

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»

В.о. завідувача кафедри

_____ М.В.Грайворонський

“ ____ ” _____ 2019 р.

Магістерська дисертація
на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Адаптивний підхід до управління інформаційною безпекою _____

Виконав (-ла): студент (-ка) _2_ курсу, групи _ФБ-81мп_____
(шифр групи)

_____ Теплицька Тетяна Павлівна _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник __доктор технічних наук, професор Архипов О.Є.__
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

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

Засвідчую, що у цій магістерській дисертації
немає запозичень з праць інших авторів без
відповідних посилань.

Студент _____
(підпис)

Київ – 2019 року

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

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (освітньо-професійна програма) – 125 Кібербезпека («Системи, технології та математичні методи кібербезпеки»)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«__»_____2019 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Теплицька Тетяна Павлівна
(прізвище, ім'я, по батькові)

1. Тема дисертації Адаптивний підхід до управління інформаційною безпекою

науковий керівник дисертації доктор технічних наук, професор Архипов О.Є
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «15» листопада 2019 р. № 3927-с

2. Термін подання студентом дисертації 10.12.2019 р.

3. Об'єкт дослідження Можливі підходи до управління інформаційною безпекою

4. Вихідні дані Результати аналізу стандартів інформаційної безпеки

5. Перелік завдань, які потрібно розробити:

1. Провести аналіз існуючих підходів до управління інформаційною безпекою.
2. Сформулювати основні аспекти адаптивного підходу до управління інформаційною безпекою.
3. Дослідити існуючі підходи до застосування адаптації в інформаційній безпеці.

4. Запропонувати спосіб обчислення прийнятного (ефективного) обсягу інвестицій у систему захисту інформації.

6. Орієнтовний перелік ілюстративного матеріалу _____

7. Орієнтовний перелік публікацій Результати роботи представлені у статті «Адаптивний підхід до управління інформаційною безпекою» та прийнято до друку у науковому журналі «Молодий вчений», №11 (75) листопад, 2019 року.

8. Дата видачі завдання _____

Календарний план

| № з/п | Назва етапів виконання магістерської дисертації | Термін виконання етапів магістерської дисертації | Примітка |
|-------|---|--|----------|
| 1 | Аналіз існуючих підходів до управління інформаційною безпекою | 30.01.2019 | |
| 2 | Дослідження особливостей адаптивного підходу в теорії управління | 02.03.2019 | |
| 3 | Дослідження практик застосування адаптації в інформаційній безпеці | 11.05.2019 | |
| 4 | Аналіз моделей потенційних зловмисників та побудова рівнів адаптації | 20.09.2019 | |
| 5 | Формулювання та застосування методів для визначення прийнятного рівня інвестицій в систему захисту інформації | 30.10.2019 | |
| 6 | Аналіз отриманих результатів, формулювання висновків | 15.11.2019 | |
| 7 | Підготовка статті для журналу | 30.11.2019 | |
| 8 | Оформлення та подання роботи | 10.12.2019 | |

Студент

(підпис)

(ініціали, прізвище)

Науковий керівник дисертації

(підпис)

(ініціали, прізвище)

РЕФЕРАТ

Обсяг роботи 90 сторінок, 29 таблиць, 3 рисунки та 18 джерел за переліком посилань.

Актуальність роботи обумовлюється необхідністю створення нових підходів та методів управління інформаційною безпекою для побудови надійних систем захисту інформації.

Мета роботи полягає у формулюванні основних положень адаптивного підходу до управління інформаційною безпекою та визначенні прийнятного (ефективного) рівня інвестицій в побудову СЗІ.

Об'єктом дослідження є можливі підходи до управління інформаційною безпекою.

Предметом дослідження є адаптивний підхід до управління інформаційною безпекою.

Наукова новизна одержаних результатів обумовлюється запропонованим способом обчислення прийнятного (ефективного) обсягу інвестицій у систему захисту інформації, структура і функції якої формуються виходячи із принципу адаптивного управління ІБ організації.

Практичне значення одержаних результатів полягає в можливості застосування запропонованого способу для обчислення ефективного обсягу інвестицій у систему захисту інформації організацій.

Ключові слова: адаптивний підхід, управління інформаційною безпекою, обсяг інвестицій, атака, захист.

ABSTRACT

This work contains 90 pages, 29 tables, 3 figures and 18 references are cited.

Urgency of the work is due to the need to create new approaches and methods of information security management to build reliable information security systems.

The goal of the work is to formulate the main aspects of an adaptive approach to information security management and to determine the acceptable (effective) level of investment in building a KIC.

The object of the research is an adaptive approach to information security management.

The subject of the research is ways to apply an adaptive approach to information security management.

The scientific novelty of the obtained results is determined by the proposed method of calculating the acceptable (effective) volume of investments in the information security system, the structure and functions of which are formed on the basis of the principle of adaptive management of the organization's IB.

The practical significance of the results obtained is the ability to apply the proposed method to calculate the effective amount of investment in an organization's information security system.

Keywords: adaptive approach, information security management, investment volume, attack, defense.

ЗМІСТ

| | |
|---|----|
| Перелік умовних позначень, символів, одиниць, скорочень і термінів | 8 |
| Вступ..... | 9 |
| 1 Підходи до управління інформаційною безпекою | 11 |
| 1.1 Стандарти інформаційної безпеки | 11 |
| 1.2 Ризик-орієнтований підхід до управління інформаційною безпекою | 15 |
| 1.3 Методики ризик-орієнтованого підходу | 21 |
| Висновки до розділу 1 | 30 |
| 2 Адаптивний підхід до управління інформаційною безпекою | 32 |
| 2.1 Проактивний захист | 32 |
| 2.2 Адаптивний підхід в теорії управління | 38 |
| 2.3 Адаптивна безпека..... | 42 |
| 2.4 Практики застосування адаптивного підходу в інформаційній безпеці. | 47 |
| Висновки до розділу 2 | 50 |
| 3 Методи визначення прийнятного рівня інвестицій в систему захисту інформації..... | 51 |
| 3.1 Економіко-вартісні моделі атакуючого..... | 51 |
| 3.2 Рівні адаптації | 60 |
| 3.3 Особливості визначення рівня інвестицій в систему захисту інформації.... | 64 |
| Висновки до розділу 3 | 70 |
| 4 Стартап-проект | 72 |
| 4.1 Ідея проекту..... | 72 |
| 4.2 Потенційні техніко-економічні переваги | 74 |
| 4.3 Ринкові можливості запуску стартап-проекту | 74 |
| 4.4 Фактори конкурентоспроможності..... | 78 |
| 4.5 Сильні та слабкі сторони стартапу | 78 |
| 4.6 Альтернативи ринкової поведінки..... | 79 |
| 4.7 Визначення стратегії охоплення ринку | 80 |
| 4.8 Стратегія конкурентної поведінки..... | 82 |
| 4.9 Стратегія позиціонування | 82 |

| | | |
|------|--|----|
| 4.10 | Маркетингова концепція товару | 83 |
| 4.11 | Маркетингова модель товару | 83 |
| 4.12 | Цінові межі | 84 |
| 4.13 | Оптимальна система збуту | 84 |
| 4.14 | Концепція маркетингових комунікацій..... | 85 |
| | Висновки до розділу 4 | 85 |
| | Висновки | 86 |
| | Перелік джерел, посилань | 88 |

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ,
СКОРОЧЕНЬ І ТЕРМІНІВ**

ІБ – інформаційна безпека.

ПЗ – програмне забезпечення.

РОП – ризик-орієнтований підхід.

СЗІ – ситема захисту інформації.

УІБ – управління інформаційною безпекою.

ВСТУП

Триваюче зростання успішних кібератак на інформаційні системи та ресурси підприємств і установ з одного боку є наслідком росту агресивності кіберзлочинців, що обумовлює пряме збільшення загальної кількості атак, а з іншого – свідомим якісним підсиленням потенціалу цих атак, зокрема покращенням програмно-технічного забезпечення атакуючої сторони, організаційного супроводу атаки, рівня її інтелектуальної підтримки. За цих умов сторона захисту мусить розробляти і впроваджувати політики інформаційної безпеки, за своїм змістом та рівнем адекватні атакуючим діям.

Актуальність роботи обумовлюється необхідністю створення нових підходів та методів управління інформаційною безпекою для побудови надійних систем захисту інформації.

Мета роботи полягає у формулюванні основних положень адаптивного підходу до управління інформаційною безпекою та визначенні прийнятного (ефективного) рівня інвестицій в побудову СЗІ.

Завдання роботи:

- Провести аналіз існуючих підходів до управління інформаційною безпекою.
- Сформулювати основні аспекти адаптивного підходу до управління інформаційною безпекою.
- Дослідити існуючі підходи до застосування адаптації в інформаційній безпеці.
- Запропонувати спосіб обчислення прийнятного (ефективного) обсягу інвестицій у систему захисту інформації.

Об'єктом дослідження є можливі підходи до управління інформаційною безпекою.

Предметом дослідження є адаптивний підхід до управління інформаційною безпекою.

Наукова новизна одержаних результатів обумовлюється запропонованим способом обчислення прийнятної (ефективної) обсягу інвестицій у систему захисту інформації, структура і функції якої формуються виходячи із принципу адаптивного управління ІБ організації.

Практичне значення одержаних результатів полягає в можливості застосування запропонованого способу для обчислення ефективного обсягу інвестицій у систему захисту інформації організації.

Апробація: Результати роботи представлені у статті «Адаптивний підхід до управління інформаційною безпекою» та прийнято до друку у науковому журналі «Молодий вчений», №11 (75) листопад, 2019 року.

1 ПІДХОДИ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Стандарти інформаційної безпеки

Аналізуючи розвиток стандартів у області інформаційної безпеки, можна розділити існуючі документи на дві групи [1]. Першу започатковано від найстарішого стандарту в галузі інформаційної безпеки - «Помаранчевої книги». Сюди також належать розроблені пізніше «Федеральні критерії», «Канадські критерії», а сучасним представником даної гілки виступають «Загальні критерії оцінки безпеки інформаційних технологій» - ISO/IEC 15408 (Рисунок 1.1).

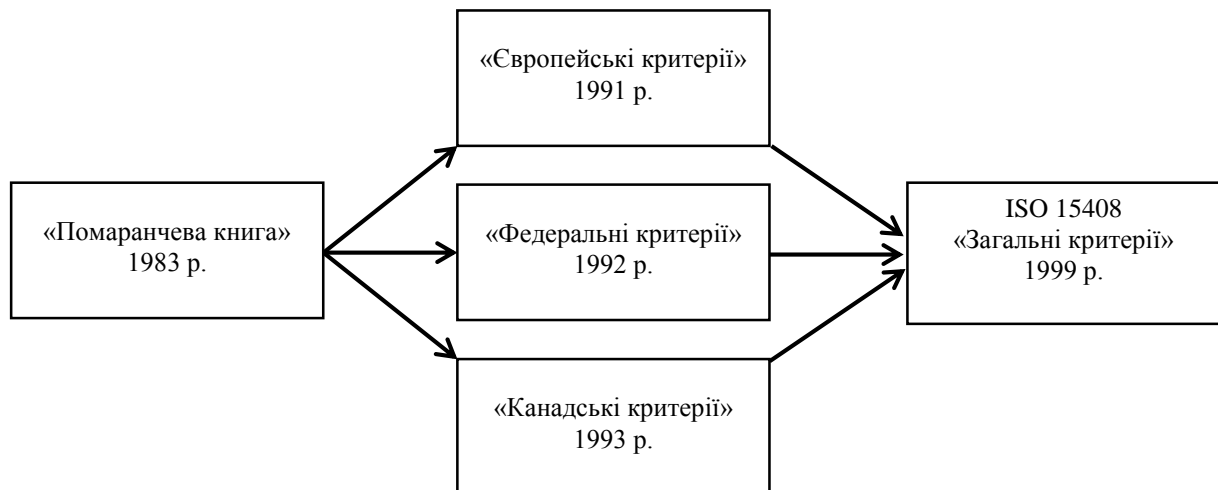


Рисунок 1.1 – Еволюція оціночних стандартів

В даному стандарті велика увага приділяється так званій адекватності реалізації функціональних вимог. Вважається, що забезпечити її можна шляхом впровадження незалежних актів тестуванням і аналізу продукту, а також використанням усіх необхідних технологій на кожному з етапів проектування та розробки. Крім того, в «Загальних критеріях» гарантованість реалізації захисту описано як найвагоміший компонент інформаційної безпеки. Тому передбачається багатоетапний контроль на кожному кроці реалізації проекту, що

дає можливість затвердити відповідність фактичних результатів поставленим спочатку цілям.

В даному стандарті втілено багаторічний досвід усіх його попередників, у порівнянні з якими він має більш високий рівень значущості та безліч переваг. Однак, у зв'язку з наявністю у пропонованому в «Загальних критеріях» підході деяки недоліків, розвиток цієї групи стандартів, виявляється не доцільним. Одним із зазначених недоліків є дуже високий рівень деталізації процесів описаних у стандарті. Проходження процедури сертифікації за даним стандартом може виявитися занадто довготривалим та коштовним процесом. Такі обмеження звужують коло установ, згодних здійснити таку сертифікацію, в основному, до структур, що мають на меті збереження інформації рівня державної таємниці. Окрім того, «Загальні критерії», як і їх попередники, не відповідають на питання оптимального рівня інвестицій потрібного для побудови надійної системи захисту.

Ключовою ідеєю стандартів цієї гілки є так званий захист «із повним перекриттям», орієнтація здійснюється на статичні, замкнуті системи, що у загальному випадку характерні для військової сфери та дуже рідко – для комерційної.

До другої ж групи можна віднести документи, що за основу взяли стандарти серії BS 7799 (British Standards) і за своїм змістом інтегруються із стандартами якості менеджменту серії ISO 900X. Саме з даної групи стандартів беруть початок основні принципи управління інформаційною безпекою.

