однак таке можливе лише при умові ідентичності організацій, що далеко не завжди має місце. У випадку неідентичності організацій може виникнути ситуація, коли зовнішніми ефектами можна знехтувати. Наприклад стан ринку такий, що на ньому існує один безумовний лідер, що володіє інформацією високої цінності, і велика кількість наближено ідентичних між собою організацій, чиї продукти не настільки хороші. Тоді негативних зовнішній ефект інвестицій в ІБ безумовного лідера на ідентичні менш успішні організації мінімізується через велике число цих організацій, так як імовірність перенаправлення атаки саме на цю організацію мала. В такому випадку можна застосувати модель Гордона-Лоєба.

Модель Гордона-Лоєба будується на двох класах ФІПЗІР. Аналіз першого класу говорить про те, що менеджерам слід зосередити свої фінансові ресурси на інформаційних ресурсах великої вразливості, тоді як аналіз другого класу показує необхідність інвестування в ІБ інформаційних ресурсів середнього діапазону вразливості. Можна аргументувати вибір одного із двох класів розмірами очікуваних втрат у випадку інвестування в ІБ. Якщо інформація надзвичайної важливості і очікуваний збиток великий, то розумніше вибрати перший клас ФІПЗІР і захищати високовразливі ресурси, щоб мінімізувати втрати. Але не слід забувати, що моделі не розглядають випадок катастрофічних втрат, так як в

даному випадку припущення про нейтральність до ризику організації не підтверджується. У випадку ж, коли очікуваний збиток не настільки великий, прибуток від інвестицій в захищеність високовразливих ресурсів мала. Наприклад, для випадку конфіденційності знання того, що організація продає певний бізнес-модуль, може стати майже загальнодоступною. В цьому випадку через множинні джерела потенційного витоку інформації буде надто дорого контролювати персонал і бізнес-контакти, щоб надати хоча б базовий рівень ІБ. А значить розумніше використовувати другий клас ФІПЗІР і концентрувати фінансові ресурси на захисті інформаційних ресурсів із діапазону середньої вразливості.

В моделі Гордона-Лоєба є і слабкі сторони. В основному це те, що вона містить неточності, котрі, однак не впливають на вибір першого і другого класі ФІПЗІР. Внаслідок незначного ослаблення умови в моделі Гордона-Лоєба стає можливим побудувати приклад, коли оптимальний об'єм інвестицій досягає 50% і навіть 100% від очікуваних втрат. Модель базується на двох специфічних класах функцій ФІПЗІР, і лишається незрозумілим чи дадуть інші класи функцій схожі результати. Також модель не враховує динамічні аспекти, а саме ефект інвестицій. А саме, не розглядається, як зловмисник змінює стратегії своїх атак у відповідь на додаткові інвестиції і ІБ.

Самі автори моделі ГЛ [88,89] відзначили її недоліки:

1. Не існує простої процедури визначення імовірності нападу і уразливості.
2. Проблематичне визначення потенційних втрат від порушення безпеки.
3. Складність реалізації результатів дослідження на конкретному об'єкті.
4. Не враховано, як зловмисник буде міняти свою стратегію при внесенні додаткових інвестицій для захисту, тобто відсутній аналіз протистояння в динамічному режимі.

Не дивлячись на те, що модель ГЛ знайшла широке визнання і одержала свій розвиток в багатьох роботах протягом десяти років з часу її опублікування,

більша частина поставлених питань до сьогоднішнього дня не вирішена. Беззаперечною заслугою авторів моделі є те, що вони вперше ґрунтовно розглянули проблему і визначили функцію уразливості, що є ключовим при розгляді протистояння в інформаційній сфері. Визначення форми функції, яка виражає уразливість динамічної системи, є ключовим завданням при математичному моделюванні інформаційного протистояння.

1.4 Економіко-мотиваційна модель

Як вже зазначалось у попередньому розділі, для моделі Гордона-Лоєба та її численних розвинень характерна суттєва вада: формально-апроксимативний спосіб задання моделі, за яким майже повністю виключається можливість врахування при формування структури й параметрів моделі відомостей про реальні механізми розвитку та реалізації інформаційних загроз і ризиків, що суттєво обмежує практичні аспекти застосування означеної моделі. В цій ситуації інтерес представляють моделі, запропоновані в [3,4] для дослідження мотиваційно-вартісних та економіко-фінансових відносин, характерних для ситуації «атака-захист» в інформаційній сфері.

Розглянемо ситуацію, що виникає при реалізації атакуючою стороною А (зловмисник) загрози T відносно деякого інформаційного ресурсу I, який належить стороні В [3,4]. Вважатимемо, що D – загальна вартість витрат атакуючої сторони А на реалізацію загрози T, g – отриманий при цьому «виграш», величина якого обумовлюється цінністю ресурсу I для зловмисника. Збитки, яких зазнала в цій ситуації сторона В (власник ресурсу I), тобто вартість ресурсу з точки зору його власника, оцінюється ним як q, а загальна вартість реалізованого комплексу захисних заходів дорівнює c.

Наведені дані дають вартісну характеристику ситуації «атака-захист». На базі цих відомостей можна побудувати логіко-евристичну схему експертного

оцінювання ймовірнісних характеристик, що використовуються для обчислення інформаційних ризиків.

Чистий прибуток зловмисника в разі успішної реалізації загрози T складає $Q = g - D$. Якщо цінність ресурсу I для атакуючої сторони А значна, зокрема, якщо $g>>D$, можна припустити, що зловмисник спробує використати будь-які шанси для реалізації цієї загрози. Навпаки, для малих значень g економічні мотиви виникнення загрози T практично відсутні: при $Q = 0$ (або ж $g = D$) атака ресурсу I стає недоцільною, в цьому випадку $P_t = 0$. Для $g<D$ спроба реалізації загрози T втрачає будь-який економічний сенс. Виходячи з цих міркувань, в [3] запропоновано співвідношення:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g}, \tag{1.10}$$

яке може бути використане для оцінювання приблизних (орієнтовних) значень ймовірності активації (виникнення) загрози T.

В загальному випадку ймовірність P_T реалізації загрози T – це добуток $P_T=P_tP_v$, де P_v – ймовірність вдалого використання зловмисником вразливостей інформаційної системи (ІС), що містить інформаційний ресурс I. Значення ймовірності P_v залежить від ступеню захищеності ІС, який в свою чергу зумовлюється обсягом інвестувань c в систему захисту інформації (СЗІ), що з певним наближенням враховується співвідношенням [3, 4]:

$$P_v = \frac{q}{q+sc} \tag{1.11}$$

де s – коефіцієнт, пов'язаний з існуючою у світовій практиці залежністю між рівнем інвестицій c у захист та цінністю критичної інформації для її власника (сторона В) : $s \geq 10 \div 45$ [3,4]. З формули (2) очевидно, що за умов відсутності критичної інформації в ІС (тобто $q=0$) ймовірність $P_v = 0$. При $q >> sc$, тобто при значному рівні критичності ресурсу I й низьких витратах на створення і функціонування СЗІ, ймовірність $P_v \rightarrow 1$. Загалом значення ймовірності при $q = const$ зростає із спадом рівня інвестицій в СЗІ.

Формули (1), (2) дозволяють побудувати оптимізаційну схему, за якою можна буде зробити висновки щодо ефективності та доцільності інвестицій у СЗІ організації. Для цього припустимо [4], що при нульових інвестуваннях у СЗІ організації $P_v = 1$ й вихідний інформаційний ризик становить $R_1 = P_t q$. Інвестування у СЗІ коштів у розмірі призводить (за умов раціональних витрат цих коштів на потреби захисту) до того, що ймовірність успішного використання вразливості стає меншою за 1, тобто $P_v<1$. Залишковий ризик в цьому випадку дорівнюватиме $R = P_t P_v q$, величина втрат, які вдалося попередити – $R_1 - R = P_t q - P_t P_v q = (1 - P_v) P_t q$, а відповідний «прибуток» –

$$\Delta_R = R_1 - R - c = (1 - P_v) P_t q - c. \tag{1.13}$$

Дослідження цього співвідношення на екстремум:

$$\frac{d\Delta_R}{dc} = \frac{s(q+sc) - s^2 c}{(q+sc)^2} P_t q - 1 = 0, \tag{1.14}$$

дозволяє визначити [4] діапазон «розумних» інвестицій: $0<c< q(P_T s–1)/s$, обсяг інвестицій c_{eff}, який забезпечує найбільше значенняΔ_R, значення ймовірності P_v та ризику R *для* цього обсягу інвестицій:

$$\begin{aligned} c_{eff} &= \frac{q}{s}\left(\sqrt{P_t s} - 1\right), \\ P_v\left(c_{eff}\right) &= \frac{1}{\sqrt{P_t s}}, \\ R\left(c_{eff}\right) &= P_t P_v q = q\sqrt{\frac{P_t}{s}} \end{aligned} \tag{1.15}$$

Вираз (2) – це оцінка ймовірності P_v так би мовити з середини, середовища ІС. Ця оцінка аж ніяк не враховує ресурсні можливості нападу. Що б, наприклад, врахувати існуючий взаємозв'язок між витратами D на реалізацію загроз та рівнем інвестицій c у захист, запишемо (2) у вигляді:

$$P_v(c, D) = \frac{q}{q + s\frac{c^2}{D}} \tag{1.16}$$

Очевидно, що зростання витрат D обумовлює збільшення ймовірності P_v, зокрема, якщо $D \to \infty$, то $P_v \to 1$. Залежність $R_1 - R = (1 - P_v) P_t q$ в цьому

випадку матиме логістичний характер, а діапазон «розумних» інвестицій визначатиметься співвідношенням:

$$\frac{qP_t}{2}\left(1-\sqrt{1-\frac{4D}{sqP_t^2}}\right)< c <\frac{qP_t}{2}\left(1+\sqrt{1-\frac{4D}{sqP_t^2}}\right) \quad (7)$$

Цікаво, що моделі (1), (6) дозволяють у аналогічний спосіб дослідити шанси атакуючої сторони А: $R_A = P_t P_v g$, $\Delta_{RA} = P_t P_v g - D$, зокрема, визначитися із рівнем «розумних» витрат D.

1.5 Оцінка оптимального рівня інвестицій згідно з економіко-мотиваційною моделлю

В ході даного дослідження аналізувалась поведінка наведених вище моделей при змінах значень параметрів, що входять до їх складу.

Спочатку досліджувались залежності ризику R та отриманої внаслідок впровадження засобів захисту вигоди Δ_R від величини співвідношення величин q та c. Для простеження даної закономірності значення цінності інформаційного ресурсу приймалося як фіксоване, а сума інвестицій змінювалась у межах: $0.04q \leq c \leq q$. При цьому інші параметри моделі також було фіксовано на певних вірогідних значеннях. Як результат було отримано залежності, що ілюструються наведеним нижче графіком.

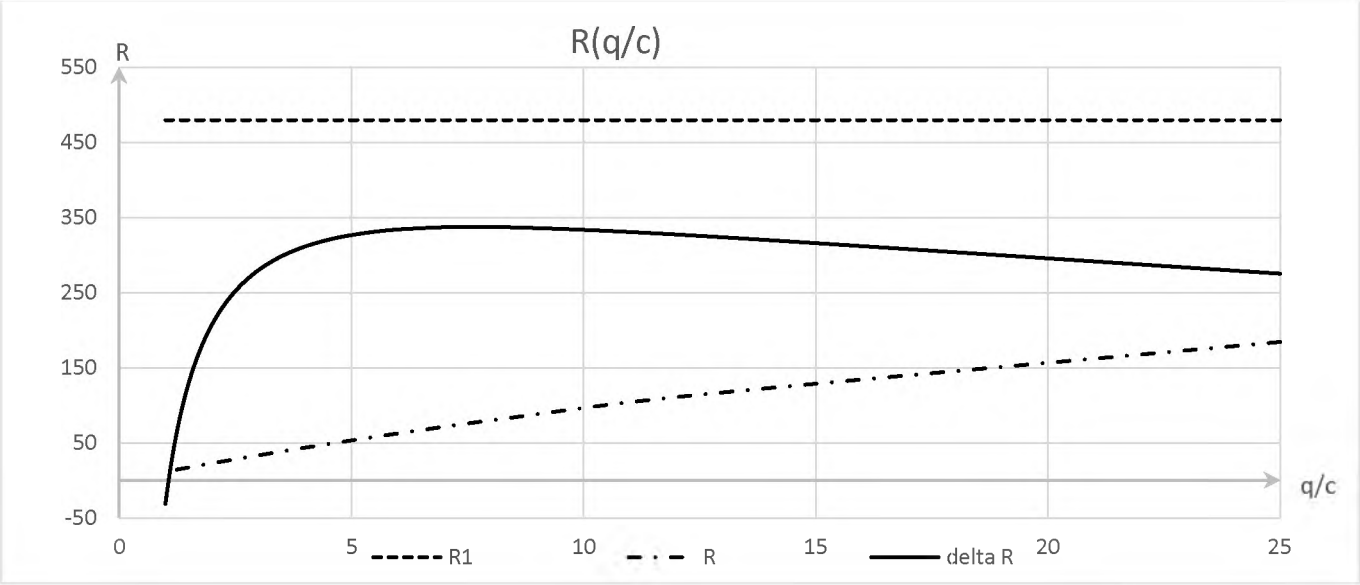

Рисунок 1.4 – Залежність зміни значення ризику від відношення вартості ресурсу до об'єму інвестицій в захист

Із графіку видно, що зі зростанням співвідношення q/c також постійно зростає значення залишкового інформаційного ризику R при сталому значенні вихідного ризику R_1, параметри якого у даному випадку лишаються фіксованими. В свою чергу крива «прибутку» Δ_R стрімко зростає на початку, досягає насичення і у проміжку, коли $\frac{q}{c} \in (5;10)$, майже не змінює свого значення, а потім починає повільно спадати – хоча ризик і продовжує зменшуватись, але витрати на захист все менше окупаються. Таким чином, найбільший «прибуток» отримуємо у ситуації, коли вартість ресурсів в 5-10 разів перевищує витрати на їх захист. Слід також зазначити, що початкові значення, при яких корисність інвестицій у захист стрімко падає до нуля і Δ_R навіть починає приймати від'ємні значення, притаманна для тих ситуацій, коли c починає наближатись до q, що доводить недоцільність надмірних інвестицій в кібербезпеку.

Наступним було дослідження впливу на результуючі модельні показники відношення g/D. В цьому випадку приймалось фіксоване значення виграшу g, який отримає зловмисник у разі успішної реалізації атаки, та змінювався обсяг витрат на її здійснення D у наступних межах: $D \in (0.04g; g)$. Як результат, були отримані значення вихідного ризику R_1, який в даному випадку вже змінювався,

та залишкового ризику R, для обчислення якого приймалось одне фіксоване значення P_v, а також вигоди від впровадження засобів захисту Δ_R.

Отримані для цього випадку залежності демонструють, що крива початкового ризику постійно зростає (спочатку стрімко – на проміжку від 0 до 5, потім повільніше – від 5 до 15, і майже не зростає на залишку графіка). Аналогічно себе поводить і крива R, але з меншим приростом.

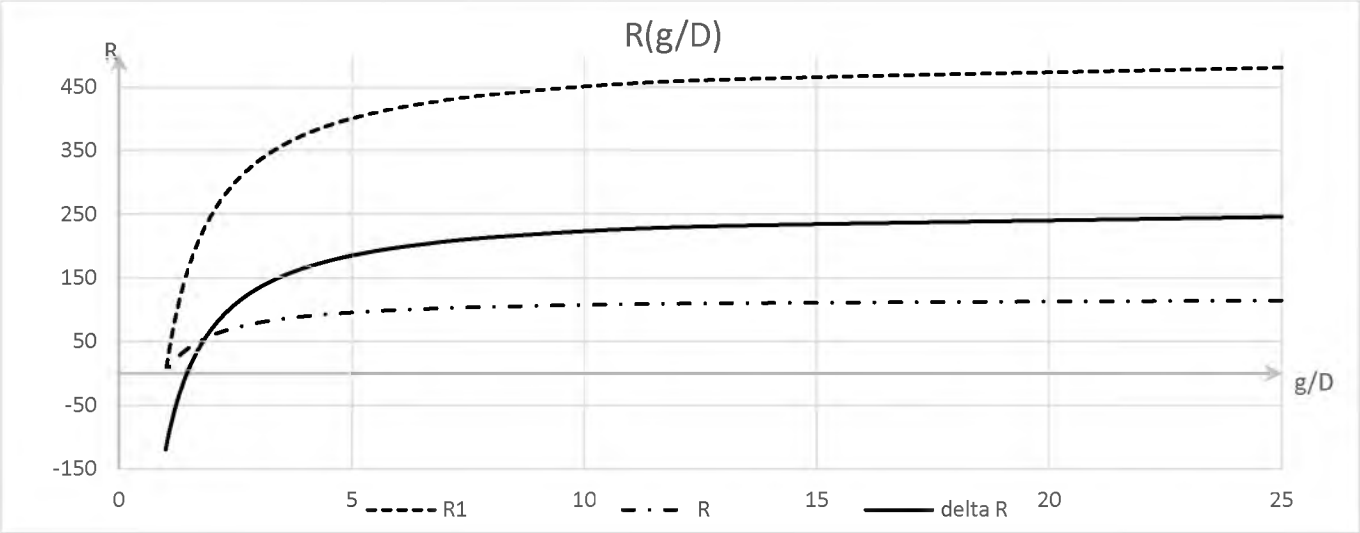

Рисунок 1.5 – Залежність зміни значення ризику від відношення цінності ресурсу для зловмисника до затрат на здійснення атаки

Таким чином можна зробити висновок, що на рівень прибутку від впровадження засобів захисту Δ_R зловмисник може відчутно вплинути лише в тому випадку, якщо наближатиме витрати на здійснення атаки до цінності інформаційного ресурсу (в сенсі цінності цього ресурсу для зловмисника). Різке зниження кривої Δ_R починається вже з моменту, коли D складає 1/5 від g. З іншого боку, значення цієї кривої на ділянці від 10 до 25 якщо і зростають, то дуже повільно. Це можна пояснити тим, що у випадку, коли затрати сторони, що атакує, не складають менше 1/10 частини від цінності ресурсу, то це майже не впливає як на вихідний ризик R_1, так і на прибутокΔ_R. Отже із незначними інвестиціями в атаку зловмисник не здатний кардинально впливати на захищеність системи.

Одним із основних недоліків моделі Гордона-Лоєба є те, що її автори ніяк не враховують, як може вплинути на інформаційний ризик прибуток від реалізації атаки, отриманий зловмисником. Цей показник у моделі оцінки та аналізу ризиків кібербезпеки є одним із ключових, так як він служить основною мотивацією для сторони, що здійснює атаку. Іншим важливим аспектом даного питання є те, що цей показник може абсолютно відрізнятись від вартості, в яку оцінює свої інформаційні активи власник ресурсу, зокрема – в багато разів її перевищувати. Це легко зрозуміти на прикладі, коли вкрадена інформація може бути продана декілька разів. Одночасно із тим оцінку вигоди для зловмисника рідко можна точно спрогнозувати, тому доцільним є розгляд різних можливих рівнів «виграшу». Графіки нижче демонструють як впливатиме зміна даного компонента моделі на результуючі значення, які нас цікавлять.

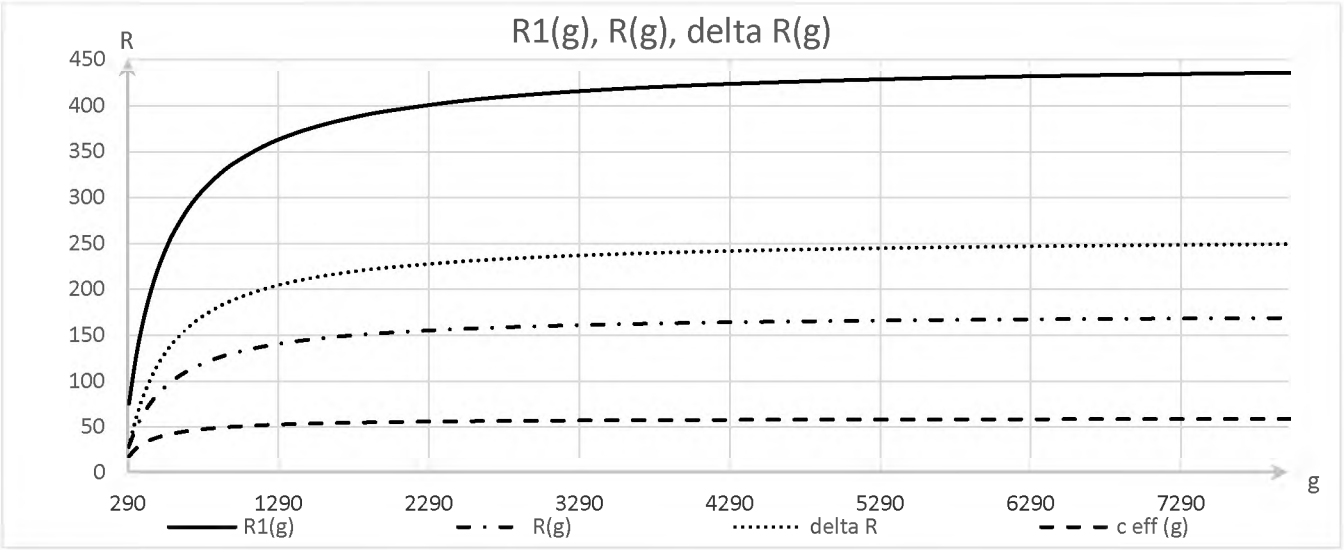

Рисунок 1.6 – Залежність зміни розрахованих значень ризиків від оцінки цінності ресурсу для зловмисника

Приведені на рисунку 3 графіки демонструють, що стрімке зростання значення ризику відбувається на початкових фазах наведених залежностей, звідси можна зроби висновок, що для коректної оцінки рівнів ризиків необхідно хоча б приблизно оцінити вигоди, які може отримати зловмисник, так як початкове зростання цінності ресурсу I для зловмисника найбільше впливає на результуюче значення імовірності активації (виникнення) загрози P_t, що обчислюється за

формулою (1), а у випадку використання в моделі для обчислення ймовірності реалізації вразливості формули (6), також і на значення P_v, що в результаті відобразиться на показнику ефективного рівня інвестицій, який може виявитись недостатнім (при недооцінюванні корисності інформації для сторони, що атакує).

Остання ситуація, що розглядається для даної моделі – це випадок зі зміною доступних зловмиснику засобів для проведення атаки. Як це очевидно випливає із формули (1), у разі, якщо цінність інформаційного ресурсу не перевищує отриманої вигоди, то, відповідно, зникає економічна доцільність реалізації загрози, а значить і імовірність $P_t \rightarrow 0$. Але слід зауважити також про те, що у випадках, коли різниця між інвестиціями в кібербезпеку та у напад значна, це відповідним чином впливає на результуючу ймовірність реалізації загрози. Дану закономірність ілюструє графік нижче. Тут для обчислення P_v використовуються два способи: зокрема, крива Pv1 – обрахована із застосуванням формули (2), а крива Pv2 – за формулою (6), у якій пропонується можливий варіант врахування зв'язку між c і D.

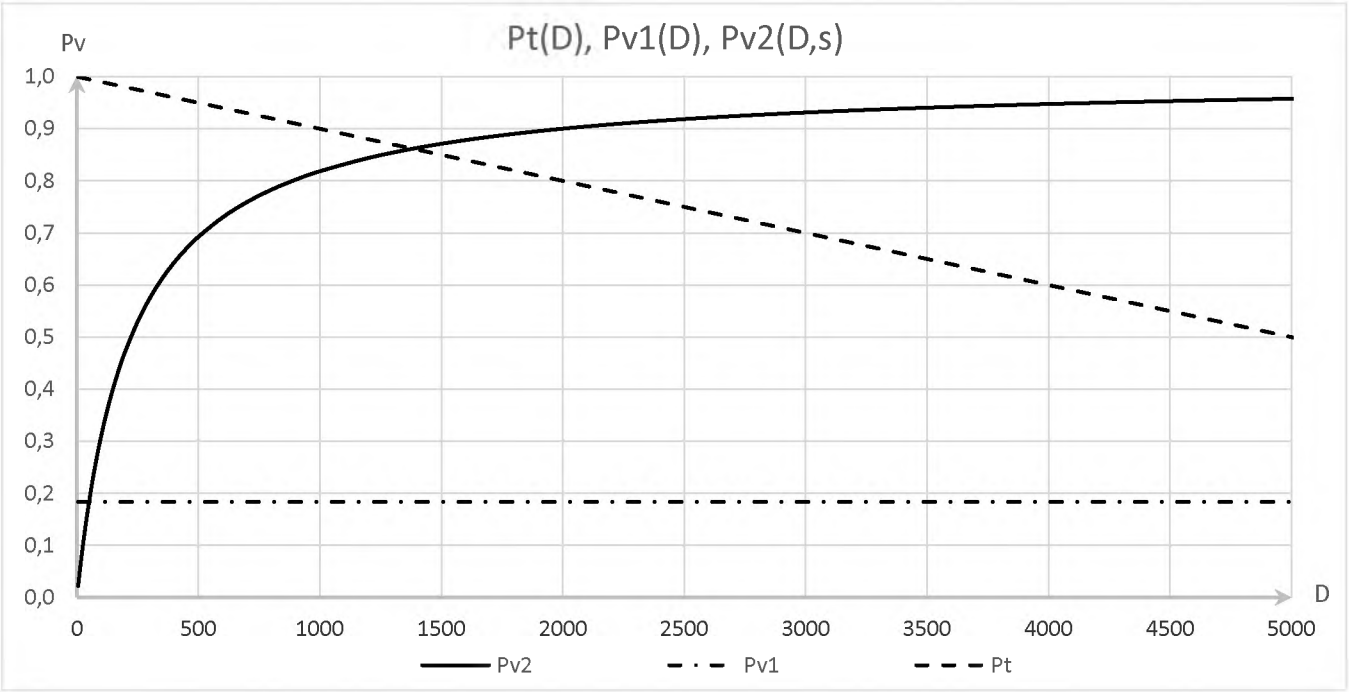

Рисунок 1.7 – Залежність зміни імовірності реалізації загрози від засобів витрачених зловмисником на атаку

Для даного прикладу значення $D = 0.1c \div 100c$.Таким чином, можна дійти висновку, що при наявності у зловмисника необмежених ресурсів нападу, він може звести імовірність реалізації загрози як завгодно близько до 1, особливо у випадках, коли затрати на атаку в багато разів перевищують витрати на кібербезпеку. Іншими словами це можна сформулювати так: неможливо захиститись у випадку, якщо противнику доступні достатньо суттєві ресурси для забезпечення проведення атаки.

Дане дослідження наглядно демонструє існуючі залежності вихідних значень ризиків або факторів ризику від вхідних параметрів, а також від співвідношень цих параметрів. В ході роботи виділено рівні значень вхідних параметрів, при яких прослідковується найсильніший вплив на рівень ризику та прибуток від впровадження засобів захисту. Основним із висновків, які можна зробити, опираючись на одержані результати, є те, що відчутний вплив на результуючий показник ризику як інвестиції у захист, так і затрати на реалізацію атаки, мають, становлячи не більше 20-25 % від вартості інформаційного ресурсу.

1.6 Підтвердження об'єктивності економіко-мотиваційної моделі

На перший погляд може здатись, що немає підстав стверджувати ніби економіко-мотиваційна модель показує справді об'єктивні значення ефективного рівня інвестицій в безпеку інформації. В цьому випадку можна знайти підтвердження доцільності саме такого рівня витрат в авторитетних джерелах, або шляхом збору статистики на підприємствах. Нажаль в ході даного дослідження не було змоги отримати статистичні дані по цьому питанню, тому приводяться погляди на дану проблему з декількох наукових праць, які включають вивчення цієї теми.

Насамперед звернемо увагу на [5], в якій автори Андрощук і Крайнєв стверджують, що не залежно від значення величини втрат, економічні інтереси господарських суб'єктів потрібно захищати. В даному питанні важливо знайти

правильне співвідношення між імовірними втратами і допустимою величиною затрат для їх запобігання чи мінімізації. Затрати на охорону власності пропорційні її величині чи цінності для власника (рис. 1.8). Графік показує, що чим вище цінність власності, що потребує захисту, тим більше коштів допустимо на це витратити. Фірми промислово розвинених країн витрачають на ці цілі від 15 до 20% прибутку, згідно з дослідженнями авторів праці.

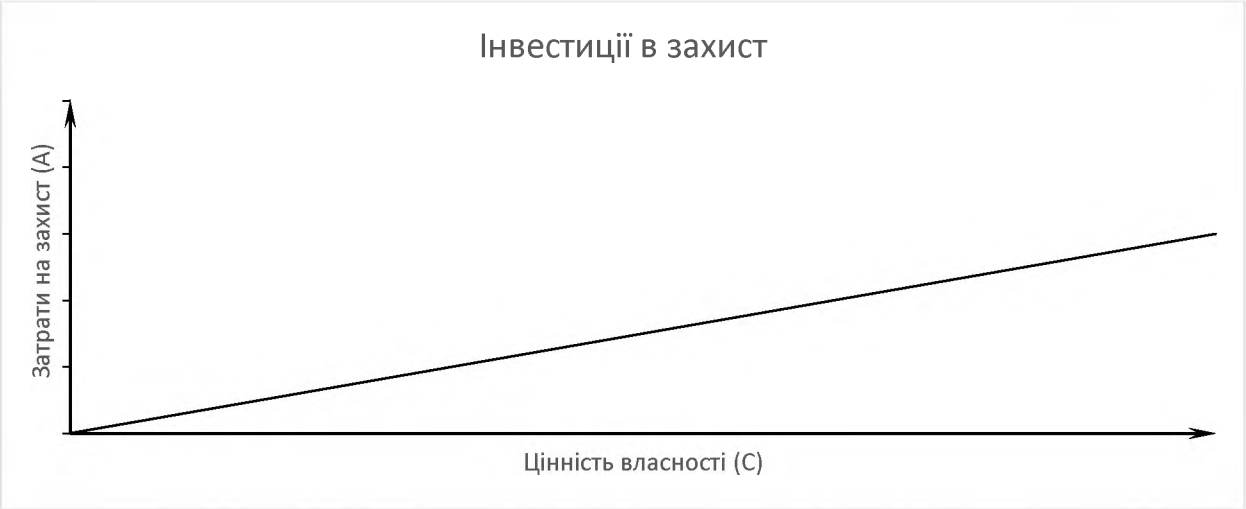

Рисунок 1.8 – Залежність затрат на захист економічних інтересів від величини власності, що захищається

Очевидно, що чим більше виділено засобів на безпеку, тим ефективніший повинен бути захист. Але існує границя або величина максимально допустимих затрат, що визначається рентабельністю. Цю межу можна оцінити, порівнюючи загальні затрати на захист і цінність власності, що захищається. Такі оцінки можуть бути представлені, як лінійні залежності (рис. 1.9).