BS 7799 Part-1 вважався «головним стандартом інформаційної безпеки». Проте, на засіданні в 2000 р. в ISO першої редакції міжнародного стандарту ISO 17799 учасника процесу не легко було досягти консенсусу. Стандарт викликав значну кількість зауважень критичного характеру з боку представників провідних держав. Останні були впевнені в тому, що він не відповідає найважливішим критеріям, які необхідні для міжнародних стандартів [2]. Відразу кілька представників, включаючи делегатів із США, Канади, Франції і Німеччини, віддали голос проти прийняття ISO 17799. Їх точка зору полягала в

тому, що розглянутий документ більш схожий на набір рекомендацій, але не на стандарт. Справа в тому, що в ті роки в світі склалася досить неоднозначна та суперечлива ситуація у сфері стандартизації з ІБ. Сертифікації за існуючими на той час стандартами на практиці постійно викликали питання та певні сумніви. У США і європейських країнах до 2000 р. вже була проведена значна робота у галузі стандартизації інформаційної безпеки. Представник США в технічному комітеті ISO, Жене Трой, коментував цю ситуацію наступним чином: «Існує кілька різних підходів до ІТ безпеки. Ми вважали, щоб отримати дійсно прийнятний міжнародний стандарт, всі вони повинні бути прийняті до розгляду, замість того щоб взяти один з документів і прискорено його узгодити. Головний стандарт безпеки був представлений де-факто, і просто не було можливості використовувати результати інших робіт в цій області». До того ж, на відміну від інших стандартів у сфері інформаційної безпеки, таких як Commonly Accepted Security Practices and Regulations (CASPR) або ISO 15408 / Common Criteria, ISO 17799 регламентував основні не технічні положення захисту інформації. В той час як у більшості спеціалістів в даній сфері превалював технічний підхід до забезпечення захищеності, а поняттям організації управління безпекою майже не приділялась увага. Однак представник BSI Стів Тайлер робив акцент саме на тому, що ISO 17799 «повинен бути таким, оскільки призначається для будь-яких видів організацій». Тобто, в даному стандарті проявлялися положення універсального характеру. Незважаючи на всі заперечення, авторитет BSI (організація-засновник ISO, розробник міжнародних стандартів, вищий орган у сфері сертифікації у світі) переважив. Було розпочато процес прискореного узгодження, після чого стандарт був прийнятий.

Отже, найважливішими перевагами ISO 17799 є його гнучкість і універсальність. Описаний в даному документі перелік кращих практик можна використовувати практично для будь-якої організації. Такий підхід завжди залишає можливість варіації використовуваних технологій. Саме цей документ дає відповідь на питання: «З чого почати?», «Як управляти ІБ?», «На відповідність яким критеріями слід проводити аудит?». Однак такі

характеристики як гнучкість та універсальність одночасно є і основними недоліками регламентованого підходу. Основна ідея критиків даного документу полягає у тому, що він занадто абстрактний, щоб представляти вагому позицію серед наявних стандартів. Недостатньо грамотний підхід до його використання може давати помилкове відчуття захищеності[2].

Сучасними представниками документів цієї групи є серія стандартів ISO/IEC 2700X (Рисунок 1.2). Згідно із широко відомим міжнародним стандартом ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги» поняття управління інформаційною безпекою розглядається як управління процесом забезпечення інформаційної безпеки [2].

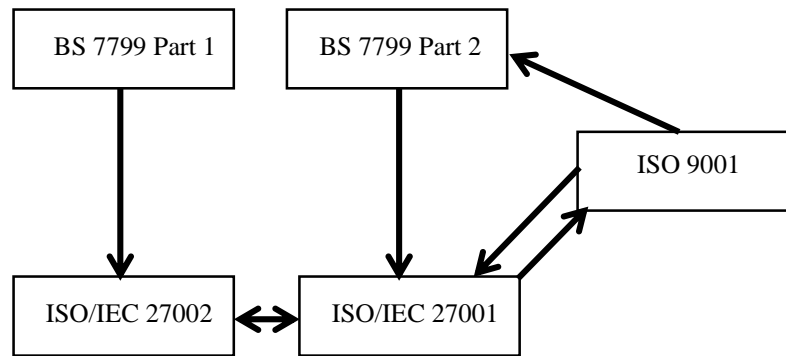


Рисунок 1.2 – Взаємозв’язок стандартів управління ІБ та управління якістю

Система управління інформаційною безпекою – частина загальної системи управління, заснованої на підході до бізнес-ризиків, яка встановлює, впроваджує, функціонує, контролює, оглядає, підтримує та покращує інформаційну безпеку.

Важливою відмінністю даних стандартів від першої групи є регламентування ризик-орієнтованого підходу до управління інформаційною безпекою (УІБ). Проте застосування даного підходу на практиці викликає певну кількість запитань. Зокрема для великих організацій із складною ієрархічною структурою розрахунок їх інтегральних ризиків являє трудомістку довготривалу процедуру, результати якої виявляються приблизними та неоднозначними. Крім того, вельми суб’єктивним є формування переліку адекватних загроз:

перестраховка, намагання не пропустити істотної загрози призводить до невинновданого розширення складу переліку загроз, що у свою чергу тягне за собою надлишкові інвестиції у створення системи захисту інформації (СЗІ).

Це питання є дуже болісним і важливим для комерційних організацій, виникає потреба у перегляді використовуваних підходів до формування базових принципів побудови СЗІ та політик УІБ в цілому, підсиленні в них ваги економічної складової, формування цих політик залежно від потенціалу та спроможності атакуючої сторони, адаптуючись до особливостей її поведінки, ймовірних намірів та можливостей.

1.2 Ризик-орієнтований підхід до управління інформаційною безпекою

Різні організації потребують забезпечення різного рівня інформаційної безпеки і, таким чином, приймають різні стратегії виявлення та виконання цілей контролю безпеки.

Деякі організації, такі як банки та інші фінансові установи, зосереджують свої зусилля з безпеки на виконанні зобов'язань щодо дотримання вимог, а інші починають прикладати зусилля до забезпечення безпеки внаслідок виявлення певних порушень або після зацікавлення в цьому вищого керівництва.

Такі підходи до кібербезпеки зазвичай мають досить короткотривалий ефект, якого достатньо максимум щоб заповнити прогалини або задовольнити інші короткострокові потреби. Проте у сфері інформаційної безпеки більш доцільним є застосування стратегічних підходів, які допомагають організації будувати систему захисту інформації (СЗІ), розраховану на подолання майбутніх загроз, а також постійна підтримка заданого рівня безпеки. Однак часто організації, що застосовують такі підходи до безпеки, часто не дотримуються узгодженої стратегії, залишаючи себе вразливими.

Більш ефективним варіантом для організацій є впровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки, який здійснює

цілісну оцінку загроз, з якими стикається організація, та вразливостей в її поточному операційному середовищі.

Ризики виникають, коли відбувається перетин існуючої (або потенційної) вразливості та визначеної (або можливої) загрози. Проводячи ретельну оцінку ризиків кібербезпеки, організації оцінюють ризик реалізації кожної можливої вразливості, а потім визначають інтегальний ризик.

Ці показники базуються на поєднанні ймовірності того, що вразливість буде використана зловмисником, і рівень впливу на організацію у разі виникнення такої ситуації. Ризик-орієнтований підхід дозволяє організації зосередити свої зусилля на більш важливих для його діяльності ризиках [3].



Рисунок 1.3 – Схема управління ризиками

У загальному випадку ризики визначаються множиною факторів, що впливають на них. Такі множини можуть перетинатися для окремих ризиків. Якщо від деякого фактора залежать два або більше ризиків, то ці ризики виявляються взаємозалежними. Їх значення необхідно корелювати, оскільки

зміна стану загального для них фактора однозначно призведе до одночасної зміни цих ризиків.

Особливістю ризику ІБ є те, що вони залежать від великої кількості факторів, безліч яких в загальному випадку перетинається з безліччю факторів, від яких залежать практично всі інші ризики. Якщо для маленьких організацій такі перетини ще можна контролювати (або хоча б перерахувати), то для великих організацій зі складною структурою граф факторів та взаємозв'язки між ними збільшуються до таких об'єгів, що їх вкрай важко відслідкувати.

З усіх ризиків із різних сфер ризику ІБ найбільш складні за своєю природою, мають найбільшу невизначеність як по ризикових подій, так і по нанесеним збиткам. Тому факторні моделі ризиків ІБ мають надзвичайно велику розмірність і різноманітні причинно-наслідкові зв'язки і відносини в порівнянні з іншими ризиками [4].

Так, наприклад, подія операційного ризику «Відмова сервера», що сталася внаслідок впливу чинників фізичної природи, значно більш передбачувана, ніж відмова як наслідок впливу людського фактора зловмисної природи. Конфлікт інтересів між зловмисником та власником серверу, що лежить в основі такої події описується незрівнянно більш складною причинно-наслідковою моделлю, ніж факторна модель надійності сервера.

Саме тому «типовий сценарій» значимої ризикової події ІБ (що спричинила значної шкоди організації) зводиться, як правило, до того, що реалізується сукупність подій (часовий ряд) з незначним збитком (часто взагалі без помітної шкоди); в результаті впливу сукупності таких подій створюється і утримується деякий час уразливе середовище - ризикова ситуація і, як наслідок, реалізується вагома за наслідками ризикова подія.

Іншими словами, особливістю ризикових подій і ситуацій ІБ є те, що вони протяжні в часі і мають накоплювальний ефект, тобто будь-яка подія окремо завдає дуже (на практиці такий, яким можна спростувати) малий збиток. В процесі пріорітизації ризиків за РОП події такого характеру отримують найнижчі пріорітети, що призводить до повного ігнорування таких подій. При

цьому незалежно від того, реагуємо ми на ці дрібні, з невеликим збитком інциденти чи ні, якщо їх відбувається багато, то накопичується так званий «негативний потенціал», який, в решті решт, породжує великий та вагомий з точки зору збитків інцидент [4].

Таку особливість в ряді випадків можна змістовно пояснити, наприклад, зловмисник може породжувати безліч дрібних інцидентів в процесі підготовки до атаки при дослідженні певної системи. Тоді інцидент з великим збитком буде результатом успішно проведеної атаки.

Якщо абстрагуватися від будь-яких можливих причин, що лежать в основі накопичення «негативних потенціалів», то в якості гіпотези можна розглядати принцип накопичення «негативного потенціалу» від сукупності інцидентів. Цей принцип підтверджується реально існуючою статистичною структурою інцидентів. У наближеному вигляді ця статистика така [4], що існує відносно велика кількість дрібних інцидентів, що створюють незначний збиток, на деяку кількість таких дрібних доводиться один великий інцидент, істотно перевершуючий дрібні за масштабами, і є особливо великі інциденти, що виникають рідше великих і також істотно перевершують їх за масштабами збитків.

Статистична структура інцидентів незмінна для кожної організації та слабо залежить від видів її діяльності і цілей. Параметри структури можуть бути встановлені через історію (минуле організації), якщо вона зафіксована. Цілком імовірно, що число дрібних інцидентів виявиться на два порядки більше великих, а збиток від одного великого інциденту приносить як мінімум на порядок більше шкоди від усіх дрібних, що припадають на нього. Особливо великі інциденти виникають на три-п'ять великих і перевершують їх або порівняні з ними за масштабам збитку.

В кінці множини інцидентів ризик стрибкоподібно змінюється до дуже великих значень. З принципу накопичення також випливає, що вплив подій ІБ на організацію залежить від її стану, від того, які значення базових ризиків склалися до моменту виникнення подій ІБ. Одна і та ж подія ІБ може дати різний ефект –

від незначного збитку до катастрофічного. Якщо говорити про загальну характеристику ризикових подій ІБ, то це провокують (створюють умови) події, що мають найнижчі пріоритети для організації.

Таким чином, ризикові події ІБ завжди «вкладені» в базові ризики бізнесу (організації) і проявляються у вигляді шкоди, який організація ідентифікує як збиток, пов'язаний з базовим ризиком. Той факт, що збиток був ініційований проблемами інформаційної сфери, не завжди сприймається, а реагування на ризик здійснюється методами, властивими базовим ризикам (економічними, фінансовими, юридичними та ін.). Часто це істотно менш ефективні і більш витратні способи реагування, ніж інформаційні [4].

Очевидно, що для більш осмисленого і якісного реагування на базові ризики організації необхідно відобразити на них інформаційну сферу організації. Однак пряме відображення інформаційної сфери на базові ризикові події або вкрай важко, або взагалі неможливо. Причина цього розрив як семантичний, так і формальний між змістом і формою подання подій в інформаційній сфері організації і кінцевим продуктом (метою) її діяльності.

Менеджмент організацій, як показує практика, більш схильний сприймати виникаючі витрати як наслідки сформованих різного роду ресурсних обмежень, але не інформаційних. Однак та ж практика, тільки *a posteriori*, кожен раз показує, що справа була зовсім не в ресурсних обмеженнях, а зводилася до того, наскільки ефективно організація була здатна добувати корисну для себе інформацію, оцінювати і систематизувати її, аналізувати, накопичувати, узагальнювати, а також своєчасно і раціонально використовувати в своїй діяльності. Без ефективно діючої інформаційної складової навіть спочатку ресурсно надлишковий бізнес загине.

Тому побудова моделі ІБ організації повинно починатися з дослідження (аналізу) ідентифікованих в ній ризиків для цілей діяльності (бізнесу). Метою цього аналізу має бути встановлення контексту ідентифікованих ризиків, тобто визначення умов, сутностей і механізмів реалізації ризикових подій, виду і величини завданої шкоди.

Встановлений контекст дозволить перейти до побудови факторних моделей базових ризиків, тобто до деякої їх формалізації, що наближає їх до сутностей інформаційної сфери. При цьому чинники і обставини, слабо пов'язані з процесами інформаційної сфери, можуть відразу ж фільтрувати як незначущі.

Одночасно необхідно формалізувати і інформаційну сферу в контексті базових ризиків організації. Такий рух назустріч дозволить подолати зазначений вище розрив. Найкращою основою такої формалізації є технологічний аспект, тобто відображення на неї ролей і суб'єктів, а також задієних ними активів і інструментів (інформаційної сфери).

Тепер можна встановити контекст інформаційної сфери для ідентифікованих ризик-факторів, тобто які активи, процеси, інструменти, суб'єкти і ролі відображаються на кожен з ризик-факторів. Тут же, якщо вже накопичено достатньо знань, встановлюється, які саме порушення (регламентів, властивостей або стану) є ознаками (або провісниками) настання подій ІБ. Подальший моніторинг цих сутностей дозволить ідентифікувати частину подій ІБ.

Саме п'ятірка «Активи, Процеси, Інструменти, Суб'єкти, Ролі» («А, П, І, С, Р») схильна до ризиків ІБ, і події, що відбуваються з ними будуть приводити до зміни значень відповідних ризик-факторів і, як наслідок, значень базових ризиків організації та її інтегрального ризику [4].

Очевидно, що п'ятірка «А, П, І, С, Р» визначає змістовно і формально критичну частину інформаційної сфери організації, здатну завдавати збитки і призводити до значних негативних наслідків для цілей організації. Таким чином, у базових ризикових подій завжди через їх ризик-фактори може бути ідентифікований їх контекст в інформаційній сфері організації [4].

Зрозуміло, що якщо перетин контекстів подій не порожній, то між ними виникає зв'язок і можна говорити про пов'язаний ланцюжок подій. Можна також говорити про силу зв'язку з цим, розуміючи під нею кількість ризиків, що залежать одночасно від різних факторів. Тобто чим більша кількість таких ризиків, тим сильніше зв'язок.

Ще більш сильною характеристикою зв'язку є сума завданої шкоди (негативні наслідки) та його інформаційний контекст. У цьому сенсі можна говорити про «понесений збиток» від події, пов'язаний з виявленням факту шкоди. Тут важлива величина збитку і по аналогії з подіями базового ризику ідентифікована з ним п'ятірка «А, П, І, С, Р» [4].

Тобто з точки зору безпеки більш важливо не сама ризикова подія, а наслідки, що наступили, їх оцінка (величина) і ідентифікований контекст, в даному випадку в термінах інформаційної сфери. Зв'язки подій можуть бути неочевидні, особливо в разі понесених збитків і подій базових ризиків. У загальному випадку вони встановлюються в результаті розслідування. Зрозуміло, що ідентифікований таким чином ланцюжок з сильними зв'язками буде відображати мету і застосований спосіб її реалізації для нанесення шкоди.

Описані вище процедури встановлення контексту базових ризиків організації в її інформаційній сфері і «зв'язування» їх з подіями ІБ є основою побудови моделі ІБ організації. Однак практична їх реалізація вимагає більш детального розгляду проблем ідентифікації подій ІБ, управління ІБ, систематизації, оцінювання, аналізу та узагальнення отриманої інформації про стан організації (бізнесу) і її інформаційної сфери.

1.3 Методики ризик-орієнтованого підходу

Розглянемо найбільш відомі методології оцінки ризику [5-8]. Методика CRAMM (CCTA Risk Analysis and Management Method), розроблена Службою безпеки Великобританії в 1985 році, базується на стандартах управління інформаційної безпеки серії BS 7799 і описує підхід до змішаної оцінки ризиків. Перехід від кількісної до якісної шкали показників проводиться за допомогою спеціальних таблиць, що відображають відповідність між показниками різного роду. За даною методикою оцінка ризиків ґрунтується на основі аналізу вартості (цінності) ІТ-активу для організації-власника, вразливостей, потенційних загроз і ймовірності їх реалізації.

Процедура управління ризиками описана у методиці CRAMM передбачає наступні кроки:

1. Ініціювання (Initiation). На даному кроці відбувається серія інтерв'ю із зацікавленими в проведенні оцінки та аналізу ризиків ІБ особами. Сюди можна віднести відповідальних за експлуатацію, налаштування, управління, адміністрування, забезпечення безпеки і застосування ІТ-активів, для яких проводиться аналіз ризиків. Результатом проведення даного етапу є формалізований опис області для подальшого вивчення її меж і визначаються особи, що беруть участь в аналізі інформаційних ризиків.
2. Ідентифікація та оцінка ІТ-активів (Identification and Valuation of Assets). Складається перелік існуючих ІТ-активів, що використовуються організацією в області, частково дослідженій на попередньому етапі. У відповідності до методики CRAMM такі активи можна розділити на декілька видів: дані, програмне забезпечення, фізичні активи. Для усіх виявлених активів визначається вагомість та критичність для забезпечення діяльності підприємства і оцінюються можливі наслідки для його безперервної діяльності від порушення конфіденційності, цілісності чи доступності кожного окремого активу.
3. Оцінка загроз і вразливостей (Threat and Vulnerability Assessment). Окрім оцінки критичності ІТ-активів, важливою складовою методології CRAMM є оцінка ймовірності реалізації вразливостей ІТ-активів. У методології CRAMM наведено таблиці, що встановлюють відповідність між уразливими ІТ-активів і загрозами, які можуть реалізовані, шляхом використання даних уразливостей. Окрім цього, в методології містяться таблиці, що надають інформацію про збиток, що може бути завданим організації в разі реалізації цих загроз. Даний етап застосовується тільки для найбільш критичних ІТ-активів, для яких недостатньо впровадження базового набору заходів забезпечення інформаційної безпеки. Для інших

активів методологія CRAMM описує перелік базових заходів, необхідних для забезпечення інформаційної безпеки.

4. Обчислення ризику (Risk Calculation). Обчислення ризику здійснюється шляхом розрахунку добутку ймовірності реалізації атаки та потенційних збитків внаслідок цього, отриманих на попередніх етапах. Тим часом ймовірність реалізації атаки розраховується за формулою: $P(\text{реалізації}) = P(\text{загрози}) * P(\text{уразливості})$. На даному етапі для кожного виявленого активу формулюються вимоги до набору необхідних заходів щодо забезпечення його безпеки за шкалою від «1» до «7», де значенню «1» відповідає мінімальний необхідний набір заходів, а значенню «7» - максимальний.
5. Управління ризиком (Risk Management). На основі отриманих розрахунків за методологією CRAMM визначається перелік необхідних заходів щодо забезпечення інформаційної безпеки. Наведені методологією заходи порівнюється із вже реалізованими організацією заходами. Після цього можливим є ідентифікація областей, які потребують додаткової уваги до застосованих заходів захисту, а також області з реалізованими надлишковими заходами. Отримана інформація дозволяє більш ефективно формувати стратегію реалізації заходів захисту для приведення рівня ризиків до необхідного рівня.

В контексті практичного застосування методології CRAMM можна виділити наступні переваги:

1. Багаторазово апробована методика, вдосконалена завдяки накопиченому досіду застосування на практиці. Отримані в результаті застосування даної методології оцінки визнаються міжнародними інститутами.
2. Наявність доступного формалізованого опису методології практично нівелює можливість виникнення помилок при проведенні процесів оцінки, аналізу та управління ризиками.
3. Наявність засобів автоматизації процесів значно пом'якшує трудовитрати і час на проведення регламентованих заходів.

4. Розроблені каталоги загроз, вразливостей, наслідків, заходів забезпечення інформаційної безпеки значно зменшують вимоги до рівня наявних спеціальних знань і компетентності учасників процесу аналізу та управління ризиками.

Проте в даній методиці наявні деякі недоліки, серед яких: необхідність значних витрат на організацію процесу, узгодження результатів за участі великої кількості зацікавлених осіб та неможливість дати оцінку ризиків в точному грошовому виразі, що ускладнює використання отриманих результатів оцінки при техніко-економічному обґрунтуванні необхідного рівня інвестицій на побудову та використання засобів і методів захисту інформації.

Методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), розроблена Університетом Карнегі-Мелон в 2007 році. В даній методиці викладено метод якісної оцінки ризиків. Головним призначенням OCTAVE є формалізація та оптимізація заходів з оцінки ризиків інформаційної безпеки в організації, мінімізація необхідних ресурсів для отримання бажаних результатів. Однією з особливостей даної методології є те, що персонал, технології, комп'ютерні системи, додатки, і т.д. розглядаються в контексті їх відношення до інформації та процесів та послуг, які вони реалізують.

Згідно з методикою OCTAVE весь процес управління ризиками інформаційної безпеки можна поділити на такі етапи:

- Визначення пріоритетів

На даному етапі визначаються критерії для оцінки ризиків. Дані критерії формуються у вигляді переліку якісних параметрів, за допомогою яких відбувається опис ризику. Серед параметрів можуть бути ймовірність реалізації загрози, потенційний збиток в результаті успішної атаки та інші можливі наслідки для організації. Окрім цього, на даному етапі ідентифікуються найбільш критичні області діяльності організації, для яких задаються різні рівні прийнятного ризику.

- Профілювання активів

На цьому кроці створюються профілі наявних активів. Профіль представляється у вигляді опису активу, в якому зазначено його унікальні особливості, характеристики, якості, цінність та вимоги до забезпечуваного рівня інформаційної безпеки. Набір таких документів складає основу для виявлення потенційних загроз і відповідних ризиків на наступних кроках.

Ідентифікація середовища активів. На доному етапі описуються місця зберігання, умови транспортування та обробки наявних активів. Будь-які ризики для середовища існування та функціонування активу успадковуються самим активом, і даний факт має ще більшу вагу для тих активів, що отримує організація від зовнішніх постачальників.

– Ідентифікація загроз

Наступними ідентифікуються так звані «слабкі місця» в організації. Даний етап є основоположним для процесу виявлення ризиків шляхом «мозкового штурму» учасників проектної команди. Результатом даного кроку є перелік високорівневих областей та типів ризиків, що є потенційно можливими для аналізованих наявних в організації активів.

Проектування сценаріїв потенційних загроз. Методологія OCTAVE визначає наступні види загроз: людський фактор у поєднанні із використанням технічних засобів, людський фактор із застосуванням фізичного доступу, а також технічні та інші можливі проблеми. Для кожного виду виявлених загроз (для кожного активу) визначаються сценарії реалізації загроз із характеристикою наслідків їх впливу на активи та ймовірністю виникнення. Оскільки в даній методології використовуються якісні шкали, ймовірність може бути визначеною як низька, середня або висока. Для спрощення та формалізації даного процесу методологія OCTAVE пропонує спеціальні опитувальні листи.

– Ідентифікація та обробка ризиків

Ідентифікація ризиків. Аналізуючи отриману на попередньому кроці інформацію про найбільш ймовірні сценарії реалізації загроз,

проводиться детальний аналіз їх впливу на активи та діяльність організації.

Аналіз ризиків. На даному етапі аналізується отримана раніше інформація, проводиться оцінка впливу потенційних загроз на основну діяльність організації та за результатами наявні ризики ранжуються відповідно до критеріїв, визначених на першому етапі.

Вибір підходу до обробки ризиків. На даному кроці визначаються стратегії обробки, що будуть застосовані окремо до кожного з виявлених ризиків в залежності від його впливу на ресурси та діяльність організації.

Отже, можемо виділити наступні переваги даної методології:

- Доступність та прозорість описаних процесів оцінки та аналізу ризиків зменшує необхідний час на вивчення методики та підготовку до її застосування.
- Рекомендований ітеративний підхід дозволяє поступово збільшувати рівень деталізації аналізу ризиків інформаційної безпеки в залежності від наявних потреб в організації та актуального обсягу необхідних ресурсів;
- Спеціально шаблонізовані матеріали, що супроводжують процес роботи з ризиками надають можливість відтворюваності результатів, полегшують ведення необхідної документації.

Однак методології OCTAVE притаманні також деякі недоліки:

- Відсутність деталізованих допоміжних матеріалів, таких як каталоги загроз, вразливостей, можливих наслідків та необхідних заходів забезпечення інформаційної безпеки підвищують вимоги до рівня спеціальних знань і компетентності учасників процесів оцінки, аналізу та управління ризиками.
- Неможливість дати оцінку ризиків в точному грошовому виразі, що ускладнює використання отриманих результатів оцінки при техніко-економічному обґрунтуванні необхідного рівня інвестицій на побудову та використання засобів і методів захисту інформації.

Методологія OCTAVE часто використовується для проведення якісної оцінки ризиків інформаційної безпеки та аналізу результатів. Актуальною вона може виявитися для організацій, реалізуючих первинне впровадження підходу до управління ризиками, у яких бракує ресурсів для реалізації процесів аналізу та управління ризиками інформаційної безпеки для всієї організації і, таким чином, виникає потреба в пріоритизації існуючих ризиків від найбільш критичних до ризиків нижнього рівня, та реалізації відповідних політик. Описана методологія дозволяє поступово поширювати впровадження зазначених процесів на всю структуру організації[7].

Методика управління ризиками інформаційної безпеки, що запропонована корпорацією Microsoft в 2006 році, викладена в її «Керівництві з управління ризиками безпеки». Дана методика дозволяє отримувати комбінований тип результатів. Згідно із MSAT об'єднуються компоненти кількісного і якісного підходів. В процесі оцінки якісний компонент застосовується для більш швидкої класифікації переліку всіх можливих ризиків ІБ, тим часом як кількісний дає можливість в подальшому провести більш деталізований аналіз найбільш вагомих ризиків. Це сприяє формуванню відносно невеликого набору пріоритетних ризиків, які потребують детального дослідження, і концентруванню зусиль на даний перелік.

Згідно із даною методологією, управління ризиками інформаційної безпеки є неперервним процесом, що складається із таких етапів:

1. Оцінка ризиків

- Побудова плану по збору необхідних даних.
- Збір перерахованих даних за розробленим планом.
- Пріоритизація виявлених ризиків.

2. Підтримка прийняття рішень

- Формулювання функціональних вимог сприятливих для зниження можливих ризиків.
- Формування перспективних рішень для забезпечення контролю.

- Експертиза сформованих рішень і тестування запропонованих компонентів контролю на відповідність визначеним функціональним вимогам.
- Оцінка зниження ризику – оцінка можливості зменшення впливу або зниження ймовірності ризиків.
- Оцінка вартості рішення – оцінка потенційних прямих і непрямих витрат, необхідних для реалізації плану по нейтралізації ризику.
- Вибір стратегії нейтралізації ризику – пошук та формулювання найбільш прийняттого варіанту по нейтралізації ризику шляхом проведення аналізу можливих вигод і витрат.

3. Етап реалізації контролю

- Вибір цілісного підходу – залучення персоналу і технологій у процес реалізації стратегії мінімізації ризику.
- Організація зпроцесу згідно із принципом багаторівневого захисту.

4. Етап оцінки ефективності програми

- Оцінка існуючого рівня і реалізованої зміни ризику, шляхом використання попередньо розробленої системи показників.
- Оцінка ефективності реалізованих заходів – оцінка застосованих підходів до управління ризиками для виявлення можливостей покращення.