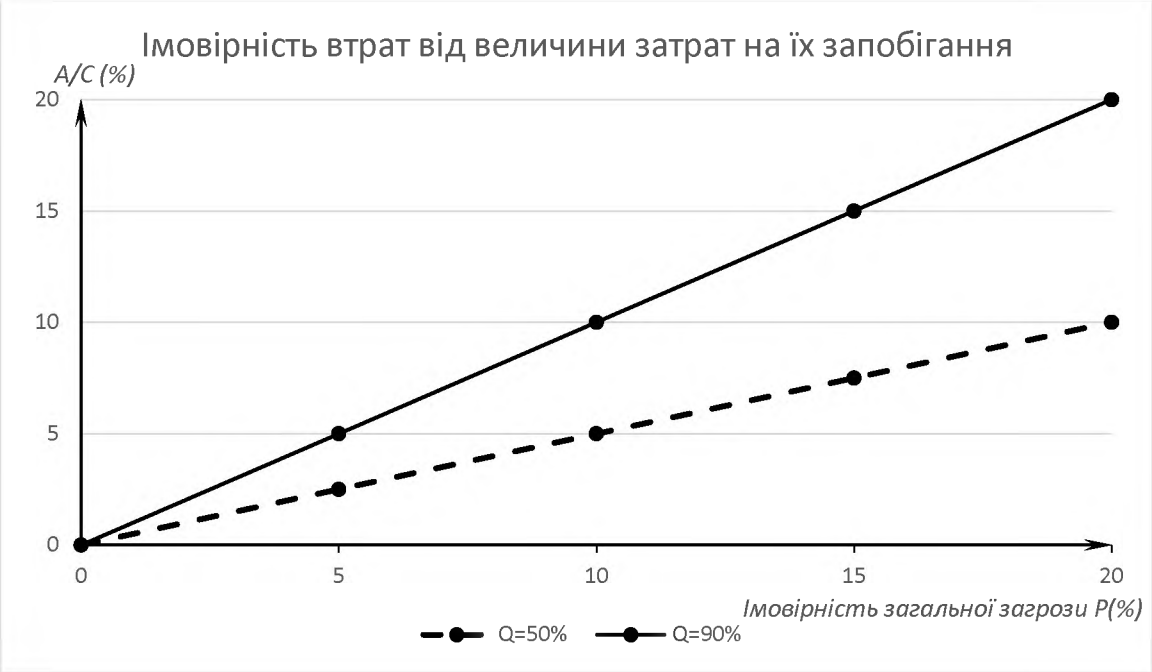

Рисунок 1.9 – Залежність імовірності втрат від величини затрат на їх запобігання

A– затрати на захист;

C– цінність власності;

Q – коефіцієнт захисту.

Однак, як показує практика, стверджують автори, на певному етапі подальший вклад засобів в охорону заходу, захист інформації не завжди підвищує їх ефективність пропорційно затратам.

Розрахунки Андрощука і Крайнєва показують, що для досягнення ефективного захисту *Q*, що дорівнює 50% (при імовірності загрози *P* за середньостатистичними даними, що приблизно відповідають майновим загрозам крупному промисловому підприємству), допустимі затрати на захист *A* повинні досягати 10% доходів. Для досягнення захисту з ефективністю, що дорівнює 90%, при тих же умовах, необхідно витрачати до 15 – 20%.

Інший вчений, що займався вивченням проблеми ефективного рівня інвестувань Петренко С.А.. В своїй монографії[6] він також згадує про долю затрат на інформаційну безпеку в обороті компанії. Згідно з його даними, там де затрати на безпеку належним чином уточнені. Вони можуть складати від 2 до 20%

і більше від об'єму продаж (обороту). Ця оцінка отримана з досвіду роботи автора на основі аналізу стану захищеності інформаційного середовища підприємств металургійної галузі і зв'язку. Типовий розподіл затрат на інформаційну безпеку представлено в табл. 1.1.

Таблиця 1.1– Розподіл затрат на ІБ

Види затрат	**Витрати на безпеку**
Затрати на втрати (зовнішні і внутрішні)	70% від загальних затрат на безпеку
Затрати на контроль	25% від загальних затрат на безпеку
Затрати на попереджувальні заходи	5% від загальних затрат на безпеку

Нехай вказані затрати на безпеку складають 10% обороту. Далі припустимо, що за рахунок збільшення об'єму попереджувальних заходів, а значить і росту попереджувальних затрат вдалось знизити загальні витрати до 6% від обороту. Тепер розподіл загальних затрат на безпеку може бути таким, як описано в табл. 1.2.

Таблиця 1.2 – Розподіл загальних затрат на ІБ.

Види затрат	**Витрати на безпеку**
Затрати на втрати (зовнішні і внутрішні)	50% від нової величини загальних затрат на безпеку
Затрати на контроль	25% від нової величини загальних затрат на безпеку
Затрати на попереджувальні заходи	25% від нової величини загальних затрат на безпеку

Однак загальні затрати на безпеку склали лише 60% від їх початкової величини.

Як новий їх розподіл виглядає по відношенню до початкових загальних затрат на безпеку, показано в табл. 1.3.

Таблиця 1.3 – Розподіл затрат на ІБ

Види затрат	**Витрати на безпеку**
Затрати на втрати (зовнішні і	$\frac{50\times60}{100} = 30\%$ від початкової величини

внутрішні)	загальних затрат на безпеку
Затрати на контроль	$\frac{25\times60}{100} = 25\%$ від початкової величини загальних затрат на безпеку
Затрати на попереджувальні заходи	$\frac{25\times60}{100} = 25\%$ від початкової величини загальних затрат на безпеку
Економія	40% від початкової величини загальних затрат на безпеку

З даних міркувань можна зробити важливий висновок про те, що економія витрат на безпеку неможлива без вдосконалення системи захисту інформації піприємства.

Як бачимо, всі вище згадані джерела вказують на рівні інвестицій, які відповідають тому діапазону значень, що дає на виході економіко-мотиваційна модель оцінки та аналізу ризиків. Таким чином можна погодитись з тим, що отримані з її використанням результати відповідають тим об'єктивним значенням, які реально застосовуються на практиці в компаніях, які приділяють увагу інформаційній безпеці.

Висновки до розділу 1

В розділі розглянуто модель Гордона-Лоєба оцінки оптимального об'єму інвестицій в інформаційну безпеку, даються практичні рекомендації по застосуванню моделі, а також як здійснюється вибір діапазону вразливостей, на якому слід зосередити фінансові ресурси, та характеризуються слабкі сторони моделі.

Але для моделі Гордона-Лоєба та її численних розвинень характерна суттєва вада: формально-апроксимативний спосіб задання моделі, за яким майже повністю виключається можливість врахування при формування структури й параметрів моделі відомостей про реальні механізми розвитку та реалізації інформаційних загроз і ризиків, що суттєво обмежує практичні аспекти застосування означеної моделі. Тому вирішено зосередити дослідження на моделі,

що відображає мотиваційно-вартісні та економіко-фінансові відносини, характерні для ситуації «атака-захист» в інформаційній сфері.

І як підсумок доведено об'єктивність використання для визначення ефективного рівня інвестицій в інформаційну безпеку саме результатів економіко-мотиваційної моделі аналізу ризиків, так як отримані на виході значення співпадають з діапазоном, який успішно застосовується для реальних організацій, згідно з дослідженнями, представленими в монографіях Андрощука і Крайнєва та Петренка.

2 ДОСЛІДЖЕННЯ ЕКОНОМІКО-МОТИВАЦІЙНОЇ МОДЕЛІ

2.1 Перелік затрат на безпеку

Самі затрати на забезпечення інформаційної безпеки являють собою складну структуру, яку можна певним чином класифікувати. Розглянемо детальніше затрати, які можна розбити на кілька груп.

До першої групи можна віднести затрати на обслуговування системи безпеки (на попереджувальні заходи), тобто на:

- управління системою захисту інформації:
  - управління СЗІ підприємства;
  - вивчення можливостей інформаційної інфраструктури підприємства по забезпеченню безпеки інформації з обмеженим доступом;
  - технічна підтримка виробничого персоналу при впровадженні засобів захисту і процедур і планів захисту інформації;
  - перевірка співробітників на лояльність, виявлення загроз безпеки;
  - організація системи допуску виконавців і співробітників конфіденційного ведення справ з відповідними штатами і оргтехнікою;
- регламентне обслуговування засобів захисту інформації:
  - обслуговування і налаштування програмно-технічних засобів захисту, операційних систем і встановленого мережевого обладнання;
  - організація мережевої взаємодії і безпечного використання інформаційних систем;
  - підтримка системи резервного копіювання і впровадження архіву даних;

- проведення інженерно-технічних робіт по встановленню сигналізації, обладнанню сховищ конфіденційних документів, захисту телефонних ліній зв'язку, засобів обчислювальної техніки і т.п.;

- аудит системи безпеки:
  - контроль змін стану інформаційного середовища підприємства;
  - система контролю за діями виконавців;
- підтримка якості обслуговування:
  - забезпечення відповідності вимогам якості інформаційних технологій, в тому числі аналіз можливих негативних аспектів інформаційних технологій, які впливають на цілісність і доступність інформації;
  - доставка (обмін) конфіденційною інформацією;
  - задоволення суб'єктивних вимог користувачів: стиль, зручність інтерфейсів та ін.;
- підтримка довіри до технологій:
  - забезпечення відповідності прийнятим стандартам і вимогам, достовірності інформації, двійсності засобів захисту;
- навчання персоналу:
  - підвищення кваліфікації співробітників підприємства в питаннях використання наявних засобів захисту, виявлення і запобігання загроз безпеки;
  - розвиток нормативної служби безпеки;
- інші затрати:
  - заробітна плата секретарів і службовців, організаційні та інші витрати, котрі безпосередньо пов'язані з попереджувальними заходами.

Другу групу складають затрати на контроль, а саме на:

- планові перевірки і випробування:

- перевірки і випробування програмно-технічних засобів захисту інформації;
- перевірка навиків експлуатації засобів захисту персоналом організації;
- забезпечення роботи осіб, що відповідають за реалізацію конкретних процедур безпеки по підрозділам;
- оплата робіт по контролю правильності вводу даних в прикладні системи;
- оплата інспекторів по контролю відповідності вимогам, пред'явленим до захисних засобів при розробці будь-яких систем (контроль виконується на стадії проектування і специфікації вимог);

- позапланові перевірки і випробування:
  - оплата роботи випробувального персоналу спеціалізованих організацій;
  - представлення випробувальному персоналу (внутрішньому і зовнішньому) матеріально-технічних засобів;
- дотримання політики безпеки:
  - затрати на контроль реалізації функцій управління захистом комерційної таємниці;
  - затрати на організацію тимчасової взаємодії і координації між підрозділами для розв'язання повсякденних конкретних задач;
  - затрати не проведення аудиту безпеки по кожній авторизованій інформаційній системі, виділеній в інформаційному середовищі підприємства;
  - матеріально-технічна підтримка системи контролю доступу до об'єктів і ресурсів підприємства;
- зовнішні контрольні затрати:

- контрольно-перевірочні заходи, пов'язані з ліцензійно-дозвільною діяльністю в сфері захисту інформації;

- аналіз політики безпеки підприємства:
  - ідентифікація загроз безпеки;
  - пошук вразливостей системи захисту інформації;
  - оплата роботи спеціалістів по виявленню можливого збитку і переоцінці степеню ризику.

Третя група включає внутрішні витрати на ліквідацію наслідків порушення політики безпеки, тобто на:

- Відновлення системи безпеки до відповідності вимогам політики безпеки:
  - установка оновлень або придбання останніх версій програмних засобів захисту інформації;
  - придбання технічних засобів замість прийшли в непридатність;
  - проведення додаткових випробувань і перевірок технологічних інформаційних систем;
  - утилізація скомпрометованих ресурсів;
- Відновлення інформаційних ресурсів підприємства:
  - відновлення баз даних і інших інформаційних масивів;
  - проведення заходів з контролю достовірності даних, що піддалися атаці на цілісність;
- Виявлення причин порушення політики безпеки:
  - розслідування порушень політики безпеки (збір даних про методи здійснення, механізм і способи приховування неправомірного діяння; пошук слідів, знарядь і предметів посягання; виявлення мотивів неправомірних дій і т.д.);
  - оновлення планів безперервності діяльності служби безпеки;
- Переробки:

- впровадження додаткових засобів захисту, які потребують суттєвої перебудови системи безпеки;
- повторні перевірки і випробування СЗІ.

Зовнішні витрати на ліквідацію наслідків порушення політики безпеки утворюють четверту групу. Вони пов'язані з:

- Зобов'язаннями перед державою та партнерами (відновлення задоволеності):
  - відновлення довіри споживача, партнерів і держави;
  - юридичні суперечки і виплати компенсацій;
  - розрив ділових відносин з партнерами;
- Тратою лідерства:
  - проведення додаткових досліджень і розробки нової ринкової стратегії;
  - відмова від організаційних, науково-технічних або комерційних рішень, які стали неефективними в результаті витоку відомостей, і витрати на розробку нових засобів ведення конкурентної боротьби;
  - зниження пріоритетності наукових досліджень і неможливість патентування та продажу ліцензій на науково-технічні досягнення;
- Просуванням продукції:
  - ліквідація «вузьких місць» в постачанні, виробництві та збуті продукції;
  - компрометація виробленої підприємством продукції та падіння цін на неї;
  - виникнення труднощів у придбанні обладнання або технологій, в тому числі підвищення цін на них, обмеження обсягу поставок;
- Економічним збитком:

- неможливість виконання функціональних завдань, визначених статутом, та ін.

Чи справді неминучі витрати на інформаційну безпеку? Очевидно, що неможливо повністю уникнути витрат на безпеку, проте їх можна звести до прийнятного рівня. Одні види витрат на безпеку є абсолютно необхідними, інші можуть бути істотно зменшені або виключені і можуть зникнути при відсутності порушень політики безпеки або скоротитися, якщо кількість і руйнівний вплив порушень стане менше.

При дотриманні політики безпеки і проведенні профілактики порушень вдається виключити або суттєво зменшити витрати на:

- Відновлення системи безпеки до відповідності вимогам політики безпеки;
- Відновлення ресурсів інформаційного середовища підприємства;
- Переробки всередині системи безпеки;
- Відновлення довіри державних організацій і партнерів;
- Юридичні суперечки і виплати компенсацій;
- Виявлення причин порушення політики безпеки.

Необхідні витрати обов'язкові навіть при досить низькому рівні загроз безпеки. Це витрати на підтримку досягнутого рівня захищеності інформаційного середовища підприємства.