Методика управління ризиками ІБ, що розроблена корпорацією Microsoft, детально описує інструкції та рекомендації по втіленню усіх зазначених кроків управління ризиками, містить огляд важливіших факторів успіху, а також типові набори активів, загроз, вразливостей. Також в методиці наводяться шаблони документів, потрібних в процесі управління ризиками інформаційної безпеки[8].

Методологія Microsoft має наступні сильні сторони:

- Доступність описаного підходу до організації процесу управління ризиками інформаційної безпеки, що дає можливість більш легкого застосування та донесення керівництву організації для ухвалення;

- Комбінування якісного і кількісного підходу до оцінки ризиків дає можливість розробки більш адекватних по ресурсності кількісних оцінок, тобто лише для тих ситуацій, коли це потрібно для ефективної організації управління ризиками інформаційної безпеки;
- Наявність можливості застосування засобів автоматизації процесу оцінки та аналізу ризиків дозволяє зменшити трудовитрати і час необхідні для виконання даних заходів;
- Деталізація кожного з кроків процесу управління ризиками інформаційної безпеки дає можливість мінімізувати ймовірність помилок учасників процесу аналізу та управління ризиками;
- Застосування неперервного циклу при організації процесу управління ризиками дозволяє проводити регулярну безперервну оцінку ризиків та підтримувати в актуальному стані дані про наявний рівень ризику, та необхідні заходи з управління ризиками;
- Можливість оцінки ризиків інформаційної безпеки у грошовому(кількісному) виразі дає можливість використання результатів оцінки ризиків при побудові економіко-вартісного плану побудови системи захисту;
- Наявність усіх необхідних допоміжних матеріалів, що супроводжують процес аналізу ризиків.

Для даної методології можна виділити наступні недоліки:

- Високий рівень трудомісткості описаного процесу управління ризиками інформаційної безпеки робить необхідним наявність досить значних ресурсів для його реалізації;
- Невизначеність типових ризикових сценаріїв підвищує необхідність додаткових трудовитрат учасників проведення визначення можливих для організації сценаріїв появи та реалізації ризиків інформаційної безпеки.

Методика Microsoft широко використовується в урядових та комерційних організаціях по всьому світу. Дана методологія може бути застосована великими

організаціях або організаціями з високим рівнем залежності бізнес-діяльності від інформаційних активів та їх конфіденційності. Дана методика загалом орієнтована на організації, реалізуючих первинне впровадження підходу до управління ризиками, у яких бракує ресурсів для реалізації процесів аналізу та управління ризиками інформаційної безпеки для всієї організації і, таким чином, виникає потреба в пріоритизації існуючих ризиків від найбільш критичних до ризиків нижнього рівня, та реалізації відповідних політик. Описана методологія дозволяє поступово поширювати впровадження зазначених процесів на всю структуру організації [7].

Висновки до розділу 1

В даному розділі наведено результати аналізу існуючих стандартів у галузі інформаційної безпеки. За результатами аналізу можна розділити існуючі документи на дві групи. Першу започатковано від найстарішого стандарту в галузі інформаційної безпеки - «Помаранчевої книги». Сюди також належать розроблені пізніше «Федеральні критерії», «Канадські критерії», а сучасним представником даної гілки виступають «Загальні критерії оцінки безпеки інформаційних технологій» - ISO/IEC 15408. Ключовою ідеєю стандартів цієї гілки є так званий захист «із повним перекриттям», орієнтація здійснюється на статичні, замкнуті системи, що у загальному випадку характерні для військової сфери та дуже рідко – для комерційної.

До другої ж групи можна віднести документи, що за основу взяли стандарти серії BS 7799 (British Standards) і за своїм змістом інтегруються із стандартами якості менеджменту серії ISO 900X. Саме з даної групи стандартів беруть початок основні принципи управління інформаційною безпекою.

Сучасними представниками документів цієї групи є серія стандартів ISO/IEC 2700X. Важливою відмінністю даних стандартів від першої групи є регламентування ризик-орієнтованого підходу до управління інформаційною безпекою (УІБ). Проте застосування даного підходу на практиці викликає певну

кількість запитань. Зокрема для великих організацій із складною ієрархічною структурою розрахунок їх інтегральних ризиків являє трудомістку довготривалу процедуру, результати якої виявляться приблизними та неоднозначними. Крім того, вельми суб'єктивним є формування переліку адекватних загроз: перестраховка, намагання не пропустити істотної загрози призводить до невиправданого розширення складу переліку загроз, що у свою чергу тягне за собою надлишкові інвестиції у створення системи захисту інформації (СЗІ).

Це питання є дуже болісним і важливим для комерційних організацій, виникає потреба у перегляді використовуваних підходів до формування базових принципів побудови СЗІ та політик УІБ в цілому, підсиленні в них ваги економічної складової, формування цих політик залежно від потенціалу та спроможності атакуючої сторони, адаптуючись до особливостей її поведінки, ймовірних намірів та можливостей.

2 АДАПТИВНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Проактивний захист

Одним із перших проявів використання адаптивного підходу у сфері інформаційної безпеки є розробка проактивного захисту. В останні кілька років на ринку антивірусної безпеки активно обговорюється тема «смерті» класичних антивірусів, що використовують для детектування шкідливого ПО ті чи інші види сигнатур. Основною причиною цього називається швидкість поширення шкідливого ПЗ, яка вище за швидкість розповсюдження оновлень антивірусної бази і, до того ж, на аналіз нового вірусу завжди потрібен якийсь час. Таким чином, на час від виявлення нової шкідливої програми до появи оновлення антивірусного оновлення користувачі залишаються беззахисними. Виходом з даної ситуації різні компанії бачать кілька підходів [12].

- Евристичний аналізатор. Коли кількість вірусів перевищила кілька сотень, антивірусні експерти задумалися над ідеєю детектування шкідливих програм, про існування яких антивірусна програма ще не знає, оскільки відсутні відповідні сигнатури. В результаті були створені так звані евристичні аналізатори. Евристичним аналізатором називається набір підпрограм, які аналізують код виконуваних файлів, макросів, скриптів, пам'яті або завантажувальних секторів для виявлення в ньому різних типів шкідливих комп'ютерних програм, не обумовлених звичайними (сигнатурними) методами. Іншими словами - евристичні аналізатори призначені для пошуку невідомого шкідливого ПЗ. Рівень детектування у евристичних аналізаторів не дуже високий, так як існують десятки різних методів їх «обману», якими користуються автори вірусів. Крім цього, для евристичних аналізаторів з високим рівнем виявлення характерний високий рівень помилкових спрацьовувань, що робить їх використання

неприйнятним. Навіть у найкращих антивірусів рівень виявлення нових шкідливих програм не перевищує 25-30%. Незважаючи на невисокий рівень виявлення, евристичні методи залишаються одним із провідних методів в сучасних антивірусах. Причина проста - комбінація різних методів превентивного виявлення призводить до підвищення якості ідентифікації.

- Безпека на основі політик. Політика безпеки є необхідним атрибутом будь-якої продуманої стратегії захисту від загроз. Продумана політика дозволяє в кілька разів зменшити ризик зараження шкідливою програмою, атаки хакерів або витоку конфіденційної інформації. Простий приклад - заборона автоматичного відкриття вкладених файлів з електронних листів знижує ризик зараження поштовим хробаком практично до 0. Заборона на використання змінних носіїв також знижує ризик впливу шкідливого коду. До розробки політики завжди потрібно підходити дуже виважено і враховувати потреби і бізнес-процеси всіх підрозділів і працівників компанії. Крім вищеприписаного підходу до політики безпеки, в матеріалах різних виробників зустрічаються згадки безпеки на основі політик (policy-based security). На сьогоднішній день існує декілька підходів до такого способу забезпечення безпеки. Підхід Trend Micro - Trend Micro Outbreak Prevention Services. Даний сервіс передбачає поширення деяких політик, що дозволяють запобігти епідемії. Тобто політика поширюється до появи оновлення антивірусних баз або патчів. З першого погляду здається, що дане рішення виглядає розумним, але справа в тому, що швидкість додавання процедур виявлення нового malware в Trend Micro низька і дане рішення зроблено для того, щоб «заткнути дірку» повільної роботи антивірусної лабораторії TrendLab. Крім цього, на формування політики також потрібен час (не завжди менше, ніж на аналіз вірусу для додавання процедур детектування в антивірусну базу) і все одно є проміжок часу, в який користувач залишається беззахисним перед новою загрозою. Іншим недоліком даного підходу є частота зміни політик безпеки. Всі плюси від

безпеки на основі політик полягають в малій частоті зміни самої політики. Це дозволяє персоналу звикнути до того, що і як робити можна, а що заборонено. Якщо ж політики будуть змінюватися по кілька разів на день, це просто внесе сум'яття і призведе до того, що ніякої політики безпеки не буде. Коректніше за все назвати метод Trend Micro HE policy-based security, а прискореним випуском деяких сигнатур. Отже, такий підхід не є в більшості випадків проактивним. Виняток становлять політики, які роблять неможливою експлуатацію тих чи інших вразливостей в програмному забезпеченні.

- Підхід Cisco-Microsoft. Обмеження доступу в корпоративну мережу для комп'ютерів, які не відповідають політиці безпеки компанії (наприклад, відсутні необхідні оновлення операційної системи, немає останніх оновлень антивірусних баз і т.д.). Для приведення комп'ютера у відповідність політиці, виділяється доступ тільки на спеціальний сервер оновлень. Після установки всіх необхідних оновлень і виконання інших дій, необхідних згідно з політикою безпеки, комп'ютер отримує доступ в корпоративну мережу.
- Intrusion Prevention System. Системи запобігання вторгнень (IPS) передбачають можливість закриття найбільш часто використовуваних шкідливими програмами вразливостей комп'ютера перед новою загрозою ще до виходу оновлення антивірусних баз: блокування портів, тобто можливості попадання інфекції на комп'ютер і її подальшого розмноження; створення політик для обмеження доступу до тек або окремих файлів; виявлення джерела інфекції в мережі і блокування подальших комунікацій з ним. Дана технологія відмінно працює проти атак хакерів і безфайлових черв'яків і вірусів, але проти поштових черв'яків, класичних вірусів і троянських програм IPS неефективна.
- Захист від переповнення буфера. Ідея технології - не допустити переповнення буфера для найбільш поширених програм, сервісів Windows, включаючи Word, Excel, Internet Explorer, Outlook і SQL Server. При

більшості сучасних атак задіюються різні уразливості, що використовують переповнення буфера. Запобігання переповнення буфера також можна віднести до проактивного захисту, тому що ця технологія просто виключає використання такої вразливості будь-яким шкідливим кодом або атакою.

- Поведінкові блокувачі. Історія поведінкових блокувачів нараховує вже понад 20 років. Даний вид антивірусного ПЗ не був популярним 15 років тому, але з появою нових видів загроз про поведінкові блокувачі знову згадали. Основна ідея блокувача – аналіз поведінки програм і блокування виконання будь-яких небезпечних дій. Теоретично блокувач може запобігти поширенню будь-якого, як відомого, так і невідомого (написаного після блокувача) вірусу. Саме в цьому напрямку і рухається більшість розробників антивірусного ПЗ. Прикладів реалізації даної технології досить багато. Останнім часом більшість систем запобігання поширенню поштових черв'яків за механізмом є поведінковими блокаторами. Перше покоління поведінкових блокувачів з'явилося ще в середині 90-х років (в самий розпал епохи DOS-вірусів). Принцип їх дії був простий – при виявленні потенційно небезпечних дій ставилося запитання користувачеві – дозволити або заборонити дію. У багатьох випадках такий підхід працював, але «підозрілі» дії виробляли і легітимні програми (в тому числі і самі операційні системи) і якщо користувач не мав належної кваліфікації, питання антивіруса викликали нерозуміння. З проникненням персональних комп'ютерів все глибше в повсякденне життя знижувався середній рівень кваліфікації користувачів і потреба у перших поведінкових блокувачах зменшилась.
- Поведінковий блокувач для VBA-програм. KAV Office Guard. Як уже згадувалося вище, основним недоліком перших поведінкових блокіраторів була велика кількість (часто незрозумілих) запитів до користувача. Причина цих запитів – нездатність поведінкового блокіратора самостійно судити про шкідливість тієї чи іншої дії. Однак, якщо розглядати програми, написані на VBA, то можна з дуже великою часткою ймовірності

відрізнити шкідливі дії від корисних. Саме завдяки цьому KAV Office Guard не настільки «нав'язливий», як його файлові брати. Але, задаючи менше питань користувачеві, цей блокувач не став менш надійним. Іншими словами, використовуючи переваги операційного середовища, вдалося домогтися розумного балансу між надійністю і кількістю питань. Але, тим не менш, KAV Office Guard за принципом своєї роботи є дуже схожим до перших поведінкових блокувачів.

- Поведінкові блокувачі другого покоління. Друге покоління поведінкових блокувачів відрізняє те, що вони аналізують не окремі дії, а послідовність дій, і вже на підставі цього робиться висновок про шкідливість того чи іншого ПЗ. Це значно зменшує кількість запитів до користувача і підвищує надійність детектування. Як приклад поведінкового блокувача другого покоління можна привести систему Proactive Defense Module.

Різні підходи до проактивного захисту. Перший продукт з нового покоління комерційних систем проактивного захисту на основі поведінкового блокіратора – StormFront – випустила компанія Okena, яка спеціалізувалася на розробці систем виявлення і запобігання вторгнень. У січні 2003 року компанія Okena була поглинена компанією Cisco Systems, і StormFront вийшов під назвою Cisco Security Agent. Даний продукт є класичним поведінковим блокатором і розрахований на використання в компаніях. Продукт вимагає попереднього налаштування кваліфікованим адміністратором. Компанія McAfee активно розвиває проактивні технології захисту в своїх продуктах сімейства McAfee Enterscept. Вони передбачають можливість закриття уразливості комп'ютера перед новою загрозою ще до виходу оновлення антивірусних баз (IPS / IDS): блокування портів, тобто можливостей потрапляння інфекції на комп'ютер і її подальшого розмноження; створення політик для обмеження доступу до тек або окремих файлів; виявлення джерела інфекції в мережі і блокування подальших комунікацій з ним. Крім цього, продукти не допускають переповнення буфера для приблизно 20 найбільш поширених програм і сервісів Windows, включаючи Word, Excel, Internet Explorer, Outlook і SQL Server, що також можна віднести до

проактивного захисту. У персональних продуктах застосовується тільки вдосконалена евристична технологія WormStopper для детектування інтернет-хробаків, які розповсюджуються по електронній пошті, що блокує підозрілу активність на комп'ютері, таку, наприклад, як відправка великого числа неавторизованих електронних повідомлень особам з адресної книги. Panda TruPrevent включає в себе три компоненти: поведінковий аналізатор процесів для дослідження поведінки запущених в системі процесів і виявлення підозрілих дій, евристичний аналізатор і набір IDS-функцій для виявлення шкідливих мережевих пакетів і захисту від переповнення буфера. Продукт позиціонується компанією Panda Software як друга лінія оборони від будь-якого невідомого шкідливого ПО (в якості першої лінії повинен виступати класичний антивірус) і призначений для виявлення невідомого malware, що запускається на комп'ютері. Продукт орієнтований на кінцевого користувача (не адміністратор).