Неминучими є витрати на:

- Обслуговування технічних засобів захисту;
- Конфіденційне діловодство;
- Забезпечення функціонування і аудит системи безпеки;
- Підтримання мінімального рівня перевірок і контролю із залученням спеціалізованих організацій;
- Навчання персоналу методам інформаційної безпеки.

2.2 Поведінка економіко-мотиваційної моделі для сценаріїв з різними типами порушників

У даному розділі дослідимо поведінку економіко-мотиваційної моделі у випадках із різими типами порушників. Класифікацію атакуючої сторони було здійснено на основі фінансово-технічного забезпечення, а також професійних навиків. Таким чином було виділено три основні типи порушників, для кожного з яких розглянуто окремі сценарії, та вказано ефективні значення інвестувань, виходячи з аналізу моделі.

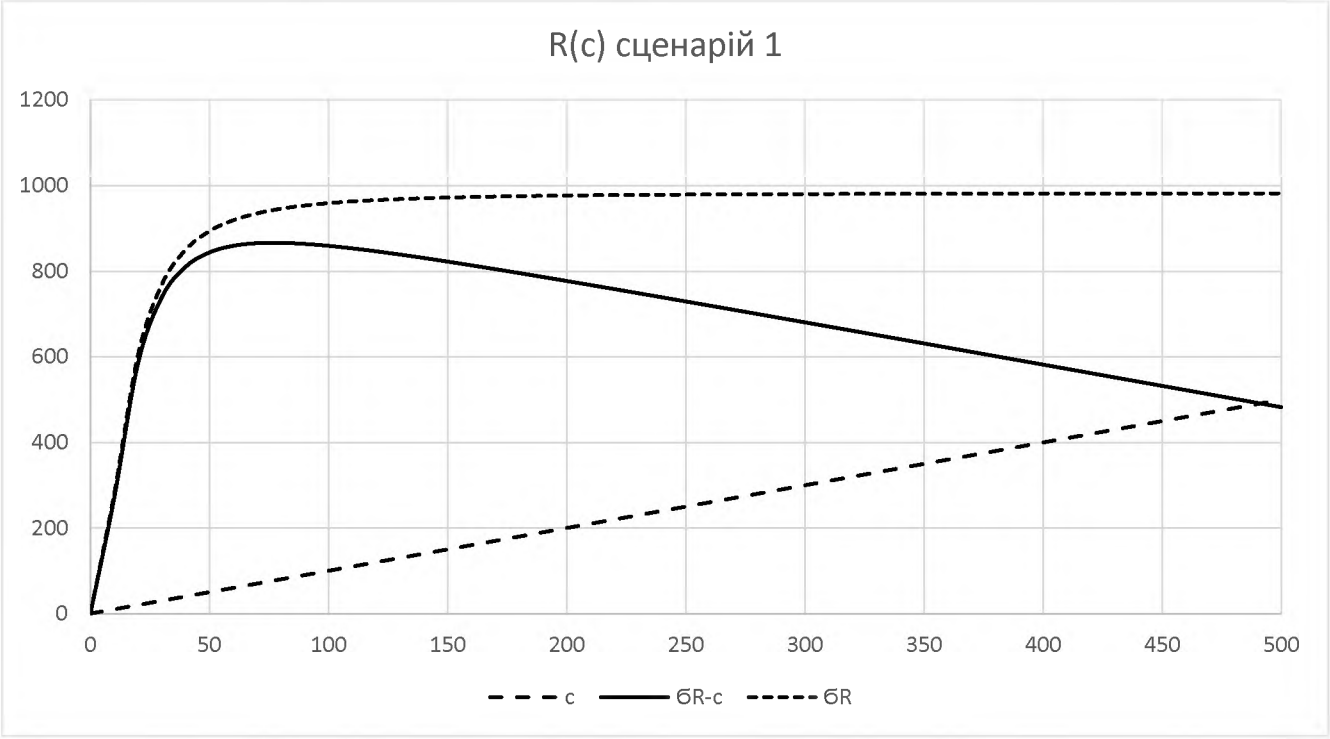

Рисунок 2.1 – Залежність зміни ризику та прибутку він інвестицій в захист у випадку з першим типом порушника

Для першого типу порушника розглядається сценарій, коли фінансово-економічні можливості атакуючої сторони вкрай скромні, зловмисник найімовірніше одинак, який не має достатнього досвіду і знань, необхідних для реалізації ефективних дій. Вважаючи, що асимптотику для цього варіанту отримуємо, досліджуючи співвідношення (1.17). при $D \to 0$, оцінимо граничні значення діапазону допустимих інвестицій:

$$0 \le c \le qP_t . \qquad (2.1)$$

Оціночне значення максимальної величини оптимальних інвестицій в СЗІ для цього випадку очевидно не перевищить $c_{eff\,\max} = 0{,}25q$.

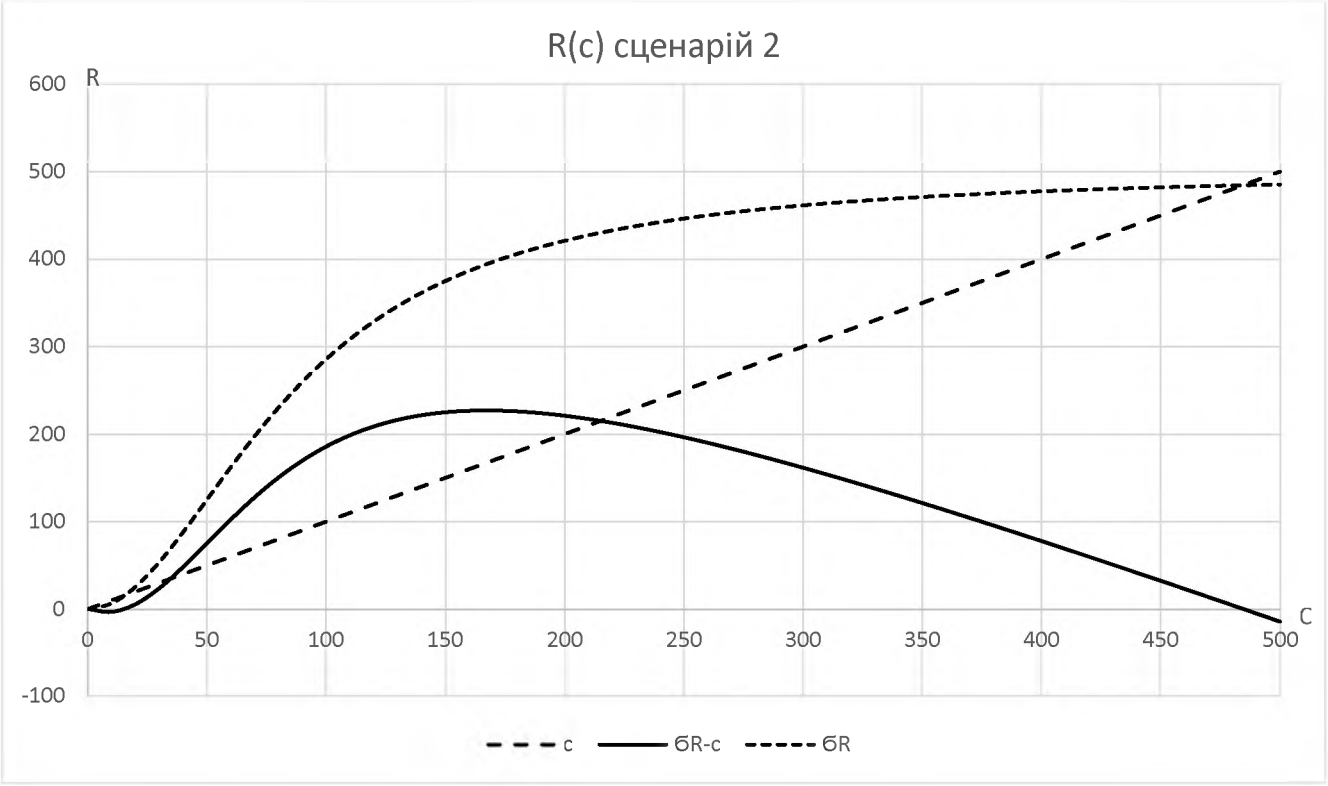

Рисунок 2.2 – Залежність зміни ризику та прибутку він інвестицій в захист у випадку з другим типом порушника

Другий сценарій відповідає ситуації, коли атакуюча сторона – одна особа або група осіб, що володіють достатнім досвідом і необхідними професійними знаннями, але має обмежені фінансово-економічні можливості. Досліджуємо цей варіант, збільшуючи значення інвестицій атакуючої сторони. При$D \to 0.25sqP_t^2$права c_1 і ліва c_2 границі діапазону (1.17) зближаються, стягуючись в точку$c = \frac{qP_t}{2}$ при $D = 0.25sqP_t^2$. У цьому граничному випадку найбільша величина оптимальних інвестицій в СЗІ складе $c_{eff\,max} = 0.5$q.

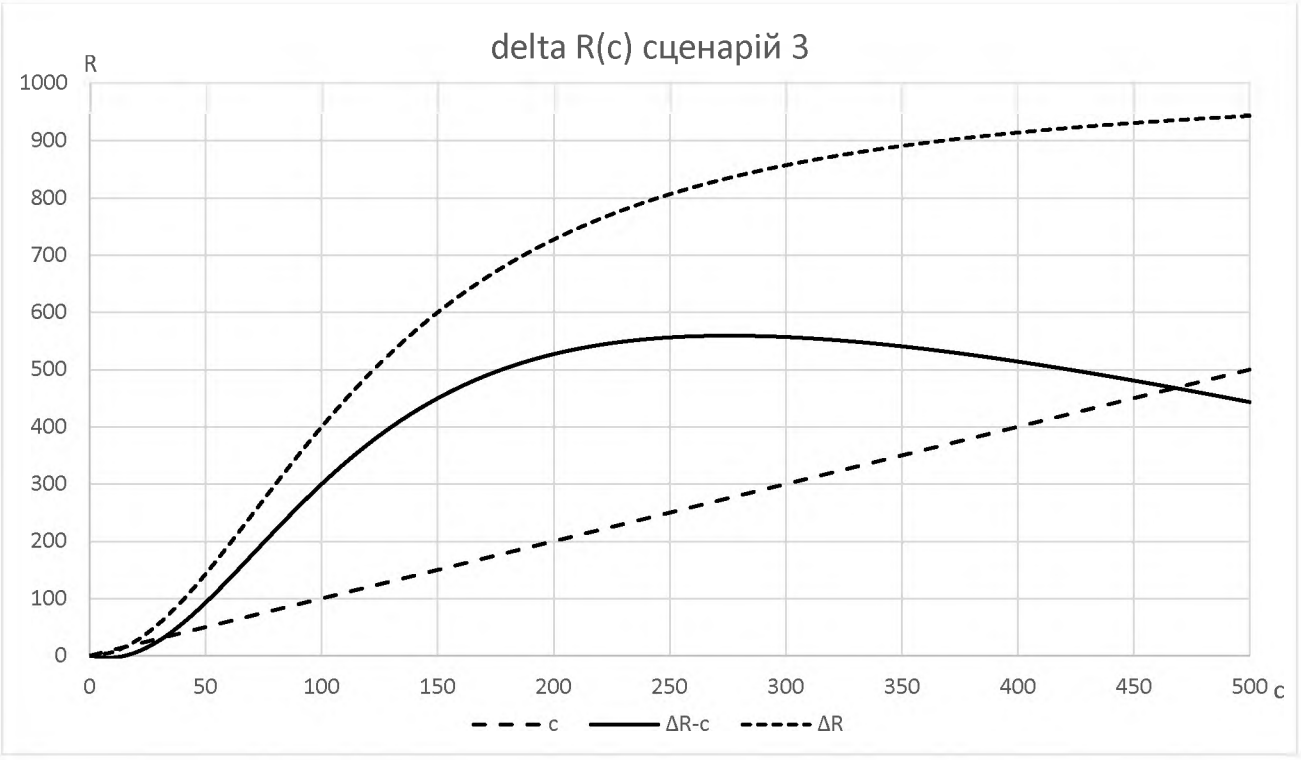

Рисунок 2.3 – Залежність зміни ризику та прибутку він інвестицій в захист у випадку з третім типом порушника

У третьому ж випадку «Зловмисник-виконавець». Модель ризику для цього варіанта має вигляд:

$$R = \frac{q}{q + s\frac{c^2}{D}} q \quad . \tag{2.2}$$

Найсуттєвіша особливість сценарію 3 полягає в тому, що в разі особливої важливості поставленої перед «зловмисником-виконавцем» цілі, він може розраховувати на залучення для підтримки своїх дій певних додаткових ресурсів: фінансових, технічних, інформаційно-аналітичних, оперативних. На практиці це означає можливість реалізації в рамках сценарію 3 дуже високозатратних атак. При цьому очевидно, що якщо $D \to \infty$, то $P_v \to 1$, тобто в цій ситуації успішна реалізація загрози атакуючої стороною А виявляється практично гарантованою. Типовим прикладом подібної ситуації є виконання особливо важливого завдання співробітником спецслужби, є професіоналом, підготовленим до здійснення зловмисних дій в кіберпросторі.

2.3 Проста і складна формули оцінки ризику

Як вже відмічалось в розділі 1.4 в моделі 1.11, яку називатимем простою формулою, ніяк не враховується рівень професійної підготовки сторони, що атакує А, та її матеріально-технічне забезпечення, та відсутнє співставлення цих характеристик за аналогічними характеристиками захисту. В цьому плані більш вдалою може виявитись оцінка імовірності реалізації вразливостей, що обчислюється за виразом 1.16, який будемо називати складною формулою. В ній для імовірності P_t облік ресурсних можливостей сторона А здійснюється шляхом множення значення інвестицій c в знаменнику виразу 1.11 на мультиплікатор c/D, що дозволяє врахувати інвестиції D, які вносяться А в реалізацію атаки. Для варіантів обчислення ризику за складною і простою формулами було побудовано наступні залежності, які представлено нижче.

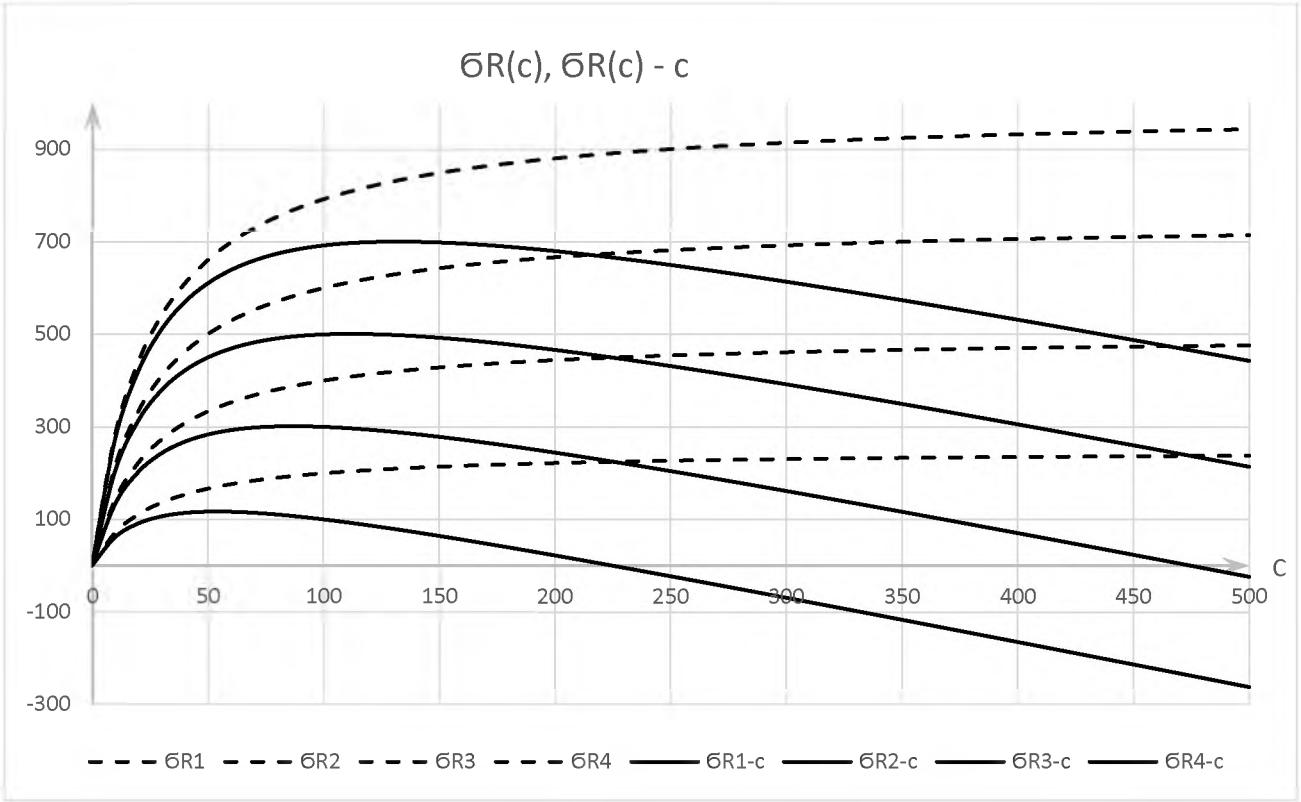

Рисунок 2.4 – Графіки зміни ризику ΔR залежно від інвестицій в захист c при різних значеннях D(проста модель)

Для побудови даних графіків використовувались діапазон значень c={0,500}, при чому для кожного з чотирьох випадків приймались різні рівні інвестицій в атаку. У першому випадку було задано фіксоване значення D = 10, що складало 1/100 від g (виграшу атакуючої сторони). Очевидно, що подібне співвідношення значною мірою відобразилось на величині імовірності реалізації загрози, яка у наступних випадках зменшувалась обернено пропорційно до відношення D/g. Це в свою чергу відобразилось і на рівні ризику, та його зміні. Тобто випадок, коли зловмиснику не доводиться витрачати значних ресурсів на реалізацію загрози характеризується особливо високими ризиками при відсутності, а також при незначних інвестиціях в оборону. Але разом із тим вигода від витрат на безпеку зростає також найбільш стрімко. У наступних же випадках було використано значення затрат атакуючої сторони у розмірах 250, 500 та 750, що становило відповідно ¼, ½ та ¾ від вигоди зловмисника в результаті успішних дій з його боку. Такі значення значно зменшували імовірність реалізації загрози, а значить це призводило в свою чергу до більш повільного наростання як самого ризику R, так і його зміни після витрат на оборону. Тобто виходить, що все ж зміни D при використанні простої моделі не повністю відображають те, наскільки зростання даного параметру впливає на імовірність вразливості, так як формула імовірності вразливості P_v використовує лише інвестиції захисту. Хоча доцільно стверджувати, що зі зростанням витрат на підготовку і проведення атаки повинні також відобразитись на величині вразливості. Тому доцільним можна вважати введення у формулу P_vкоефіцієнта, який би відображав вплив співвідношення коштів інвестованих в атаку та оборону. Подібний підхід дозволив отримати наступні залежності, для тих же значень, що і в попередніх випадках.

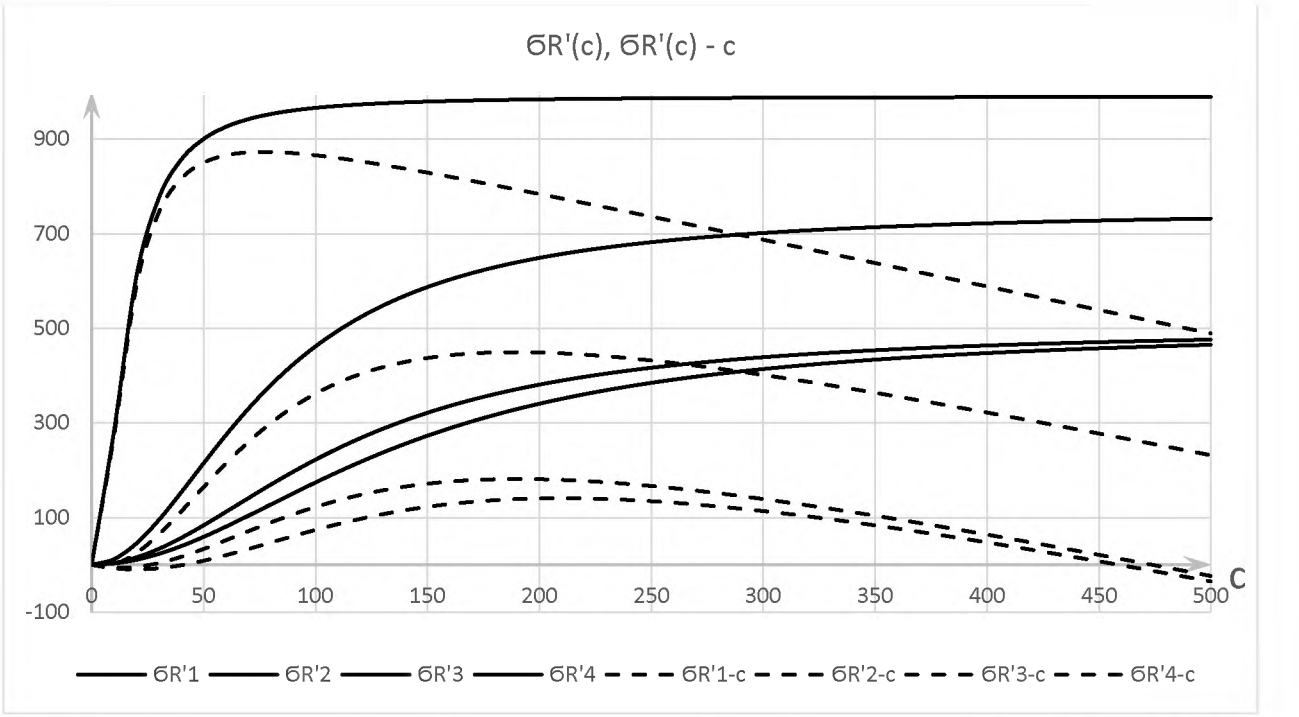

Рисунок 2.5 – Графіки зміни ризику δR залежно від інвестицій в захист c при різних значеннях D(складна модель)

При використанні у розрахунках складної моделі отримуються майже ідентичні графіки зміни ризику лише при незначних значеннях D, але разом із тим прослідковується більш стрімке падіння вигоди від інвестицій у захист одразу після досягнення точки екстремуму. У тих же випадках, коли затрати на атаку значні по відношенню до тих, які спрямовані на їх протидію, рівні, або навіть переважають їх, як це було у третьому (D = 500)чи четвертому (D = 750) варіантах, прослідковується плавне наростання вигоди від витрат на захисні заходи, так само які повільне збільшення зміни ризику. Разом із тим слід відмітити, що при високих D незначні інвестиції c майже зовсім не впливають на рівень захищеності, що досить таки відповідає реаліям. Адже при спробі протистояти зловмиснику, який добре підготовлений та забезпечений необхідними йому ресурсами, маючи при цьому на озброєнні досить дешеву, а значить у переважній більшості неякісну системою захисту інформації, сторона, що обороняється, з високою імовірністю терпить поразку. В цьому плані подібна модель має сенс у реальному житті. Інша цікава деталь, яку можна помітити проаналізувавши графіки зміни вигоди від інвестицій в оборону, що навіть при

значних витратах зловмисника рівні, при яких отримана вигода власника інформації стає максимальною збігаються зі рівнями інвестицій c, при яких вони складали 20% (у випадках, коли $D = g/4$ і $D = g/2$) та 22% ($D = 3g/4$) від вартості активу. Тобто не залежно від подальшого зростання вкладів атакуючої сторони, можна виділити рівень оптимальних інвестицій, який забезпечує максимальну вигоду від проведення заходів спрямованих на захист.

Порівняльну характеристика обох моделей найкраще відображають залежності вигоди він атаки, на одному графіку.

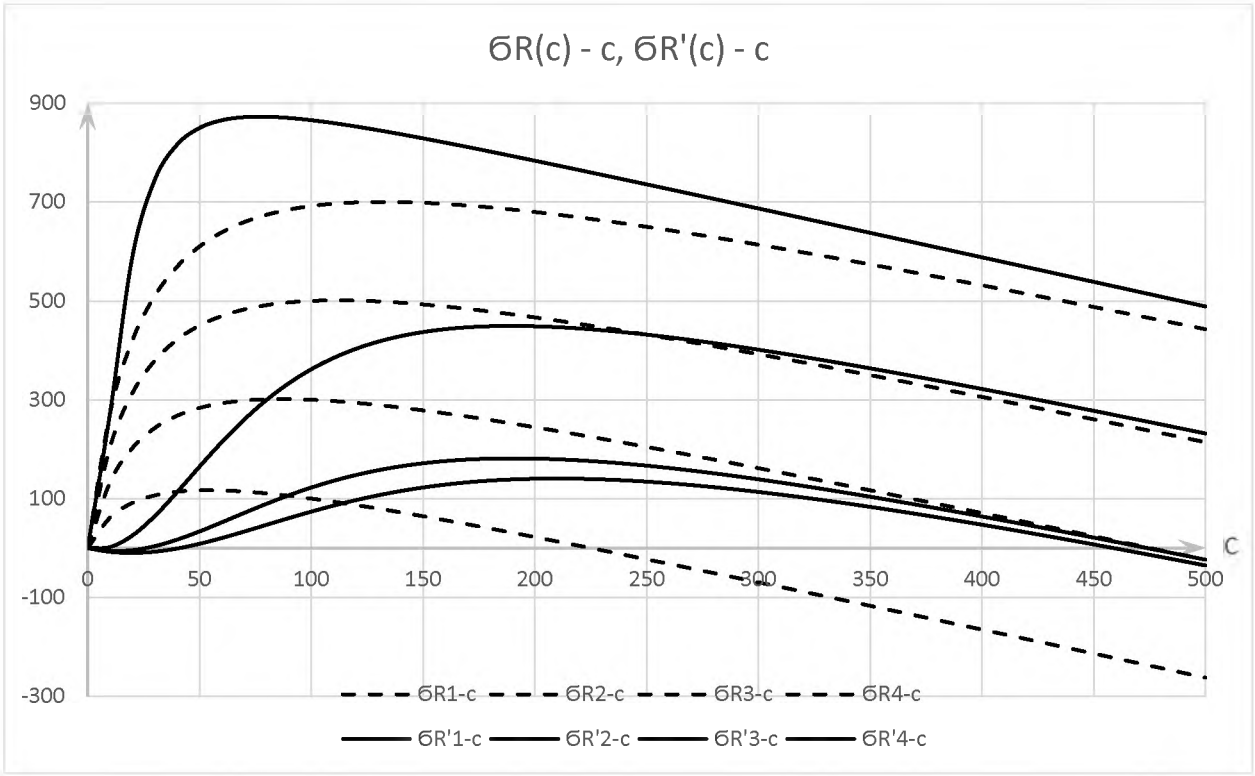

Рисунок 2.6 – Порівняльна характеристика простої і складної моделей на основі графіків вигоди він інвестицій в захист

Ще одна особливість, яку стає помітно з Рисунка 3, це те, що у випадку зі складною моделлю значно різкіше змінюється вигода при нарощенні інвестицій зловмисника в здійснення атаки, але подальші нарощення ресурсів чим далі, тим менше впливають на ризики сторони, яка обороняється.

Інша особливість, характерна для моделі, яка враховує інвестиції в атаку на етапі розрахунку імовірності вразливості, у тому, що для випадків з відносно високим рівнем D (маються на увазі рівні, при яких $D \geq g/2$ в межах даного

досліду) можна виділити три характерні зони діапазону зміни витрат на захист c, які повторюються у кожному з випадків. Насамперед рівень інвестицій в оборону, при якому значення вигоди від них залишається нульовим або навіть від'ємним, а значить таке значення витрат c не несе жодного покращення стану захищеності. Інший рівень характеризується поступовим наростанням величини вигоди він інвестувань в захист аж до досягнення максимального його значення, утримання його для певного проміжку зміни c і подальшого спадання. І третя зона, в якій відбувається різке спадання вигоди, яке згодом знову наближається до нуля і набуває від'ємних значень навіть при подальшому зростанні c, таким чином рівень захищеності продовжує підвищуватись, але подібні інвестування стають нерентабельними для власника. Протяжність кожної з цих зон прямо пропорційна розміру D, тобто з його зростанням збільшуються проміжки задовільних значень c, але разом із тим крива вигоди починає наближатись до нульових значень на всьому діапазоні. Таким чином все одно залишаються рівні інвестицій, вигідні для власника інформації, але вигода стає меншою. Характерним є також зміщення рівня оптимальних інвестицій у захист, в порівняння з простою моделлю.

Якщо для складної моделі побудувати залежність верхньої та нижньої межі ефективних значень c від зміни D, що можна побачити на рисунку 4, отримаємо сходження обох кривих в одній точці, яка відображає саме той рівень, який дозволяє отримати найвищий прибуток від витрат на захист. Також помітно те, що верхня межа значно швидше спадає, у порівнянні з наростанням нижньої.