У продуктах Symantec в якості проактивного захисту використовується вбудований евристичний аналізатор, здатний виявляти ще невідомі модифікації вірусів на підставі їх специфічних дій в системі, а також компоненти IPS / IDS (Intrusion Prevention / Detection System) Norton Internet Worm Protection, які дозволяють закрити найбільш поширені шляхи потрапляння інфекції в систему (Prevention) і детектувати підозрілі дії (Detection). Додатково компанія пропонує Outbreak Alert – засіб оповіщення про появу особливо небезпечних інтернет-загроз (входить до складу Norton Internet Security 2005). Крім цього, на рівні сервісів Symantec пропонує послугу Early Warning Services (EWS) яка дозволяє отримувати ранні оповіщення про виявлені вразливості. В даний час послуга інтегрується в нову систему Global Intelligence Services.

Microsoft також працює в напрямку розробки проактивних методів захисту від шкідливого ПЗ.

Trend Micro в якості проактивного захисту PC-cillin Internet Security використовує евристичний аналізатор і Outbreak Alert System - проактивне оповіщення про нові наступаючих загрози. У корпоративному продукті Trend Micro OfficeScan Corporate Edition використовуються сигнатури з Outbreak

Prevention Service, які дозволяють автоматично встановлювати захисні правила для запобігання заражень ще до виходу оновлення антивірусних баз. Така можливість відсутня в персональному продукті.

У продуктах BitDefender під проактивним захистом мається на увазі поведінковий аналізатор, який блокує шкідливі програми на підставі аналізу їх специфічних дій в системі (контролюються системні файли, реєстр і інтернет-активність).

У нових продуктах об'єднаний ряд новітніх технологій проактивного захисту. Використовується і система виявлення і запобігання вторгнень (IPS / IDS), спрямована на боротьбу з хакерськими атаками і безфайловими вірусами. Система нотифікації дозволяє попереджати користувачів про епідемії та інші події, що стосуються безпеки. Але найбільш важливим нововведенням, з точки зору боротьби з новими загрозами, є поведінковий блокувач другого покоління. Даний блокувач відрізняє важлива особливість - «відкат» дій, скоєних шкідливим кодом. Це дозволяє значно скоротити кількість питань користувачеві і зменшити ризик пошкодження системи до детектування нового шкідливого ПО.

Інші методи

Для захисту поштового трафіку можуть використовуватися особливі методи, засновані на аналізі листів, що проходять через поштовий сервер. За допомогою такого аналізу можна зупинити епідемію в самому її початку. Статистика, що дає підстави підозрювати початок епідемії, може бути наступною: масова розсилка або прийом однакових вкладень; масова розсилка або прийом однакових листів з різними вкладеннями; наявність подвійного розширення у вкладень і т.д. Крім цього, можливий лінгвістичний аналіз змісту листів.

2.2 Адаптивний підхід в теорії управління

Класичні підходи до управління будуються припущенні про те, що можна отримати нехай складну, але точну аналітично задану форму функціональної

залежності вхідних і вихідних сигналів системи управління з подальшими уточненнями значень коефіцієнтів, що входять в неї [9]. Однак при всій витонченості напрацьованого математичного інструментарію областю застосування таких методів управління залишаються порівняно прості об'єкти управління з очевидними властивостями, тобто добре формалізовані об'єкти. На практиці ж типовими є об'єкти управління, які формалізуються погано. Їх властивості апіорі погано відомі або змінюються в процесі функціонування. Через недостатність знань про об'єкт і середовищі, в якому він функціонує, спроби отримати точну модель поведінки такого об'єкта не представляються можливими. Однак управління такими об'єктами представляє не менший інтерес і є не менш важливим, ніж управління добре формалізованими об'єктами.

В останні роки активно розвивається так званий некласичний підхід до теорії управління. Такий підхід пов'язують із застосуванням алгоритмів і методів інтелектуального управління автономними рухомими об'єктами на основі нечіткої логіки, нейронних мереж і генетичних алгоритмів. З цим же підходом пов'язані ситуаційне управління на основі ієрархічних моделей з нечіткими предикатами; моделі і алгоритми прийняття рішень щодо захисту інформації на основі методів штучного інтелекту. Автори пропонують для цього використовувати висновок по прецедентах - метод прийняття рішень, в якому використовуються знання про ситуації або прецеденти, що вже мали місце раніше. При розгляді нової проблеми (поточного випадку) відшукується схожий прецедент. Замість того щоб кожен раз шукати рішення спочатку, можна спробувати використовувати рішення, прийняте в схожій ситуації, можливо, адаптувавши його до поточного випадку. У ситуації, коли відомих параметрів об'єкта управління та навколишнього середовища недостатньо для однозначного визначення поведінки цього об'єкта, управління необхідно здійснювати не за параметрами об'єкта, а по його стану, який більш повно визначає тенденцію його подальшої поведінки. Виникає запитання ідентифікації стану об'єкта управління з його спостережуваними (відомими) параметрами. Для цього потрібно вміти сформулювати на основі апіорної інформації узагальнені образи - класи станів

об'єкта. Отримати необхідні знання з набору наявних даних можна за допомогою методів видобутку даних - класифікації та кластеризації. Якщо стан об'єкта управління зводиться до присутності в одному з цих класів, то керуючий вплив можна розглядати як відображення об'єкта з одного класу в інший (зокрема, як утримання об'єкта в тому ж класі). У розглянутих ситуаціях замість точного виду математичної моделі об'єкта доступна тільки апріорна інформація про стани об'єкта управління, керуючих впливах на нього і результати впливів. У термінах виведення з прецедентів інформація про стан об'єкта - це опис проблеми, а видача керуючого впливу є вирішення проблеми; тоді результат керуючого впливу необхідно розглядати як результат застосування рішення [9].

Таким чином, постає необхідність у підході до інтеграції методів видобутку даних, виведення на основі прецедентів і адаптивного управління в єдиній самонавчальній системі, що дозволяє управляти об'єктами з погано формалізованих поведінкою. У цьому підході стан об'єкта управління порівнюється з прецедентами з заздалегідь накопиченої бази даних. На основі якоїсь міри близькості обирається один з схожих прецедентів. Керуючий вплив, пов'язаний з ним, використовується безпосередньо або адаптується до поточних потреб, виходячи зі ступеня близькості прецеденту. Результат впливу також прогнозується по прецеденту. Підсумок впливу заноситься в базу прецедентів для подальшого використання [9].

Одночасно ставиться і більш конкретне завдання вибору міри близькості для визначення подібності керованого об'єкта з прецедентами. Шукана міра повинна сприяти обмеженню перебору можливих варіантів, їх ранжування при виборі керуючих впливів, а також полегшення адаптації керуючого впливу від прецеденту до поточного стану об'єкта управління.

Для розкриття змісту терміна адаптивність в теорії управління необхідно розглянути основні типи керуючих систем.

При моделюванні процесів управління зазвичай розглядають три типи управління [9]:

- відкрите, або розімкнуте,

- замкнуте, або управління зі зворотним зв'язком, і
- адаптивне.

Перший тип - розімкнуте управління, яким передбачається наявність мети, що визначає напрямок керуючого впливу для досягнення цієї мети. Структура розімкнутого управління проста. Відсутність зворотного зв'язку спрощує управління. При відхиленні результату від запланованого проводиться аналіз, який пояснює причини відхилення, але не ставить завдання змінити що-небудь в управлінні.

Другий тип - замкнуте управління (управління зі зворотним зв'язком), при якому передбачається можливість змінювати управління в залежності від його впливу на кінцевий результат. Ця методика управління розрахована в основному на малі проміжки часу. Якщо ж результат впливу фактора проявляється через досить великий час, часто виникають значні труднощі.

Третій тип - адаптивне управління відрізняється від замкнутого наявністю моделі керованого об'єкта, в якій аналізуються можливі наслідки управління (прогноз). Правильна реакція можлива лише при побудові максимально точної моделі об'єкта, адекватно відображаючої середовище функціонування і сам об'єкт управління.

З терміном адаптація пов'язані поняття адаптивного управління, адаптивної системи і адаптивної моделі [9]. Адаптація - це процес зміни параметрів і структури системи, а можливо, і керуючих впливів на основі поточної інформації з метою досягнення певного, зазвичай оптимального, стану системи при початковій невизначеності в умовах, що змінюються в процесі роботи.

Адаптивною вважають систему, яка може пристосовуватися до змін внутрішніх і зовнішніх умов. Адаптивна система зберігає працездатність при непередбачених змінах властивостей керованого об'єкта, цілей управління або навколишнього середовища шляхом зміни алгоритму свого функціонування, програми поведінки або пошуку оптимальних станів.

Поняття управління з адаптацією (адаптивне управління) - це управління в

системі з неповною апріорною інформацією про керований процес, яке змінюється в міру накопичення інформації і застосовується з метою поліпшення якості роботи системи.

Адаптивної моделлю системи управління об'єктом вважають таку модель, в якій в результаті зміни характеристики внутрішніх і зовнішніх властивостей об'єкта відбувається відповідна зміна структури і параметрів регулятора управління з метою забезпечення стабільності функціонування об'єкта.

Неможливість точної математичної формалізації структури об'єкта, похибка вимірювань, відсутність достовірної інформації про початкові координати, наявність непередбачуваних зовнішніх впливів зумовлює необхідність реагування управляючих впливів на зміни параметрів об'єкта і характеристик зовнішнього середовища. Такого роду адаптація (приспосовування) відбувається шляхом зміни структури і параметрів регулятора.

Конкретизація визначення адаптації пов'язана з цілями дослідження і конструювання. Таким чином, основна властивість адаптивних систем – реалізація мети управління в умовах недетермінованої зовнішнього середовища і змінних параметрів об'єкта.

2.3 Адаптивна безпека

Постійне поповнення множини актуальних загроз та їх різноманіття нашоюхує на пошук нових, більш гнучких підходів до побудови стратегій управління інформаційною безпекою.

Стрімко еволюціонуюче середовище роботи програмних засобів, комп'ютерних систем та мереж створює нові загрози, а статичні механізми забезпечення ІБ виявляються дієвими далеко не у всіх ситуаціях. Таким чином, виникає потреба у програмному забезпеченні, здатному до саморегулюванні та адаптації механізмів безпеки. Метою адаптації є забезпечення належного рівня безпеки в різних ситуаціях. Самоадаптивне програмне забезпечення - це система із замкнутим циклом із зворотним зв'язком, спрямована на коригування реакцій

під час роботи [10]. Це досягається за допомогою компонентів моніторингу та модифікаційних компонентів. Компоненти моніторингу контролюють навколишнє середовище, виявляючи зміни, а модифікатори виконують адаптацію. З точки зору безпеки, відстежувані зміни стосуються змін середовища та використання, які впливають на необхідний або досягнутий рівень безпеки. Модифікаційний компонент зосереджується на механізмах та політиці безпеки.

Наразі дуже розхпвсюдженням є застосування організаціями для вирішення питань теми інформаційної безпеки так звані часткові підходи [10]. Такі підходи зазвичай формуються під впливом досвіду організації, суб'єктивного сприйняття ризиків інформаційної безпеки адміністраторами, наявного рівня доступних ресурсів, зокрема фінансових. Однією із ключових причин такої ситуації є схильність адміністраторів реагувати лише на зрозумілі для них події. Проте таким чином велика кількість важливих подій може залишитись без уваги. Такі адміністратори часто сподіваються, що усі випадки неправильного використання ресурсів системи і ознаки зовнішніх атак будуть виявлені та зафіксовані технічними засобами, проте рівень їх компетентності у можливих вразливостях мереж, операційних систем, програмному забезпеченні не завжди відповідає очікуваному. Характерним для сучасних адміністраторів безпеки є також наявність знань про існуючі міжмережеві екрани, системи розмежування доступу, криптографічний захист, системи авторизації та аутентифікації, проте недостатній рівень обізнаності в необхідних технічних характеристиках даних систем для забезпечення надійного захисту. Подібний підхід до організації процесу забезпечення інформаційної безпеки дозволяє на практиці захиститися лише від 20-30% існуючих загроз. Даний підхід можна описати формулою Безпека = Традиційні засоби захисту [10].

Насправді, такий варіант є досить суб'єктивним та недалекоглядним представленням на багатогранного захисту. Застосовуючи такий підхід можна зменшити лише деякі виявлені ризики, а в той самий час залишити інші існуючі ризики зовсім без уваги. Такий підхід не дає керівництву організації побачити

справжній рівень захищеності активів, оскільки обіцяне значно перевищує реальну кількість усунених загроз.

Без застосування більш глибинного підходу, згідно з яким формується єдина політика безпеки, визначаються умови поточного контролю системи істотно знизити рівень існуючих ризиків практично неможливо. До того ж стрімкий та безперервний розвиток інформаційних технологій постійно поповнює перелік актуальних загроз.

Безліч сучасних організацій витрачають багато часу на те, щоб виявити закономірності постійного розвитку загроз. Проте ключевим в даному питанні є зменшення прогалини між узгодженою політикою безпеки та її втіленням на практиці.

Таким чином, можна виділити найперший крок для побудови надійної системи захисту – підвищення рівня кваліфікації персоналу. Важливо, щоб учасники процесу захисту чітко дотримувались стандартизованого узгодженого підходу до забезпечення безпеки, могли впроваджувати процедури і технічні засоби захисту, проводили неперервний контроль підсистем захисту та аудиту, що будуть забезпечувати виявлення та аналіз якомога більшої частини існуючих потенційних загроз.