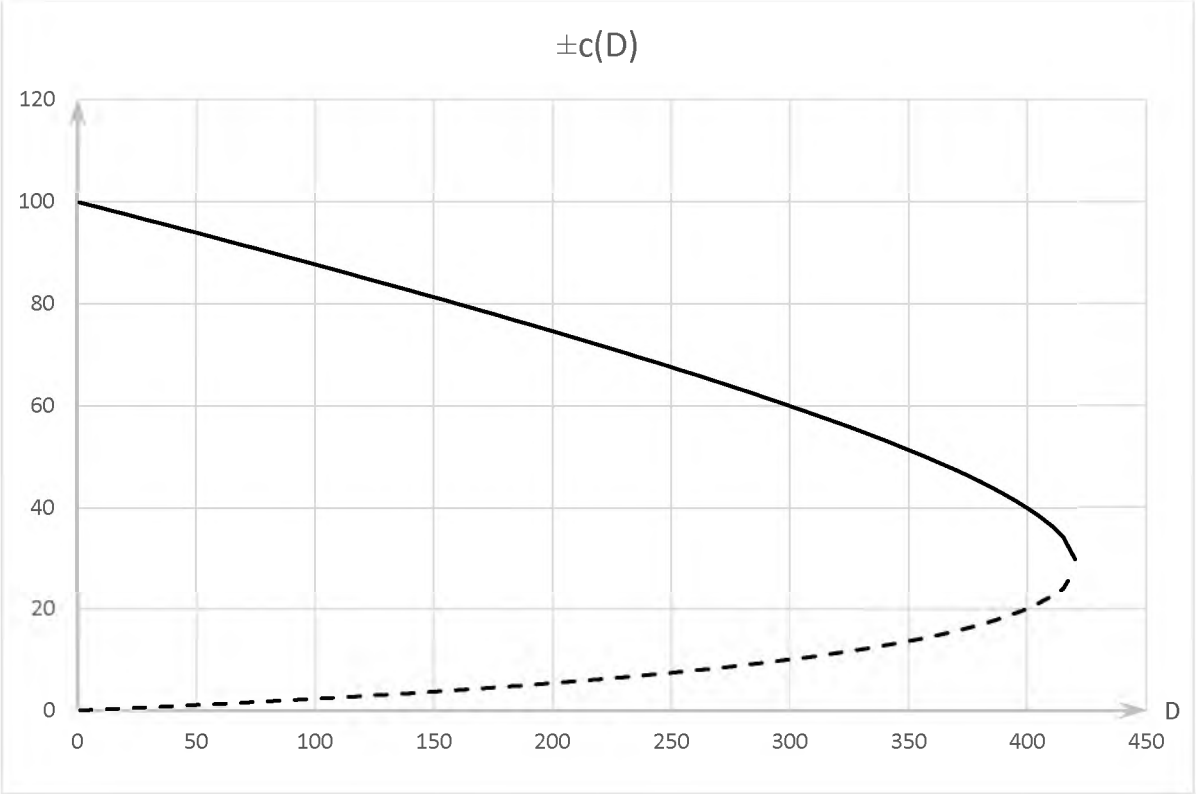

Рисунок 2.7 – Зміна верхньої та нижньої межі ефективних значень інвестицій у захист залежно від зміни витрат на атаку

Значення параметрів економіко-мотиваційної моделі оцінки ризиків, як і було використано для дослідів, що показано на рисунках 2.4, 2.5 і 2.6 показано в таблиці 2.1.

Таблиця 2.1 – Значення параметрів

Параметри	Досліди			
	1	2	3	4
q	1000	1000	1000	1000
g	1000	1000	1000	1000
s	40	40	40	40
D	10	250	500	750
c	[0,500]	[0,500]	[0,500]	[0,500]

2.4 Рівень зрілості організації як параметр моделі оцінки та аналізу ризиків

Одним із параметрів економіко-мотиваційної моделі оцінки та аналізу ризиків є величина, яка відображає так званий рівень зрілості організації. У світовій практиці прийнято для даної випадку приймати це значення в діапазоні 10..60, при чому для загальної більшості підприємств воно становить 50. Але метод визначення цього параметру для конкретної організації досі залишається не формалізованим.

В своїй монографії Петренко С.А. також приділяє значну увагу ставленню всередині компанії до захисту інформації. Згідно з його твердженням, основним фактором, від котрого залежить відношення організації до питань інформаційної безпеки, є степінь її зрілості. Так, наприклад, відома аналітична компанія GartnerGroupта університет CarnegieMellon запропонували свої моделі визначення зрілості компанії. Різним рівням зрілості відповідають різні потреби в області інформаційної безпеки. В наступних підрозділах розглянемо детальніше суть обох вище згаданих моделей.

2.5 Модель Gartner Group

GartnerGroup виділяє чотири рівня зрілості компанії – починаючи з нульового і закінчуючи третім.

Згідно даним GartnerGroup, компанії розподілились по рівням зрілості наступним чином: 30% компаній - 0-го рівня, 55% компаній – 1-го рівня, 10% – 2-го рівня і 5% – 3-го рівня. Також вони прогнозують подальшу тенденцію зміни процентного співвідношення компаній різних рівнів, а саме: 20% компаній – 0-го рівня, 35% – 1-го рівня, 30% – 2-го рівня, 5% – 3-го рівня зрілості.

Рівень зрілості 0

Необхідність забезпечення ІБ компанії належним чином не усвідомлена і формально така задача не ставиться. Виділеної служби інформаційної безпеки немає. Служба автоматизації використовує традиційні механізми і засоби захисту стеку протоколів TCP/IP і сервісів Intranet, а також операційного середовища і застосунків (ОС, СУБД, СППР, ERP, ERP II, CRM).

Рівень зрілості 1

Проблема забезпечення ІБ розглядається управлінням компанії як виключно технічна. Виділеної служби захисту немає. Організаційні міри підтримання ІБ не приймаються. Фінансування здійснюється в рамках єдиного бюджету на IT-технології. Служба автоматизації додатково до засобів захисту інформації рівня 0 може залучати засоби відмово стійкості, резервного копіювання інформації, джерела безперебійного живлення, а також між мережеві екрани, віртуальні приватні мережі (VPN), антивірусні засоби, засоби прозорого шифрування і e-Token.

Рівень зрілості 2

Проблема забезпечення ІБ компанії усвідомлена і розглядається як взаємно ув'язаний комплекс організаційних і технічних заходів. Впроваджені методики аналізу інформаційних ризиків, що відповідають мінімальному базовому рівню захищеності КІС. В компанії визначені склад і структура штатної служби ІБ. Прийнята корпоративна політика інформаційної безпеки. Фінансування ведеться в рамках окремого бюджету на створення і підтримку корпоративної системи захисту інформації. Служба ІБ додатково до засобів захисту інформації рівнів 0 і 1 залучає засоби захисту від НСД, системи виявлення втручання (IDS), інфраструктуру відкритих ключів (PKI), а також організаційні заходи, що відповідають політиці безпеки компанії (зовнішній і внутрішній аудит, розробка планів захисту і безперервного ведення бізнесу, дії в позаштатних ситуаціях та ін.)

Рівень зрілості 3

Проблема забезпечення ІБ компанії усвідомлена повною мірою. Поряд із бізнес-культурою існує поняття культури інформаційної безпеки компанії. Активно застосовуються методики повного кількісного аналізу інформаційних ризиків, а також відповідні інструментальні засоби. Впроваджена штатна посада – директор служби інформаційної безпеки (CISO). Визначені склад і структура групи внутрішнього аудиту безпеки КІС (CISA), групи попередження і розслідування комп'ютерних злочинів, групи економічної безпеки. Керівництвом компанії утверджені концепція і політика безпеки, план захисту та інші нормативно-методичні матеріали і посадові інструкції. Фінансування виділяється виключно в рамках окремого бюджету. Служба ІБ додатково до засобів захисту інформації рівнів 0-2 звертається до засобів централізованого управління ІБ компанії і засобів інтеграції з платформами управління мережевими ресурсами.

2.6 Модель Carnegie Mellon University

Більш розширену модель визначення рівня зрілості компанії з точки зору інформаційної безпеки запропонував університет CarnegieMellon. Відповідно до цієї моделі виділяється п'ять рівнів зрілості компанії, котрим можна поставити у відповідність різне розуміння проблем інформаційної безпеки організації.

Проблема забезпечення режиму інформаційної безпеки буде формулюватись (хоча б в неявному вигляді) і розв'язуватись по-різному для організацій, що знаходяться на різних рівнях розвитку.

1. Анархія

Співробітники самі визначають, що добре, а що погано. Затрати і якість не прогнозуються. Відсутні формалізовані плани. Відсутній контроль змін. Вище керівництво погано уявляє реальне положення справ.

Політика в області ІБ не формалізована, керівництво не займається цими питаннями. Забезпеченням інформаційної безпеки співробітники можуть займатись за власною ініціативою, у відповідності зі своїм розумінням задач.

2. Фольклор

Виявлена певна повторюваність організаційних процесів. Досвід організації представлений у вигляді переказів корпоративної міфології. Знання накопичуються у вигляді власного досвіду співробітників і зникають при їх звільненні.

На рівні керівництва існує певне розуміння задач забезпечення інформаційної безпеки. Існують процедури інформаційної безпеки, що склалися стихійно, їх повнота та ефективність не аналізуються. Процедури не документовані і повністю залежать від особистостей залучених в них співробітників. Керівництво не ставить задач формалізації процедур захисту інформації.

Комплекс заходів (організаційних і програмно-технічних) дозволяє захиститись від найбільш імовірних загроз, як потенційно можливих, так і тих, що відбулись раніше. Таким чином поступово складається неформальний список актуальних для організації класів ризиків, котрий поступово поповнюється.

3. Стандарти

Корпоративна міфологія записана на папері. Процеси повторювані і не залежать від особистих якостей виконавців. Інформація про процеси для вимірювання ефективності не збирається. Наявність формалізованого опису процесів не означає, що вони працюють. Організація починає адаптувати свій досвід до специфіки бізнесу. Проводиться аналіз знань та вмінь співробітників з ціллю визначення необхідного рівня компетентності. Виробляється стратегія розвитку компетентності.

Керівництво усвідомлює задачі в області інформаційної безпеки. В організації є документація (можливо, неповна), що відноситься до політики інформаційної безпеки. Керівництво зацікавлено у використанні стандартів в

області інформаційної безпеки, оформленні документації у відповідності з ними. Усвідомлюється задача управління режимом ІБ на всіх стадіях життєвого циклу інформаційної технології.

На цьому рівні в організації прийнято слідувати в тій чи іншій мірі стандартам і рекомендаціям, що забезпечують базовий рівень інформаційної безпеки (наприклад, ISO 17799). Питанням документування приділяється належна увага. Аналіз ризиків розглядається як один із елементів технології управління режимом інформаційної безпеки на всіх стадіях життєвого циклу. Поняття ризику включає декілька аспектів: імовірність, загрозу, вразливість, іноді вартість

4. Вимірюваний

На даному рівні процеси вимірювані і стандартизовані.

Також наявний повний комплект документів, що відносяться до забезпечення режиму інформаційної безпеки і оформлених у відповідності до якого-небуть стандарту. Діючі інструкції дотримуються, документи служать інструкцією до дій посадових осіб. Регулярно проводиться внутрішній (і, можливо, зовнішній) аудит в області ІБ. Керівництво приділяє належну увагу питанням інформаційної безпеки, насамперед має адекватне уявлення відносно існуючих рівнів загроз та вразливостей, потенційних втрат у випадку можливих інцидентів.

Актуальними є питання вимірювання параметрів, що характеризують режим інформаційної безпеки. Ризики як правило оцінюються за декількома критеріями (не лише вартісними). Застосовуються кількісні методи, що дозволяють оцінити параметри залишкових ризиків і ефективність різних варіантів контрзаходів при управлінні ризиками.

5. Оптимізований

Це рівень характерний фокусом на повторюваності, вимірюванні ефективності, оптимізації. Вся інформація про функціонування процесів фіксується.

Керівництво зацікавлене в кількісній оцінці існуючих ризиків, готове нести відповідальність за вибір певних рівнів залишкових ризиків, ставить оптимізаційні задачі побудови системи захисту інформації.

2.7 Рекомендації по самооцінці згідно стандрату ISO 9004

Самооцінка – це усестороннє оцінювання, підсумком якого є думка чи судження про результативність і ефективність організації і рівень зрілості системи менеджменту якості. Самооцінку зазвичай проводить керівництво організації. Ціль самооцінки полягає в представленні організації рекомендацій, що базуються на фактах, які стосуються областей застосування ресурсів для покращення її діяльності.

Самооцінка може бути корисною при вимірюванні досягнень в порівнянні з цілями, а також для повторної оцінки постійної відповідності цим цілям.

На сьогодні існує багато моделей самооцінки організацій по критеріям системи менеджменту якості. Найбільш широко визнані та використовуються моделі національних і регіональних премій по якості, що вважаються також моделями досконалості організації.

Метод самооцінки забезпечує простий і легкий в застосуванні спосіб встановлення рівня розвитку (зрілості) системи менеджменту якості організації в визначенні основних областей для покращення.

Конкретні особливості методу самооцінки по ISO 9004 такі, що він може:

- застосовуватись по всій системі менеджменту якості або її частині, чи до будь-якого процесу;
- застосовується до організації в цілому або до її частини;
- бути швидко здійснений внутрішніми засобами;
- бути здійснений багатопрофільною групою або одним робітником організації при підтримці вищого керівництва;

- сформулювати вхідні дані для більш усестороннього процесу самооцінки системи менеджменту;
- визначити і забезпечити розстановку пріоритетів можливостей для покращення;
- сприяти розвитку системи менеджменту якості в напрямку рівня світового класу.

Метод самооцінки, викладений в стандарті ISO 9004 призначений для оцінювання рівнів розвитку системи менеджменту якості по кожному основному розділу шляхом бальної шкали від 1 (відсутня формалізована система) до 5 (кращі показники в класі діяльності).

Висновки до розділу 2

У розділі було приведено структуру затрат на інформаційну безпеку у вигляді класифікації. Насамперед можна виділити такі основні групи, як затрати на обслуговування системи безпеки, на контроль, внутрішні та зовнішні витрати на ліквідацію наслідків порушення політики безпеки. Одні види витрат на безпеку є абсолютно необхідними, але інші можуть бути істотно зменшені чи навіть виключені у випадку дотримання політики безпеки.

Також було описано та проілюстровано як поводить себе економіко-мотиваційна модель у сценаріях з різними типами порушників. У випадку з низькими ресурсними можливостями нападника може сильно зростати кількість спроб реалізації вразливості, але разом із тим незначні інвестиції у захист приводять до повного запобігання реалізації атак подібного рівня. Натомість для другого сценарію, коли атакуючу сторону представляють досить досвідчені спеціалісти, для запобігання загрози ефективний рівень інвестицій може досягати 50% від вартості ресурсу, який захищають. І нарешті третій сценарій ілюструю ситуацію, при якій оборонитись від дій нападника майже неможливо, так як його ресурси необмежені. Тому доцільним при побудові СЗІ буде все ж звернути увагу

саме на другий сценарій, який разом із першим найчастіше зустрічаються в реальності.

І нарешті було досліджено поведінку моделі у випадках використання простої і складної формул обчислення імовірності вразливості, які у випадку зі складною формулою демонструють наявність характерних зон, при зміні параметру, що відображає рівень інвестицій в безпеку. Перша зона характеризуються нульовими або навіть від'ємними значеннями вигоди від інвестицій в оборону. Друга зона відображає наростанням цієї вигоди аж до досягнення максимального значення і утримання його для певного діапазону *c*. Третя зона характеризується різким спаданням вигоди, яке згодом знову наближається до нуля, чи навіть набуває від'ємних значень, так що хоч рівень захищеності продовжує зростати, але рішення стає нерентабельним для власника. Протяжність кожної з цих зон виявилась прямо пропорційною до розміру витрат зловмисника на атаку і очевидно, що з її зростанням також і зменшується вигода власника інформації від інвестиції в її оборону. Графіки значень ризику та вигоди від інвестицій в безпеку інформації було виконано в умовах різних рівнів витрат на атаку, що наглядно ілюструє вигляд вище згаданих зон для чотирьох випадків.