Швидкий розвиток доступних технологій за відсутності безперервного проведення аналізу їх захищеності призводить до падіння рівня інформаційної безпеки активів, оскільки виникають нові невраховані раніше загрози і вразливості системи, які автоматично стають чорним ходом для зловмисників.

Отже, формулу побудови надійної системи забезпечення мережевої безпеки можна описати наступним чином: Безпека = Політика безпеки + Традиційні засоби захисту + Аналіз ризику + Реалізація контрзаходів. Для такого підходу рівень ефективності СЗІ можна оцінити в 40-60% [10].

Для такого підходу необхідним заходом для побудови системи захисту є оцінка ризиків. Реалізація даного заходу передбачає виявлення та ранжування існуючих вразливостей (за рівнем потенційної шкоди організації). Враховуючи постійні зміни в конфігурації мережі, процес оцінки ризиків має безперервно

відтворюватись. Ефективність побудованої системи захисту буде напряду залежати від прийнятих в процесі рішень, їх зваженості, доцільності, та здатністю бути адаптованими до нових умов середовища функціонування.

Проте важливо усвідомлювати, що через певний проміжок часу настане момент зміни конфігурацій системи адміністраторами чи користувачами. Будь-які зміни будуть знову відкривати двері для великої кількості вразливостей, пов'язаних з операційними системами та програмним забезпеченням. Крім того, технології, що їх супроводжують розвиваються неймовірно швидко, так нові версії існуючого програмного забезпечення та просто нове ПЗ з'являється щомісяця. Зловмисники постійно підвищують рівень своєї кваліфікації. Такий стрімкий розвиток, що збільшує використання Internet для передачі та обробки чутливих даних серед підприємців, недостатній рівень ресурсів для забезпечення належного захисту призводить до того, що організації потребують нових підходів до забезпечення інформаційної безпеки, що дозволяли бі системі захисту «йти в ногу» з неперервними змінами.

Останній описаний підхід є найближчим до ідеального. Проте рівень існуючих вразливостей все ще характеризується досить високими значеннями: від 60 до 40% [10]. Такі вразливості все ще роблять актива високосприйнятливими до атак або некоректного використання. Тому провідні організації, що вимушені забезпечувати безпеку для своїх активів, такі як British Telecom / Syntegra, Центр ведення інформаційної війни ВПС США, DISA і DRA (Великобританія) розробили підхід, що дає можливість не тільки розпізнавати ці 40-60% вразливостей і потенційних атак, але і виявляти зміни в переліку актуальних уразливостей і протиставляти їм відповідні засоби захисту. Компанія Internet Security деталізувала та формалізувала такий підхід і сформувала Модель адаптивного управління безпекою (Adaptive Network Security, ANS) [10].

Зазначений підхід можна описати за допомогою такої формули: Безпека = Аналіз ризику + Політика безпеки + Традиційні засоби захисту + Реалізація контрзаходів + Аудит + Моніторинг + Реагування.

Зменшення кількості інцидентів в інформаційній безпеці потребує адаптивного, високочутливого навіть до незначних на перший погляд змін механізму, що безперервно працюватиме в режимі реального часу.

Вважається, що саме адаптивна безпека – це той підхід, що дає можливість контролювати, аналізувати і реагувати в реальному режимі часу на потенційні ризики безпеки, використовуючи грамотно побудовані і узгоджено керовані процеси і засоби.

В [10] ANS представлено як процес, який містить:

- технологію аналізу захищеності (security assessment) або пошуку вразливостей (vulnerabilities assessment);
- технологію виявлення атак (intrusion detection);
- адаптивний компонент, який включає в себе і розширює дві перші технології;
- керуючий компонент.

Аналіз захищеності - процес пошуку потенційно уразливих, слабких місць в системі. Так, до слабких місць, що виявляються на даному етапі можна віднести: так звані «люки» в системах (back door) і програми типу «троянський кінь»; ненадійні паролі; можливість проведення атак типу «відмова в обслуговуванні»; старі версії без виправлення уразливих місць (patch, hotfix) в операційних системах; неправильна конфігурація міжмережевих екранів, Web-серверів і серверів баз даних і т.д.

Проведення аналізу захищеності є дійсно дієвим методом, що дозволяє контролювати реалізацію узгодженої політики безпеки та отримувати інформацію про слабкі місця перш, ніж здійсниться використання таких вразливостей для реалізації атак.

Виявлення атак - це оцінка дій, які відбуваються в системі та виявлення потенційно підозрілих з них. Даний процес проводиться за допомогою аналізу журналів реєстрації подій операційної системи або аналізу мережевого трафіку в реальному часі.

Компоненти пошуку атак, розміщені на вузлах або в сегментах мережі, контролюють різні дії, в тому числі при цьому використовуються вже відомі уразливості.

Адаптивний компонент ANS відповідає за побудову процесу аналізу захищеності, передаючи для цього актуальну інформацію про нові вразливості. Даний компонент також коригує компонент, відповідальний за виявлення атак, надаючи йому актуальну інформацію про нові атаки. Приклад адаптивного компонента - механізм оновлення баз даних антивірусних програм для виявлення нових вірусів [10].

2.4 Практики застосування адаптивного підходу в інформаційній безпеці

В даний час існує декілька підходів до застосування адаптації у сфері інформаційної безпеки. Дані підходи можна умовно розділити на дві групи. До першої віднесемо підходи, зосереджені на адаптації певного механізму захисту або підтримці заданого рівня для конкретного атрибута безпеки. Друга група об'єднує в собі більш загальні підходи, що підтримують заданий рівень безпеки в цілому, для різних атрибутів та механізмів. Розглянемо більш детально та порівняємо найпопулярніші з цих підходів.

У роботі [11] представлено архітектурний підхід до «самоадаптування» механізмів безпеки за допомогою політики ESCA (події, стан, умова та дії). За даним підходом відокремлюється логіка програми від рівня додатків, а елементи адаптації розташовані на рівні middleware. Крім того, механізми захисту відокремлені від логіки програми до рівня middleware. Автори розробили архітектуру middleware відповідно до моделі Спільного простору даних (Shared Data Space, SDS). Архітектура містить компонент ядра на рівні middleware та проксі-елемент, який обробляє зв'язок між додатком та ядром. Компонент ядра складається з трьох частин, тобто операційної підсистеми, підсистеми безпеки та підсистеми контексту. Операційна підсистема містить функціонал, необхідний

для реалізації моделі SDS, і, таким чином, вона не пов'язана безпосередньо з адаптацією безпеки. Підсистема безпеки, в свою чергу, складається з декількох частин. Перша частина - це керівник політики ESCA. Друга частина підсистеми безпеки - це набір механізмів захисту, які адаптуються на основі обраної політики. Автори згадують механізми аутентифікації, авторизації, шифрування та відмовостійкості. Підхід має бути загальним, і, таким чином, ці механізми не названі більш докладно. Кінцевою підсистемою в компоненті ядра є підсистема контексту, яка містить набір служб для надання контекстної інформації для перших двох підсистем. Автори описують такі контекстні послуги: рівень довіри, рівень загрози, монітор доступності, монітор пам'яті та монітор пропускну здатності.

Серед переваг даного підходу - чітко структурована на виділені підсистеми та компоненти архітектура. Однак поведінка цих підсистем при інтеграції на практиці ще доволі мало досліджена.

В роботі [11] представлено програмну основу для автономної безпеки. Авторами впроваджено термін «цикл адаптації». Даний цикл складається з етапів моніторингу, аналізу та реагування. На програмному рівні кожному етапі відповідає окремий модуль.

Модуль моніторингу відповідає за спостереження за подіями, пов'язаних із безпекою, які називаються контекстом безпеки. Автори наводять приклад переліку подій безпеки, наприклад, доступна нова схема автентифікації, зміна місця розташування користувача, низька рівень доступної пам'яті тощо. Отже, події, що стосуються безпеки, можуть відбуватися в пристрої чи середовищі виконання.

Модулі аналізу отримують та обробляють інформацію про події, розпізнані модулями моніторингу. На основі отриманих подій кожен модуль-аналізатор пропонує високоефективні заходи безпеки для зміни конфігурацій системи.

Реагуючий модуль відповідає за застосування пропонованих аналізаторами заходів безпеки високого рівня конкретними підсистемами, наприклад, підсистеми зв'язку, аутентифікації пристроїв, додатків тощо. В якості прикладу

заходу безпеки автори наводять: "підвищити рівень шифрування", що можна реалізувати шляхом збільшення розміру ключа або проведення додаткових етапів шифрування.

Також окрім зазначених вище модулів в роботі окремо описано модуль підтримки. Модуль підтримки пропонує базу даних профілів для інших модулів. Події модулів моніторингу можуть бути збережені у базі даних профілів для подальшого використання. База даних надає інформацію для аналізуючих модулів для підтримки прийняття рішень. Окрім того, реагуючий модуль зберігає інформацію про поточну конфігурацію в базі даних профілю.

Такий підхід може бути застосовано для адаптації як окремого пристрою, так і всієї мережі. Обидва варіанти адаптації використовують аналогічний цикл адаптації. Однак прикладів використання такого підходу на практиці представлено не було.

В роботі [11] представлено програмне забезпечення GEMOM, орієнтоване на повідомлення, яке використовує парадигму обміну повідомленнями публікації та підписки (publish-subscribe). Метою функцій самовідновлення та адаптації для даного ПЗ є забезпечення оптимального рівня безпеки та безперебійної роботи в умовах зміни середовища та появи загроз. Самовідновлення досягається за допомогою реплікації. У GEMOM передбачено компонент Adaptive Security Manager (ASM), що відповідає за виконання завдань, пов'язаних з адаптацією. Отже, ASM контролює та аналізує безпеку, планує заходи безпеки та виконує їх.

Також передбачається компонент, відповідальний за навчання. Робота даного компоненту відбувається в рамках фази аналізу. На жаль, навчальна частина не описана більш докладно.

У представленому підході моніторинг здійснюється за допомогою виявлення аномалій, моніторингу якості обслуговування та вимірювання рівня безпеки за заданими критеріями.

Важливим аспектом адаптивного підходу є постійна потреба у актуальній та вичерпній інформації. Так, кожен із розглянутих вище підходів передбачає обробку та аналіз наявної інформації як про зовнішнє, так і про внутрішнє

середовище системи. Однак процес отримання та зберігання даної інформації недостатньо освітлено. Так, деякі з підходів передбачають наявність бази даних, що буде застосовуватись на різних етапах адаптації. Однак вміст бази даних не описаний у цих підходах. В роботі [11] є згадування про політику та служби моніторингу. У цьому підході політики описують механізм захисту, який слід використовувати в тій чи іншій ситуації. Крім того, служби моніторингу також виконують етап аналізу, і необхідна інформація інтегрується в ці служби. Таким чином, кожен з підходів передбачає використання інформації. Проте жоден з цих підходів не конкретизує вимоги до оброблюваної інформації.

Висновки до розділу 2

В даному розділі розглянуто адаптивний підхід до управління інформаційною безпекою. В теорії управління поняття управління з адаптацією (адаптивне управління) розглядається як управління в системі з неповною апріорною інформацією про керований процес, яке змінюється в міру накопичення інформації і застосовується з метою поліпшення якості роботи системи.

В даний час існує декілька підходів до застосування адаптації у сфері інформаційної безпеки. Найбільш відомі з них мають такі компоненти: технологію аналізу захищеності (security assessment) або пошуку вразливостей (vulnerabilities assessment); технологію виявлення атак (intrusion detection); адаптивний компонент, який включає в себе і розширює дві перші технології; керуючий компонент. Проте такі підходи не відповідають на одне з найважливіших питань управління інформаційною безпекою – визначення прийнятного рівня інвестицій в побудову системи захисту інформації.

3 МЕТОДИ ВИЗНАЧЕННЯ ПРИЙНЯТНОГО РІВНЯ ІНВЕСТИЦІЙ В СИСТЕМУ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Економіко-вартісні моделі атакуючого

Розглянемо описані в роботах [13, 14] економіко-вартісні моделі атакуючого. Для опису інтегрального ризику використовується наступна формула:

$$R = P_T Q, \quad (3.1)$$

де Q – можливі втрати, а P_T – ймовірність виникнення втрат Q . P_T представлено у наступному вигляді:

$$P_T = P_t P_v, \quad (3.2)$$

P_t - ймовірність мотивованості зловмисника (виникнення зацікавленості в інформаційному ресурсі I організації, що мотивує виконувати будь-які дії зловмисного характеру відносно цього ресурсу), P_v - ймовірність вдалого використання зловмисником для реалізації своїх атакуючих дій вразливостей ІС організації. Структуризація ймовірності P_T зручна тим, що ймовірність мотивації P_t фактично визначається тільки рівнем інтересу атакуючої сторони до інформаційного ресурсу організації, що робить доцільним перебування цієї ймовірності у вигляді окремої експертної оцінки. Один із способів отримання цієї оцінки - застосування евристичної залежності

$$P_i(g, D) = \frac{g - D}{g} = 1 - \frac{D}{g}, \quad (3.3)$$

де g - цінність ресурсу I для зловмисника, D - витрати на підготовку та реалізацію атаки, приведені до грошової форми, $g - D$ - прибуток зловмисника в разі успішності проведеної атаки. Очевидно, що з ростом g , значення ймовірності P_t все більше наближається до 1. І, навпаки, зі зменшенням g , у випадку коли $g \leq D$ реалізація атаки втрачає сенс, окрім випадків, коли зацікавленість

атакуючого виходить за рамки комерційної. Слід також зазначити, дві особливості, важливі для практичного застосування формули (3.2):

1) параметри, що входять у даний вираз, визначаються тільки інтересами і мотивами поведінки зловмисника;

2) сприйняття цінності одного й того ж інформаційного ресурсу атакуючою стороною та стороною захисту в загальному випадку різне - «асиметричне». Наприклад, для власника ресурсу його цінність зазвичай розраховується на основі аналізу вартісних аспектів створення цього ресурсу, процедура розрахунку часто носить збірний характер, одержувані оцінки досить стійкі. Для атакуючої сторони цінність «добутої» інформації формується на основі ринкової вартості ресурсу та кількості потенційних покупців, охочих дістати його в свою власність, в результаті $q \neq g$.