В розділі приводиться огляд двох моделей для оцінки зрілості організації, а саме GartnerGroupта CarnegieMellonUniversity. Кожна з них пропонує декілька рівнів, які відображають певні етапи розвидку підприємства. Недоліком подібних моделей є те, що їх складно застосувати для реальних організацій, так як немає чітко визначених метрик, які можна виміряти для отримання точного значення оцінки зрілості.

Додатково розглядається рекомедації по саооцінці, які приведені у стандарті ISO 9004, який пропонує трохи інший підхід, ніж у вище згаданих моделях.

3 ЕКОНОМІЧНІ АСПЕКТИ МОДЕЛЕЙ РИЗИКІВ

3.1 Поняття рефлексивних моделей ризику

Стандарт ISO / IEC 15408-1: 2009 вводить в якості характеристики атакуючої сторони поняття «потенціалу нападу», включаючи в нього три показника: компетентність, ресурси і мотивації порушника (зловмисника, атакуючого). Виходячи з цього набору показників і враховуючи, що кожен з них може мати різну ступінь інтенсивності, спробуємо відповісти на питання, чи можна виділити існування деяких характерних значень цих показників для найбільш часто зустрічаються типів порушників. Звернемося до спеціальної літератури, в якій питання безпеки інформації розглядаються з позицій атаки і взлому інформації.

Вільям Столлінгс [14]: «... насправді існує два типи хакерів. На вищому рівні знаходяться добре підготовлені фахівці, які прекрасно розбираються в технологіях, а на нижчому - «рядові солдати», просто використовують існуючі програми злому і мають досить туманне уявлення про те, як ці програми працюють. Ця робоча команда об'єднує два дуже грізних фактора: глибоке знання методів злому систем захисту і тупе бажання нескінченно довго «стукати в закриті двері», перевіряючи всі уразливості системи ».

Дана В. Столлінгсом досить загальна характеристика атакуючої сторони дозволяє затверджувати існування в ній двох груп, контрастних з точки зору рівня компетентності, методів дій і використовуваного при цьому інструментарію. Спробуємо уточнити і деталізувати їх характеристики, зібравши по кожній з груп додаткові відомості, що відображають різні аспекти поведінки і підготовки атакуючої сторони: вибір стратегії атаки, методи і способи реалізації інформаційних загроз, соціально-психологічний контекст дій атакуючої сторони,

існуючі (часто директивно визначаються) цільові установки цих дій. Розглядаючи зібрані за відповідними групами відомості як вербальні специфікації, використовуємо їх для побудови приватних моделей ризиків організації, яка піддається атакуючими діями кожної з цих груп. Сформовані таким чином приватні моделі ризиків, будемо називати рефлексивними (від лат. Reflexus - відображення, віддзеркалення) моделями ризиків, кожній з яких властиві певні особливості, що залежать від характеристик атакуючої групи, включених в її специфікацію.

Підбір відомостей, що вводяться в специфікації, проведемо, почавши його з уточнення характеристик групи «рядових солдатів» нижчого рівня

3.2 Типізація рефлексивних моделей

3.2.0 Узагальнена модель ризику

В [6], [7] для оцінки значень ймовірностей P_t, P_v були запропоновані, з урахуванням мотиваційно-економічних аспектів ситуації «атака / захист», Апроксиматичні моделі виду:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g}, \quad g \geq D, \tag{3.1}$$

$$P_v(q, c, D) = \frac{\mu q}{\mu q + s\frac{c^2}{D}}, \tag{3.2}$$

де g і q - оцінки цінності ресурсу I з точки зору його сприйняття атакуючої і захищаючої сторони, $\mu = g/q$ - коефіцієнт асиметрії сприйняття цінності ресурсу сторонами, D - витрати на підготовку і реалізацію атакуючих дій стороною А, c - інвестиції організації У в СЗІ, s - оцінка ступеня зрілості сторони, яка захищається в сфері інформаційної безпеки (коефіцієнт s визначає рівень

ефективності функціонування СЗІ, $s \le 85$ [6]-[8]: чим більше значення s, тим нижче, за умови одного і того ж обсягу c інвестицій, ймовірність P_v).

Підстановка виразів (3.1), (3.2) в формулу

$$R_T = P_T q = P_t P_v q, \tag{3.3}$$

дає можливість побудувати узагальнену математичну модель інтегрального ризику, в яку величина c входить як параметр:

$$R_T(c) = (1 - \frac{D}{g}) \frac{\mu q}{\mu q + s\frac{c^2}{D}} q. \tag{3.4}$$

Ця ж параметричну залежність від значень c збережеться і для величини сумарних втрат Δ_Σ ($\Delta_\Sigma = c + R_T = c + P_t P_v q$,). З урахуванням отриманого вище висновку про те, що найбільш ефективний рівень інвестицій, при якому забезпечується мінімум сумарних витрат, формалізуємо поняття ефективного обсягу інвестицій:

$$c_{eff} = \arg\min_{c \in C} \Delta_\Sigma(c), \tag{3.5}$$

де С – безліч рівнів допустимих (раціональних) інвестицій c, для яких значення $\Delta_\Sigma(c)$ збігаються або трохи вище мінімуму $\Delta_\Sigma(c_{eff})$. На жаль аналітичне рішення рівняння (3.5) після підстановки в нього формули ризику (3.4) в загальному випадку є неможливим.

Однак в деяких окремих випадках виявляється реальним отримання аналітичного рішення оптимізаційної задачі (3.5) і ряду доповнюючи це рішення відомостей. Для цього, в залежності від характеристик атакуючої сторони, формуються рефлексивні (від лат. Reflexus - відображення, віддзеркалення) моделі ризиків [8], що відображають специфічні аспекти поведінки і підготовки атакуючої сторони, соціально-психологічний фоновий контекст її дій, цільові установки цих дій, багато в чому впливають на вибір атакуючої стратегії, методи і

способи реалізації інформаційних загроз. Аналіз і дослідження отриманих моделей ризиків дозволяє для кожної відповідної типової ситуації «атака-захист» оцінити необхідний ефективний обсяг c_{eff} інвестицій в СЗІ.

3.2.1 Скрипт-кідді

В. В. Платонов [10]: «старі загрози реалізуються атаками, що базуються на використаних добре відомих вразливостей і скриптів атак (експлойтів). Такі загрози походять від недостатньо компетентних хакерів (названих script kiddies) або зовсім некомпетентних (званих newbies). Ці категорії порушників використовують готові скрипти атак і можуть абсолютно не розуміти діючих механізмів застосовуються (використовуваних) експлойтів, а також їх можливих побічних ефектів. Але це не зменшує їх небезпеку для організацій, так як реалізація старих незахищених загроз може завдати значної шкоди, якщо організація не приймає відповідних заходів ».

Відповідно до наведеної цитатою, при описі ризиків, що асоціюються з групою порушників нижчого рівня, для моделювання ймовірності P_v слід використовувати модель, в якій захищеність системи від злому визначається в першу чергу внутрішніми факторами, що визначають стійкість організації до інформаційних атак, зокрема, такими як рівень зрілості організації в сфері менеджменту безпеки інформації, обсяг c інвестицій в СЗІ, вартість q критичної інформації з точки зору її власника. Цим вимогам в повній мірі задовольняє формула (3.4) де характеристики атакуючої сторони враховуються лише значенням коефіцієнта μ, певною мірою відбиває цілеспрямованість і наполегливість атак.

У цьому плані інтерес представляє ще одне уточнення [11]: «скрипт-кідді ... зазвичай не хвилюють фінансові або політичні міркування, вони більше прагнуть прославитися або « викликати порушення сервісу і породити хаос із спортивного інтересу »». Іншими словами, загрози з боку скрипт-кідді не носять цільовий характер. Фінансовий інтерес не становить єдину і визначальну мотивацію їх дій, уявлення про ринкову вартість атакується ресурсу часто відсутні. Тому в моделі (3.3) слід виключити останню що залишилася можливість впливу атакуючої сторони на значення ймовірності P_v, поклавши $\mu = 1$.

Крім того, спонтанність і нецільовий характер вибору об'єкта атак заперечує можливість детермінованого завдання значень ймовірності P_t з використанням формули (3.2), можливо більш адекватним є опис P_t деякої випадкової величиною. Однак, з іншого боку, репліка Столлінгс: «тупе бажання нескінченно довго « стукати в закриті двері », перевіряючи всі уразливості системи» дозволяє хоча б в ряді випадків передбачається, що P_t=1

Якщо далі використовувати термін «скрипт-кідді» як збірний (що включає і newbies), то практично всі наведені вище відомості компактно узагальнюються Вікіпедією: скрипт-кідді (англ. Script kiddie - «дитина, який використовує скрипти» - людина, котра не розуміє принципів роботи використовуваних їм хакерських коштів для злому.) - в хакерській культурі назва тих, хто для атаки комп'ютерних систем і мереж користується скриптами або програмами чужої розробки, не розуміючи механізму їх дії. Передбачається, що скрипт-кідді занадто недосвідчені, щоб написати свій власний експлойт або програму для злому, і що їх метою часто є лише спроба справити враження на друзів або отримати похвалу від спільнот комп'ютерних ентузіастів.

Наведеним вище узагальненим відомостями про скрипт-кідді відповідає рефлексивна модель ризику виду:

$$R(c) = P_t \frac{q}{q + sc} q, \tag{3.6}$$

де ймовірність вдалого використання зловмисником для реалізації своїх атакуючих дій вразливостей ІС організації визначається формулою

$$P_v = \frac{q}{q + sc}. \tag{3.7}$$

З виразу (3.6) випливає, що в разі атаки скрипт-кідді ризики організації в першу чергу залежать від її внутрішніх рішень: суми інвестицій в СЗІ, рівня зрілості організації, оцінки вартості об'єкта, що захищається інформаційного ресурсу. Зростання значень параметрів і веде до зменшення ймовірності (3.7).

За оцінкою А. В. Лукацкого [12], скрипт-кідді складають до 95% від загального числа атакуючих інформаційні та комп'ютерні системи, тобто це найбільш поширений тип порушника, необхідність захисту від якого є першочерговим завданням, розв'язуваної при побудові СЗІ. В цілому вираз для моделі рефлексивного ризику (3.6) набагато простіше загальної моделі ризику (3.4) і допускає проведення досить детальних аналітичних досліджень. Додавши до рефлексивного ризику (3.6) значення інвестицій в СЗІ, отримаємо вираз сумарних втрат:

$$\Delta_\Sigma(c) = R(c) + c = P_t \frac{q}{q + sc} q + c. \tag{3.8}$$

Рішення оптимізаційної задачі (3.5), в якій вираз для $\Delta_\Sigma(c)$ задається формулою (3.8), дозволяє визначити ефективний обсяг інвестицій c_{eff}. окрема, досліджуючи на екстремум залежність $\Delta_\Sigma(c)$, як функцію змінної c, приходимо до рівняння:

$$\frac{d\Delta_\Sigma}{dc} = \frac{-s}{(q + sc)^2} P_t q^2 + 1 = 0, \tag{3.9}$$

з якого отримуємо квадратне рівняння і знаходимо його корені:

$$c^2 + 2\frac{q}{s}c + \frac{q^2}{s^2}(1 - P_t s) = 0, \tag{3.10}$$

$$c_{1,2} = -\frac{q}{s}(1 \pm \sqrt{P_t s}). \tag{3.11}$$

За своїм змістом витрати c не можуть бути негативними, тому $\sqrt{P_t s} > 1$ і ефективний обсяг інвестицій:

$$c_{eff} = \frac{q}{s}(\sqrt{P_t s} - 1) \tag{3.12}$$

Досліджуючи на екстремум залежність (3.12) як функцію змінної s, отримуємо:

$$\frac{dc_{eff}(s)}{ds} = q(s^{-2} - \frac{1}{2}s^{-3/2}\sqrt{P_t}) = 0, \tag{3.13}$$

звідки

$$\max[c_{eff}(s)] = c_{eff}(4/P_t) = 0{,}25qP_t. \tag{3.14}$$

Очевидно, що найбільшою величина ефективних інвестицій в СЗІ виявиться при P_t=1, тобто, максимальний обсяг ефективних інвестицій в СЗІ дорівнює $c_{eff\max} = 0{,}25q$, складаючи 25% від вартості об'єкта, що захищається ресурсу.

Однак при загальному високому рівні інформаційної культури огранізації, зокрема, при високій компетентності фахівців підрозділу захисту, що забезпечують високоефективні захисні рішення, (наприклад, для $s = 60$ і вище), відповідно до формули (3.12) навіть при P_t=1 обсяг інвестицій в СЗІ може виявитися на рівні 11-13% від значення q. Отриманий результат добре узгоджується з емпіричними оцінками обсягу інвестицій в СЗІ, наведеними в ряді публікацій [3], [13], автори яких акцентують увагу на рівні в 15-20% від вартості ресурсу I.

Завершуючи дослідження моделі ризику (3.6), спробуємо формалізувати поняття діапазон раціональних («розумних», допустимих) інвестицій.

Очевидно, що найбільше значення $R_1 = P_t q$ інтегральний ризик (3.7) приймає за умови $P_v = 1$, величину можливих втрат, які вдалося запобігти завдяки створенню в організації СЗІ:

$$\Delta_R = R_1 - R_T = P_t q - P_t P_v q, \tag{3.15}$$

З огляду на, що будь-які обсяги інвестицій в СЗІ не приведуть до нульового значення залишкового ризику $P_t P_v q$ (аксіома інформаційної безпеки), виникає питання: після досягнення якогось рівня інвестицій $c_{\max}$ їх подальше зростання слід вважати нераціональним? По-перше, очевидно обмеження $c_{\max} < q$. Однак більш жорсткою, але досить очевидною буде умова $\Delta_R(c) > c$. При цьому, якщо в рамках одного і того ж обсягу інвестицій можливі альтернативні варіанти СЗІ, вибір слід зробити на користь того, для якого більше різниця $\Delta_R(c) - c = \Delta_c(c)$ - свого роду «чистий прибуток», отримана завдяки діючій СЗІ.

Розрахувавши за рефлексивною моделлю ризику (3.6) величину запобіглих втрат $\Delta_R(c)$ і зіставивши її з обсягом c інвестицій в СЗІ, отримаємо аналітичний вираз для «чистого прибутку» $\Delta_c(c)$, обумовленої побудовою СЗІ:

$$\Delta_c(c) = \Delta_R(c) - c = \frac{sc}{q + sc} P_t q - c. \tag{3.16}$$

Аналіз виразу (3.16) дає оцінку [7], [8] діапазону «розумних» інвестицій: $0 \le c \le q(sP_t - 1)/s$, в межах якого $\Delta_R(c) \ge c$. Також як і розглянуті вище втрати $\Delta_\Sigma(c)$, «чистий прибуток» $\Delta_c(c)$ дозволяє реалізувати процедуру обчислення ефективного обсягу інвестицій шляхом розв'язання оптимізаційної задачі

$$c_{eff} = \arg\max_{c \in C} \Delta_c(c), \tag{3.17}$$

де С-діапазон раціональних інвестицій, («розумних» інвестицій), для яких $\Delta_R(c) > c$, приводячи в кінцевому підсумку до аналогічних з отриманими вище результатами [7], [8].

Підводячи підсумки розгляду цієї рефлексивної моделі ризику, введемо коротку вербальну специфікацію атакуючої сторони.