Імовірність успішності реалізації атаки визначається співвідношенням потенціалів сторін атаки та захисту і може бути представлена евристичним співвідношенням виду:

$$P_v(q, c, D) = \frac{\mu q}{\mu q + s \frac{c^2}{D}}, \quad (3.4)$$

де c - загальний обсяг інвестицій в СЗІ організації, $\mu = q/g$ - коефіцієнт асиметрії сприйняття цінності інформаційного ресурсу сторонами, s - коефіцієнт, що відображає рівень зрілості організації та, відповідно, рівень ефективності інвестицій: чим більше значення s , тим нижче, за умовою незмінності рівня інвестицій c , величина ймовірності P_v . Кількісну оцінку рівня зрілості можна отримати застосувавши методику самостійного оцінювання рівня зрілості системи управління ризиками в організації, наведену в [18]. Максимально можливому значенню s відповідає 85 балів, високий рівень зрілості організації характеризується діапазоном 51 - 85 балів. Очевидно, за відсутності інтересу зі сторони зловмисника $g \rightarrow 0$, коефіцієнт $\mu \rightarrow 0$ та, відповідної й імовірності проведення успішної атаки $P_v \rightarrow 0$. Та навпаки, якщо ресурс I не становить

цінності для організації (тобто власника ресурсу), тоді інвестиції в СЗІ практично відсутні, тобто $c = 0$, і тоді ймовірність успішної атаки максимальна $P_v = 0$. Якщо ж атакуючий має надзвичайно високий інтерес до ресурсу I і задля його отримання ладен піти на практично необмежені витрати, тоді $D \rightarrow \infty$, $P_v = 1$.

Підстановка виразів (3.3), (3.4) у формулу (3.2) дає можливість побудувати формалізовану узагальнену модель інтегрального ризику:

$$R(c) = \left(1 - \frac{D}{g}\right) \frac{\mu q}{\mu q + s \frac{c^2}{Dq}}, \quad (3.5)$$

в котру величина c входить як один із параметрів, а потім сформулювати в загальному вигляді залежність запобіглих втрат $\Delta R(c)$ від рівня інвестицій в СЗІ організації.

Для проведення досліджень в рамках аналізу ризиків високого рівня визначаються поняття ефективності СЗІ організації. Вважається, що обов'язковим для ефективної СЗІ є виконання умови $\Delta R(c) > c$. Тоді найбільш ефективною вважається СЗІ, для якої різниця, що представляє «чистий прибуток $\Delta R(c) - c = \Delta C(c)$, обумовлений побудовою СЗІ, виявиться найбільшим. Ефективний обсяг інвестицій в цьому випадку складає [13, 14]:

$$c_{eff} = \arg \max_{c \in C} \Delta_c(c), \quad (3.6)$$

де C – множина значень c , для яких $\Delta R(c) > c$. На жаль, використання узагальненої моделі інтегрального ризику не дозволяє знайти c_{eff} в явному вигляді в аналітичній формі подання. Однак в ряді випадків, застосовуючи більш детальний опис можливостей і характеристик атакуючої сторони, мотиваційно-економічних аспектів її поведінки, виявляється реальним отримання аналітичного рішення оптимізаційної задачі і ряду доповнюючих це рішення відомостей.

Також в роботі [13] описано чотири вербальних специфікації зловмисника, що відображають різні аспекти поведінки і підготовки атакуючої сторони,

соціально-психологічний контекст її дій, існуючі (часто директивно визначаються) цільові установки цих дій, які багато в чому впливають на вибір стратегії атаки, методи і способи реалізації інформаційних загроз. Відповідно введеним специфікаціям формуються рефлексивні (від лат. *Reflexus* - відображення, віддзеркалення) моделі ризиків, кожній з яких властиві певні особливості, які залежать від характеристик зловмисника, що містяться в його специфікації.

Специфікація 1 - скриптікідді (*scriptkiddie, newbies*).

Атакуюча сторона - недосвідчений одинак або група, що не має достатньої підготовки і знань для написання експлойта або складної програми, що використовує для атаки на інформаційні системи і мережі скрипти або програми, вже розроблені іншими, котрий розуміє механізм їх дії, але не здатний до самостійної реалізації ефективних атакуючих рішень, з досить скромними ресурсними можливостями (зокрема фінансовими). Мета дій скриптікідді - спроба справити враження на друзів або отримати похвалу від спільнот комп'ютерних ентузіастів.

За оцінкою А.В.Лукацького [19], скрипт кідді складають до 95% від загального числа зловмисників, атакуючих інформаційні та комп'ютерні системи, тобто це найбільш поширений тип порушника, необхідність захисту від якого є першочерговим завданням при побудові СЗІ. Зокрема, відзначається, що використовувані скрипт кідді «старі» загрози можуть завдати дуже значної шкоди організації, якщо вона не приділяє належної уваги захисту своєї інформації. Крім того, необхідно враховувати, що спільноти скриптікідді досить неоднорідні, і ті з них, хто отримав непогану базову освіту і навчився вчитися, складають резерв для більш просунутих кіберзлочинців.

Таким чином, відносно скрипт кідді справедливими є наступні підсумкові твердження:

- атакуюча активність скрипт кідді не носить цілеспрямований характер, об'єктами їх атак виявляються випадкові комп'ютери, в руки атакуючого потрапляє різнопланова випадкова інформація (хоча іноді і дуже цінна). У зв'язку

з цим формула (3.2) не актуальна для скрипт кідді, його мотивація вкрай нестійка і носить спонтанний характер;

- скрипт кідді не в змозі самостійно розробляти засоби і нові механізми атак, більш того, такі атакуючі часто не розуміють механізму дії вже відомих атак, засновуючи при цьому свої дії головним чином на застосуванні переборного принципу в реалізації загроз. Тому грамотно втілений в СЗІ організації базовий рівень захищеності, орієнтований на застосування засобів і способів захисту від уже відомих «старих» загроз, досить ефективний для протидії атакам скрипт кідді.

Таким висновкам відповідає рефлексивна модель ризику виду:

$$R(C) = P_i \frac{q}{q + sc} q, \quad (3.7)$$

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

$$P_v = \frac{q}{q + sc} \quad (3.8)$$

З (3.8) випливає, що безпека інформації в організації в першу чергу залежить від внутрішніх параметрів: суми інвестицій в СЗІ, рівня зрілості організації (визначається значенням параметра s) і цінності q її інформаційного ресурсу. Зростання значень параметрів c і s веде до падіння значень ймовірності (3.8).

Розрахувавши для рефлексивної моделі ризику (3.8) величину втрат $\Delta R(c)$ та співставляючи їх з обсягом інвестицій в СЗІ знаходиться обсяг «чистого прибутку» організації, обумовленого побудовою СЗІ:

$$\Delta_c(c) = \Delta_R(c) - c = \frac{sc}{q + sc} P_i q - c, \quad (3.9)$$

Аналізуючи вираз (3.9) можна визначити [7] діапазон виправданих (розумних) інвестицій $0 \leq c \leq q(s-1)/s$, в межах якого $\Delta_R(c) > c$, формулу для визначення ефективного (прийнятного) обсягу інвестицій в СЗІ

$$c_{eff} = \frac{q}{s}(\sqrt{P_i s} - 1), \quad (3.10)$$

а також формули для розрахунку значень ймовірності P_v та ризику R_v в умовах ефективного обсягу інвестицій:

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_i s}}, \quad R_T(c_{eff}) = P_v(c_{eff})P_i q = q \sqrt{\frac{P_i}{s}} \quad (3.11)$$

Шляхом аналізу отриманих виразів в [23] отримано, що максимальний ефективний обсяг інвестицій в СЗІ складає $c_{eff \max} = 0,25q$, тобто 25% від вартості ресурсу q , що підлягає захисту, а для вискоефективних захисних рішень (наприклад, $s = 60$) у відповідності з формулою (3.10) навіть при $P_i = 1$ прийнятний обсяг інвестицій складе 11-13% від вартості захищеного ресурсу.

Специфікація 2 - зловмисник-професіонал.

Атакуючу сторону представляє професіонал або група професіоналів, що володіє необхідними знаннями, навичками і достатнім досвідом, для якої хакинг - основна діяльність відверто комерційного характеру. Зловмисник-професіонал зазвичай може користуватися певними фінансово-економічними ресурсами, але для нього, проте, зберігає достатню актуальність обмеження $D \leq g$. Якщо сторони атаки і захисту приблизно однаково оцінюють вартість інформаційного ресурсу, тобто $\mu = 1$, рефлексивна модель ризику для цього випадку має вигляд:

$$R(c) = (1 - \frac{D}{g}) \frac{q}{q + s \frac{c^2}{D}}, \quad (3.12)$$

Дослідження відношення (3.12) для $D = 0$ дозволяє оцінити існуючі граничні значення для діапазону ефективних інвестицій в СЗІ: $0 \leq c \leq q$. Зі збільшенням значень D , при $D \rightarrow 0,25sqP_i^2$, обмеження дуже зближаються, та

сходяться в точку $c = \frac{qP_t}{2}$ для $D = 0,25sqP_t^2$. В даному граничному випадку максимальний рівень ефективних інвестицій в СЗІ складає $c_{eff\ max} = 0,5q$, тобто 50% від вартості ресурсу, що підлягає захисту. Розподіл цього обсягу інвестицій вимагає проведення аналізу можливих загроз безпеки інформації, виділення актуальних загроз з наступною реалізацією системи захисних заходів у формі комплексної системи захисту інформації (КСЗІ) в умовах оптимального розподілу виділених інвестицій.

Як вже зазначалося вище, зловмисники можуть вкласти в організацію і проведення атаки значні кошти, зіставні за величиною зі значеннями вартості самого ресурсу для організації-власника, але, як правило, виділяємий атакуючий потенціал не перевищує меж економічної доцільності. Однак у випадку $\mu \gg 1$, тобто при істотній асиметрії сприйняття цінності інформації сторонами атаки і захисту, виникає ситуація, яку можна визначити як довгострокова (тривала) цільова атака. При цьому атакуюча сторона, попередньо вже виділила на свої дії неабиякі ресурси для підготовки атаки, але ще не досягла успіху, та переходить на вичікувальну тактику, супроводжувану веденням постійного контролю за якістю функціонування СЗІ організації-цілі. Рано чи пізно, при виникненні локального зниження рівня її захищеності (поява навіть короткочасно доступної уразливості), атакуюча сторона проводить успішну атаку. Основним витрачаємим ресурсом зловмисника в цьому випадку є його час та витрати на здійснення моніторингу стану захищеності об'єкта атаки.

З формальної точки зору, якщо $\mu \neq 1$, то при $g \rightarrow \infty$ ймовірність активації загрози $P_t \rightarrow 1$, тобто загроза існує постійно і її реалізація відбудеться як тільки випаде зручний момент. При наявності інсайдера в організації, що підлягає атаці, саме він може повідомити про настання цього моменту, а також сприяти його появі. Цьому моменту буде відповідати локальний сплеск ймовірності, яка, згідно з введеним в [3] визначенням, представляє собою «термінальну» ймовірність, величина якої змінюється в часі відповідно до обраної тактики атак. У свою

чергу, правильний вибір стратегії стороною захисту, - так званий проактивний захист, який ґрунтується на попереджувальних захисних діях, що спираються на вивчення поведінки, тактики і стратегії атакуючої сторони, тобто використання підходів та принципів рефлексивного управління [14, 15] - дозволяє відстрочити настання моменту успішної реалізації загрози теоретично на необмежено довгий період часу.

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 - спрямованих цільових атак АРТ (Advanced Persistent Threat), динамічних технік обходу АЕТс (Advanced Evasion Techniques), проти яких застосовуються сьогодні комплекси захисних заходів малоефективні. Перспективним може виявитися розробка проактивних систем захисту, які використовують підходи і принципи рефлексивного управління.

Специфікація 3 - Професіонал-виконавець.

Атакуюча сторона для досягнення своїх цілей користується послугами найманого виконавця, зобов'язаного за будь-яких обставин виконувати своє завдання. Зокрема, якщо його завдання - реалізація будь-якої загрози, то професіонал-виконавець відразу приступає безпосередньо до пошуку і експлуатації уразливості ІС організації, тобто очевидно, що в цій ситуації $P_i = 1$. При цьому в попередніх специфікаціях атакуюча сторона в своїх діях керується принципом економічної доцільності (розумної достатності). Особливість же Специфікації 3 складається саме в тому, що, в зв'язку з особливою важливістю поставленого перед професіоналом-виконавцем завдання, ресурсні обмеження знімаються і, крім того, він може розраховувати на залучення для підтримки своїх дій різних додаткових ресурсів: фінансових, технічних, інформаційно-аналітичних, оперативних і т.п. На практиці це означає можливість реалізації в рамках специфікації 3 дуже високозатратних атак ($D \rightarrow \infty$). Типовим прикладом подібної ситуації є виконання особливо важливого завдання співробітником

спецслужби, що є професіоналом, підготовленим до здійснення атакуючих дій в кіберпросторі [3, 7].

Рефлексивна модель ризику для цього випадку проста:

$$R(c) = \frac{q}{q + s \frac{c^2}{D}} q, \quad (3.13)$$

Аналізуючи дану модель стає очевидно, що зі зняттям ресурсних обмежень ($D \rightarrow \infty$) ймовірність $P_v \rightarrow 1$, тобто успішна реалізація загрози атакуючої стороною виявляється практично гарантованою і в підсумку $R(c) \rightarrow q$. Це досягається за рахунок здійснення зловмисником нових оригінальних атак, захист від яких в рамках представленої в діючих інструкціях з ризик-менеджменту стандартної методології РОП, що базується на дослідженні і аналізі вже реалізованих раніше інцидентів в сфері безпеки, передбачити практично неможливо.

Специфікація 4 - хактивіст.

Атакуюча сторона - ідейний хакер («кібер-активіст»), прагне перенести в кіберпростір просування політичних або соціальних ідей (нерідко досить сумнівного характеру), що організує акції громадянської «електронної» непокорі 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-хакинг і комп'ютерні зломи, комп'ютерні віруси і черв'яки [14]. В діях хактивіста практично відсутня комерційна складова, його атакуючий потенціал, зокрема, ресурсне забезпечення, зазвичай обмежені, тому Специфікація 4 для хактивіста, в залежності від доступних для нього ресурсів, може бути близька до специфікації 1 або 2. Це дозволяє припускати, особливо при встановленні належності хактивіста до тієї чи іншої протестної спільноти і з огляду на груповий характер

акції, її тип, тривалість, масовість, інтенсивність і можливі наслідки, що застосування РОП в подібних ситуаціях може бути досить ефективним.