В цілому для скрипт-кідді характерний низький потенціал нападу, що дозволяє для захисту від їх атак застосовувати базовий рівень забезпечення безпеки до всіх систем інформаційних технологій, що реалізується шляхом вибору стандартних захисних заходів, орієнтованих на застосування засобів і способів захисту від уже відомих «старих» загроз (термін введений В. В. Платоновим, див. вище [10]).

Таким чином, якщо кваліфікація атакуючої сторони, її ресурсні можливості і характер мотивації не виходять за рамки специфікації скрипт-кідді, в якості моделі ризику слід прийняти модель (3.6). При цьому рівень інвестицій в СЗІ не повинен перевищувати 25% від вартості атакується ресурсу.

3.2.2 Професіонал

Уточнимо характеристики другої групи атакуючих, склад якої за В. Столлінгс це - добре підготовлені професіонали прекрасно розбираються в технології атак, з глибоким знанням методів злому систем захисту. Однак високий рівень компетентності фахівця сам по собі ще недостатній для підготовки і реалізації «нових» небезпечних і гранично небезпечних загроз. «Деякі методи здатні забезпечити захист від рядового користувача, але виявляються безсилі, якщо атаку виконує професіонал. А ті засоби захисту, які здатні зупинити професіонала, необов'язково є непереборною перешкодою для урядового агентства великої світової держави »[14]. «Тому, якщо коли-небудь розвідувальне управління зацікавиться вашою компанією, приготуйтеся до того, що проти вас будуть спрямовані величезні людські і технічні ресурси (досвідчені технарі, новітнє апаратне забезпечення і професіональні шпигуни)» [15]. Хоча наявність знань і компетентності є необхідною умовою формування «нової» атаки, її потенціал, гострота, успішність в значній мірі визначаються ще двома факторами:

1) завданням (стратегічної установкою) атакуючої сторони: комерційний успіх, економічні та соціально-політичні інтереси, оборона країни і т.п .;

2) рівнем ресурсних обмежень, зокрема, можливістю реалізації високозатратних атак, які потребують залучення додаткових кадрових, технічних, оперативних ресурсів.

У зв'язку з цим розширимо лінійку рефлексивних моделей ризиків, додавши в неї дві нові моделі.

1. Атакуюча сторона - професіонал або група професіоналів, що володіють необхідними знаннями, навичками і достатнім досвідом, для яких хакінг - основна діяльність, що носить очевидно комерційний характер, мета якої - фінансово-економічна ефективність. Зловмисник-професіонал користуватися певними технічними, фінансово-економічними ресурсами, проте для нього актуально обмеження $D \le g$.

Рефлексивна модель ризику для цього випадку має вигляд (вважаємо, що μ =1):

$$R(c) = (1 - \frac{D}{g}) \frac{q}{q + s\frac{c^2}{D}} q. \qquad (3.18)$$

Залежність $\Delta_R(c)$ для ризику (3.18) носить логістичний характер, а аналіз нерівності $\Delta_c(c) \ge 0$ дає можливість визначити межі діапазону «розумних» інвестицій [7], [8]:

$$\frac{qP_t}{2}(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}) \le \mathrm{c}, \qquad (3.19)$$

$$\frac{qP_t}{2}(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}) \ge c. \qquad (3.20)$$

На жаль, для ризику (3.18) рішення оптимізаційної задачі (3.19) не дозволяє отримати в явному вигляді вираз для c_{eff}.

Наявність процедури вилучення квадратного кореня в формулах (20), (21) передбачає очевидне умова $1 \ge 4D/sqP_t^2$, що трансформується в обмеження виду:

$$D \le 0{,}25sqP_t^2, \qquad (3.21)$$

доповнює характерне обмеження $D \le g$. Таким чином, зловмисник-професіонал може реалізовувати тільки щодо низьковитратні атаки. Дослідження співвідношень (3.19), (3.20) показує, що при $D \to 0{,}25sqP_t^2$ праві і ліві межі діапазону інвестицій зближуються, стягуючи для $D = 0{,}25sqP_t^2$ в точку $c = \frac{qP_t}{2}$. Цьому граничного випадку відповідає найбільша величина інвестицій в СЗІ $c_{eff\,\max} = 0{,}5q$.

Особливий інтерес представляє випадок асиметричного оцінювання сторонами атаки і захисту вартості ресурсу I, при якому $g >> q$, тобто $\mu >> 1$. У цій ситуації, якщо $D \le g$, то з точки зору боку атаки виділяється атакуючий потенціал не перевищує економічних меж доцільності. Тому атакуюча сторона А може виділити для організації та проведення атаки дуже значні ресурси, які можна порівняти за величиною зі значенням або навіть перевищують це значення. Виникає ситуація, яку можна назвати довготривалої цільової атакою [8]. Суть її полягає в тому, що атакуюча сторона А, попередньо вже вклала великі кошти в атаку, але ще не досягла успіху, переходить до вичікувальну тактику, супроводжуваної веденням постійного контролю функціонування СЗІ організації В. Рано чи пізно, при виникненні локального зниження рівня її захищеності (поява навіть короткочасної уразливості), атакуюча сторона А завершує свою успішну атаку. У цій фазі атаки основним витрачаються ресурсом зловмисника є його час плюс витрати на моніторинг стану захищеності об'єкта атаки.

Рефлексивна модель ризику для цього випадку повністю збігається з виразом (3.4). Для з'ясування особливостей ризиків довготривалої цільової атаки оцінимо в асимптоті при $g \to \infty$ граничні значення ймовірностей P_t, P_v (два перших множника у формулі (3.4)). З огляду на, що значення D обмежена, при $g \to \infty$ ймовірність активації загрози $P_t \to 1$, тобто загроза атаки існує постійно і вона реалізується як тільки випаде зручний момент. Приклади здійснення подібних атак - інциденти в практиці банківської безпеці, Зокрема, при наявності інсайдера в атакується організації саме він може повідомити про настання

потрібного моменту або спробує створити його, забезпечивши локальний сплеск ймовірності Ця ймовірність, що змінюється в часі відповідно до обраної тактикою атаки, згідно введеному в [7] визначення називається «термінальній» ймовірністю. Так як з ростом g коефіцієнт $\mu = g/q$ зростає, а з ростом D доданок sc^2/D зменшується, то в асимптоті $g \to \infty$ ймовірність $P_v \to 1$.

Хоча отримані вище граничні значення ймовірностей P_t, $P_v \to 1$, вони є лише деякими оціночними асимптотичними величинами, реальна ж ситуація далеко не настільки фатальна по відношенню до команди, що захищається стороні.

У цьому сценарії правильна стратегія, яка захищається - так званий проактивний захист. Вона базується на попереджувальних захисних діях, що спираються на вивчення поведінки, тактики і стратегії атакуючої сторони, тобто використовує підходи та принципи рефлексивного управління [8], що дозволяє відстрочити настання моменту реалізації довгострокової цільової атаки теоретично на необмежено довгий термін [8]. Рефлексивність дій захисту забезпечується усвідомленням нею можливості асиметричного сприйняття атакуючої стороною цінності ресурсу I. В іншому випадку, якщо захищається,, створюючи СЗІ, ґрунтується на принципі розумної достатності, виходячи виключно зі своїх «внутрішніх» уявлень про цінності q захищеного ресурсу I, успішна реалізація загрози атакуючої стороною при $\mu >> 1$ виявляється практично гарантованою.

2. Можливі обставини, при яких принцип економічної доцільності для атакуючої сторони виявляється несуттєвим.

Типовим прикладом подібної ситуації є виконання особливо важливого завдання співробітниками спецслужби - професіоналами, підготовленими до здійснення дій в кіберпросторі [7], [8]. У цьому випадку завдання атакуючої сторони А - реалізація певної загрози щодо ресурсу I, - повинна бути виконана за будь-яких обставин, практично з $P_t = 1$, що відрізняє дану ситуацію від попередньої, в якій атакуюча сторона в своїх діях виходила тільки з принципу економічної доцільності. У зв'язку з надзвичайною важливістю поставленого

завдання, ресурсні обмеження для її вирішення знімаються. Крім того, виконавець може розраховувати на залучення для підтримки своїх дій різних додаткових ресурсів: фінансових, аналітичних, технічних, оперативних і т.п., що забезпечує реалізацію надзвичайно високозатратних атак ($D \to \infty$).

Рефлексивна модель ризику для цього випадку проста:

$$R(c) = P_v q = \frac{q}{q + s\frac{c^2}{D}} q . \qquad (3.22)$$

З неї очевидно, що зі зняттям ресурсних обмежень ($D \to \infty$) ймовірність $P_v \to 1$, тобто в цій ситуації, якщо захищаюча сторона, створюючи свою СЗІ, спирається на принцип розумної достатності, виходячи виключно з власного («внутрішнього») розуміння цінності q захищаючого ресурсу *I*, успішна реалізація загрози атакуючої стороною виявляється практично гарантованої, в результаті $R(c) \to q$. Це досягається за рахунок проведення нових оригінальних атак, захист від яких в рамках діючих посібників щодо ризик-менеджменту, що грунтуються на аналізі і дослідженнях що мали місце в раніших інцидентів в сфері безпеки, здійснити практично неможливо. Таким чином, КСЗІ, побудована тільки відповідно до вимог діючих нормативних документів системи НД ТЗІ, не забезпечує достатніх гарантій захисту від атак, що реалізуються сьогодні в кіберпросторі, зокрема, спрямованих цільових атак APT (Advanced Persistent Threat), динамічних технік обходу AETs (Advanced Evasion Techniques), проти яких застосовуються комплекси традиційних захисних заходів молоеффективні. Перспективною в цьому випадку може виявитися розробка проактивних систем захисту, які використовують підходи і принципи рефлексивного управління [8].

3.2.3 Хактивіст

Атакуюча сторона - ідейний хакер («кібер-активіст»), який добивається своїми діями в кіберпросторі просування деяких політичних або соціальний ідей (нерідко досить сумнівного характеру), організує акції громадянської

«електронного» непокори в кіберпросторі, який намагається привернути увагу влади і громадськості (іноді в досить жорсткій формі) до тих чи інших питань і проблем сучасного суспільства шляхом синтезу соціальної активності і хакерства. Найбільш характерними для хактивістів акціями є віртуальні «сидячі страйки» і блокади, бомбардування електронної пошти, WEB-хакінг і комп'ютерні зломи, комп'ютерні віруси і черв'яки [11]. В діях хактивіста практично відсутня комерційна складова, його атакуючий потенціал, зокрема, ресурсне забезпечення, зазвичай обмежені, тому специфікація хактивістом, в залежності від доступних для нього ресурсів, може бути близька до специфікації Професіонала (версії 1., 2. Встановивши приналежність хактивістів до того чи іншого протестної спільноти, оцінивши груповий або одиночний характер акції, її тип, інтенсивність, масовість, тривалість і можливі наслідки, можна припустити загальну вартість захисних заходів, ефективних в подібних ситуаціях.

Висновки до розділу 3

Застосування ризик-орієнтованого підходу дозволяє сформулювати в загальній постановці завдання оптимізації обсягу інвестицій для створення СЗІ організації і в ряді випадків отримати в аналітичній формі раціональну оцінку необхідного обсягу інвестицій. При цьому виділяється ряд типових ситуацій «атака-захист», що відрізняються характерними особливості поведінки і дій атакуючої сторони. Наведені описи (вербальні специфікації) кількох подібних ситуацій, умовно названих Скрипт-кідді, Професіонал, хактівістом, і відповідні їм (рефлексивні) моделі ризиків, для яких оцінені ефективні обсяги інвестицій і кордони так званих «розумних» інвестицій. Показано, що найбільші ефективні обсяги інвестицій в захист від реалізації низьковитратних атак не перевищують в специфікаціях: Скрипт-кідді - 25% вартості об'єкта, що захищається інформаційного ресурсу, Професіонал 1 - 50%. Застосування традиційних типових

систем захисту від високозатратних атак в специфікації Професіонал 2 неефективне.

ВИСНОВКИ

В даній роботі було розглянуто моделі оцінки оптимального об'єму інвестицій в інформаційну безпеку. Як підсумок доведено об'єктивність використання для визначення ефективного рівня інвестицій в інформаційну безпеку саме результатів економіко-мотиваційної моделі аналізу ризиків.

Було досліджено поведінку моделі у випадках використання простої і складної формул обчислення імовірності вразливості, які у випадку зі складною формулою демонструють наявність характерних зон, при зміні параметру, що відображає рівень інвестицій в безпеку.

Використовуючи письмовий опис типів порушників було створено рефлексивні моделі. Застосування ризик-орієнтованого підходу дозволяє сформулювати в загальній постановці завдання оптимізації обсягу інвестицій для створення СЗІ організації і в ряді випадків отримати в аналітичній формі раціональну оцінку необхідного обсягу інвестицій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. *Gordon L.A.* The Economics of Information Security Investment / *Gordon L.A., Loeb M.P.* // ACM Transactions on Information and System Security. Vol. 5. No. 4. November 2002. P. 438–457.

2. *Gordon L.A.* Externalities and Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model / Gordon L.A., Loeb M.P., W. Lucyshyn, L. Zhou // Journal of information Security – 2015.– No.6. – P. 24-30.

3. *Willemson J.*On Gordon & Loeb Model for Information Security Investment [Електронний ресурс] / Jan Willemson // The Fifth Workshop on the Economics of Information Security (WEIS 2006). – 2006. – Режим доступу до ресурсу: http://www.econinfosec.org/archive/weis2006/docs/12.pdf.

4. *Willemson J.* Extending the Gordon&Loeb Model for Information Security Investment. [Электронный ресурс]] / Jan Willemson. – 2010. – Режим доступу до ресурсу: http://cyber.ee/uploads/2013/05/Villemson_GordonLoeb_Model.pdf.

5. *Андрощук Г.А*Экономическая безопасность предприятия: защита коммерческой тайны. Монография. / Андрощук Г.А., Крайнев П.П., – К.: Издательский Дом «Ин Юре», 2000. – 400 с.

6. *Петренко С.А.* Управлене информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В.– М. : Компания АйТи : ДМК Пресс, 2004. – 384 с. : ил. – (Информационные технологии для инженеров).

7. *Архипов А.Е.* Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков / Архипов А.Е. // Захист інформації – 2011. – №2 (51) – С. 69-76.

8. *Архипов А.Е.* Применение мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «атака-защита». /Архипов А.Е., Архипова С.А.//Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ-2008р, випуск 1(16).–С. 57-61.

9. *Архипов А.Е.* Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков / Архипов А.Е. // Захист інформації – 2011. – №2 (51) – С. 69-76.

10. ISO 9004:2009 – Managing for the sustained success of an organization. A quality management approach.

11. В.В. Платонов. *Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей*. – М.: «Академия», 2006. – 240 с

12. Д. В. Скляров. *Искусство защиты и взлома информации.* – СПб.: БХВ-Петербург, 2004. – 288 с

13. Д. Макнамара. *Секреты компьютерного шпионажа: Тактика и контрмеры*. М.: БИНОМ. Лаборатория знаний. - 2004. – 536с.

14. В. Столлингс. *Основы защиты сетей. Приложения и стандарты*. - М.: Издательский дом «Вильямс», 2002. – 432 с.

15. Качинський А.Б. Безпека, загрози та ризик / А. Б. Качинський. – К. : ІПНБ РНБО ; НА СБ України, 2004. – 472 с.