Таким чином описане в роботі [13] дослідження рефлексивних моделей ризику, що відображені для ряду типових ситуацій «атака-захист», характерні особливості поведінки і дій атакуючої сторони, представлені в рамках Специфікацій 1, 2, 4 (скрипт кідді, зловмисник-професіонал, хактивістом), дозволяє здійснити аналіз ризиків високого рівня, спрогнозувати оцінки граничного обсягу інвестицій в СЗІ організації, провести пріоритизацію ризиків і виділити групи актуальних інформаційних загроз, забезпечивши тим самим ефективний розподіл коштів, що інвестуються в СЗІ організації.

Аналіз застосування ризик-орієнтованого підходу (РОП) до побудови СЗІ організації з використанням моделі ризиків, яка визначається в рамках специфікації 2 для довгострокових цільових атак, призводить до висновку про неможливість забезпечення достатніх гарантій захисту від ряду атак (зокрема, спрямованих цільових атак АРТ (Advanced Persistent Threat), динамічних технік обходу АЕТс (Advanced Evasion Techniques)), що реалізуються в кіберпросторі.

З огляду на те, що базова методологія РОП, представлена в стандартах ризик-менеджменту інформаційної безпеки, ґрунтується на дослідженні та аналізі вже реалізованих раніше, відомих інцидентів в сфері безпеки, успішне застосування РОП для побудови ефективної СЗІ, що дозволяє відображати нові, непрогнозовані наявною передісторією атаки, не представляється можливим. У зв'язку з цим застосування РОП для побудови СЗІ від атак зловмисників, які потрапляють під Специфікацію 3, є марним.

3.2 Рівні адаптації

Аналіз сформованих рефлексивних моделей дозволяє для кожної відповідної ситуації оцінити необхідний обсяг інвестицій в СЗІ. В залежності від характеристик потенційного атакуючого можна виділити наступні рівні адаптації:

Рівень 1. В ролі атакуючої сторони розглядається «повсякденний хакер» (скриптікідді, scriptkiddie) – одинак з доволі невеликим досвідом проведення атак (або взагалі без досвіду), обмежений у фінансових ресурсах, без достатньої підготовки та знань для написання експлойта або складної програми, який використовує для реалізації атаки на комп'ютерні системи і мережі вже існуючі скрипти або програми, загалом розуміючи механізм їх дії, але не здатний до самостійної реалізації ефективних рішень для здійснення атак. Таким чином, атаками, очікуваними від даного атакуючого, є найбільш популярні і вже відомі атаки. Організаціям, для яких потенційним атакуючим є скриптікідді достатньо реалізувати базовий рівень захисту. До методів, що дозволяють організувати даний рівень захисту можна віднести: аутентифікація, розмежування доступу, використання антивірусного програмного забезпечення, брандмауерів, протоколювання та аудит, реагування на інциденти ІБ і т.д.

Рівень 2. Атакуючу сторону представляє професіонал або група професіоналів, що володіє необхідними знаннями, навичками і достатнім досвідом реалізації атак. Для такого зловмисника хакинг – це основна діяльність, що носить відверто комерційний характер. Атакуючий-професіонал зазвичай у своєму розпорядженні має достатні фінансові ресурси, але для нього, існують певні обмеження, що накладаються можливими наслідками розкриття. Для такого атакуючого, окрім найпопулярніших атак, мають місце соціальна інженерія, фішинг. Як зазначено у роботі [15], людина є найменш надійною ланкою в системі захисту інформації. З усіх відомих вдалих спроб злочинів у сфері комп'ютерної інформації переважна більшість була скоєна за допомогою співників в установі (інсайдерів), або за допомогою недостатньо кваліфікованих в галузі інформаційної безпеки працівників, які не змогли розпізнати загрозу і зловмисника. Наслідками таких злочинів зазвичай є порушення конфіденційності корпоративної інформації фірм, підприємств, установ і закладів. Найчастіше соціальну інженерію надзвичайно недооцінюють в процесі створення організаційних заходів та комплексних систем захисту інформації, а також у процесі самої діяльності організації. На людський чинник звертають

дедалі менше уваги. Тому на данному рівні адаптації важливим аспектом протидії атакуючому, окрім базового рівня захисту, є підвищення рівня обізнаності персоналу у сфері інформаційної безпеки. Також важливим аспектом є побудова проактивного захисту – використання поведікових аналізаторів та блокувачів, що допомагають розпізнати та заблокувати підозрілі дії. Застосування таких технологій потребує грамотного налаштування та вчасного коригування.

Рівень 3. Атакуюча сторона - «Професіонал-виконавець». В такому сценарії для досягнення своїх цілей зловмисник користується послугами найманого виконавця, зобов'язаного за будь-яких обставин виконати свою роботу. Як правило, в попередніх сценаріях для ситуації «атака-захист» сторони в своїх діях керуються принципом економічної доцільності. Особливість професіоналу в тому, що, як правило, у зв'язку з особливою важливістю поставленого перед професіоналом-виконавцем завдання, він може розраховувати на залучення для підтримки своїх дій різні додаткові ресурси: фінансові, технічні, інформаційно-аналітичні, оперативні. На практиці це означає можливість реалізації дуже високозатратних та складних атак. При цьому успішність реалізації загрози атакуючою стороною являється практично гарантованою. Типовим прикладом подібної ситуації є виконання особливо важливого завдання співробітником спецслужби, що є професіоналом, підготовленим до здійснення дій в кіберпросторі [14].

При проведенні цільових атак такі зловмисники часто використовують так звані загрози нульового дня. Тобто віруси або експлойти, що були написані спеціально для атаки на конкретну організацію і ще не потрапили в сигнатурні бази традиційних засобів захисту. Важливою складовою СЗІ на даному рівні можна вважати пісочниці, що дозволяють виявити шкідливі дії в безпечному середовищі, де злочинна програма може намагатися нашкодити наскільки можливо і без будь-якого результату. Пісочниця – ізольоване безпечне середовище, яке імітує операційну систему з усіма її компонентами - драйверами, налаштуваннями, поширеним ПЗ і т. д. У пісочниці можна запускати підозрілі файли і програми, щоб відстежувати їх поведінку і розбиратися в призначенні, не

піддаючи небезпеці мережу організації і кінцеві точки. Таким чином це безумовно важливий елемент в системі інформаційної безпеки кожної організації.

Пісочниці можуть працювати як окреме апаратне рішення, так і в якості віртуального або хмарного сервісу (застосовується і комбінація цих методів). При цьому вважається, що найефективнішим рішенням є саме апаратне забезпечення. Апаратні рішення поставляються і як самостійні засоби, і як частина комплексних продуктів по боротьбі з цільовими атаками та іншими загрозами. Тому для реалізації даного методу захисту (як і на попередньому рівні) важливим є грамотний підхід до обрання та конфігурації пісочниць.

Рівень 4. «Хактивіст» - це ідейний хакер («кібер-активіст»). Головною метою такого зловмисника є просування в кіберпростір політичних або соціальних ідей (нерідко досить сумнівного характеру), що організує акції громадської «електронної» непокори в кіберпросторі, який намагається привернути увагу оточення, влади (іноді в досить жорсткій формі) до тих чи інших питань і проблем сучасного суспільства шляхом синтезу соціальної активності і хакерства. На даному рівні пісочниці можуть виявитися не досить ефективними, адже існують спеціальні “детектори”, що дозволяють виявити пісочниці. Одним із можливих варіантів засобів захисту для даного сценарію можуть стати ловушки та помилкові інформаційні системи. Такі системи імітуючи тематичне наповнення справжніх комп'ютерних систем організації допомагають непомітно для атакуючого виявляти, спостерігати, досліджувати та запобігати спробам реалізації атак. Проте усі зазначені засоби захисту можуть виявитися малоефективними в тому випадку, коли атакуючий реалізовує сучасну складну спрямовану кібератаку (APT).

3.3 Особливості визначення рівня інвестицій в систему захисту інформації

Важливим аспектом в управлінні інформаційною безпекою є визначення необхідного рівня інвестицій в побудову системи захисту інформації (СЗІ). Адаптивний підхід до УІБ, як вже було зазначено вище, дозволяє вирішити цю задачу за допомогою залучення додаткових відомостей про потенційного атакуючого. В якості методу визначення оптимального рівня інвестицій в СЗІ використаємо методи теорій ігор. Так, наприклад, побудуємо та розглянемо дві гри, що будуть відповідати першим двом рівням адаптації: скрипткідді та професіонал.

В даній грі беруть участь два гравця: атакуюча сторона (А) та організація, що захищається (З). Оскільки виграш зловмисника при вдалій спробі реалізації атаки далеко не завжди сумірний з програшем організації в даному сценарії – будемо розглядати гру з ненульовою сумою.

Для кожної із сторін визначимо набір стратегій в грі наступним чином: Стратегії захисту відрізнятимуться сумою інвестицій в побудову СЗІ, що представлена у вигляді відсотку від вартості захищаємого ресурсу. Оскільки інвестування в СЗІ не вважається ефективним при перевищенні вартості самого ресурсу, що захищається, будемо розглядати лише такі стратегії, за яких $c < q$, де c – сума інвестицій в побудову СЗІ у відсотках, q – вартість захищаємого ресурсу. Таким чином, стратегії гравця З (захист) можна представити у вигляді множини: $\{0,05; 0,25; 0,5; 0,75; 0,95\}$.

Стратегії атакуючих будуть відрізнятися витратами атакуючих на реалізацію атаки. За [16] витрати на реалізацію атак для Scriptkiddie та Професіоналу дорівнюють відповідно \$100 і \$1000. Проте в інших джерелах [17] вказуються інакші дані. Так, наприклад, вважається, що Scriptkiddie не вкладає ніяких фінансових капіталів в реалізацію атаки. Тому сформуємо стратегії таким чином: Scriptkiddie $\{0, \$50, \$100\}$ та Професіонал $\{\$500, \$750, \$1000\}$.

Очевидно, що виграш зловмисника в разі вдалої реалізації атаки складатиме різницю між вартістю отриманого в результаті ресурсу та витратами, задіяними на підготовку та реалізацію атаки. Оскільки виграш атакуючого залежить також від його мотивації, задіяних ресурсів та рівня захищеності ресурсу, при розрахунку виграша будемо враховувати ймовірність успішної атаки. Визначимо функцію виграшу для гравця А наступним чином:

$$\pi_A = gP_{\text{усп.}} - D, \quad (3.14)$$

де g – вартість атакуемого ресурсу для злочинника, D – витрати на реалізацію атаки, $P_{\text{усп.}}$ – ймовірність успішної атаки.

Задамо функцію виграшу для грака З наступним чином:

$$\pi_Z = -qP_{\text{усп.}} - c. \quad (3.15)$$

Ймовірність успішної атаки будемо розраховувати за формулами, отриманими в роботі [3]. Відповідно для атакуючого Скрипткідді ймовірність успішної атаки визначатимемо за формулою:

$$P_{\text{усп.}} = \frac{q}{q+sc}, \quad (3.16)$$

де s – рівень зрілості організації. Кількісну оцінку рівня зрілості можна отримати застосувавши методику, наведену в [18]. Для даних розрахунків було використано значення $s \in [20, 60]$.

Ймовірність успішної атаки Професіоналом визначатимемо за допомогою формули [3]:

$$P_{\text{усп.}} = \frac{q}{q+s\frac{c^2}{D}}, \quad (3.17)$$

Розглянемо декілька прикладів побудованих ігор.

Таблиця 3.1 – Результати гри з ненульовою сумою для атакуючого Scriptkiddie при $q = \$1200$

| | <u>Scriptkiddie</u> <u>D = 0</u> | Scriptkiddie D = 50 | Scriptkiddie D = 100 |
|----------------------------------|-------------------------------------|------------------------|-------------------------|
| $c = 0,05 * q$ | -860, <u>800</u> | -860, 750 | -860, 700 |
| <u>$c = 0,25 * q$</u> | <u>-642, 342</u> | <u>-642, 292</u> | <u>-642, 242</u> |
| $c = 0,5 * q$ | -800, <u>200</u> | -800, 150 | -800, 100 |
| $c = 0,75 * q$ | -1041, <u>141</u> | -1041, 91 | -1041, 41 |
| $c = 0,95 * q$ | -1254, <u>114</u> | -1254, 64 | -1254, 14 |

Таблиця 3.2 – Результати гри з ненульовою сумою для атакуючого Професіоналу при $q = \$1200$

| | <u>Професіонал</u> <u>D = 500</u> | Професіонал D = 750 | Професіонал D = 1000 |
|---------------------------------|--------------------------------------|------------------------|-------------------------|
| $c = 0,05 * q$ | -1192, <u>632</u> | -1213, 403 | -1225, 165 |
| $c = 0,25 * q$ | -780, <u>-20</u> | -900, -150 | -985, -314 |
| <u>$c = 0,5 * q$</u> | <u>-771, -328</u> | <u>-840, -510</u> | <u>-900, -700</u> |
| $c = 0,75 * q$ | -982, <u>-417</u> | -1020, -630 | -1054, -845 |
| $c = 0,95 * q$ | -1192, <u>-447</u> | -1217, -672 | -1241, -898 |

Таблиця 3.3 – Результати гри з ненульовою сумою для атакуючого Scriptkiddie при $q = \$1500$

| | <u>Scriptkiddie</u> <u>D = 0</u> | Scriptkiddie D = 50 | Scriptkiddie D = 100 |
|----------------------------------|-------------------------------------|------------------------|-------------------------|
| $c = 0,05 * q$ | -1075, 1000 | -1075, 950 | -1075, 900 |
| <u>$c = 0,25 * q$</u> | <u>-803, 428</u> | <u>-803, 378</u> | <u>-803, 328</u> |
| $c = 0,5 * q$ | -1000, 250 | -1000, 200 | -1000, 150 |
| $c = 0,75 * q$ | -1301, 176 | -1301, 126 | -1301, 76 |
| $c = 0,95 * q$ | -1567, 142 | -1567, 92 | -1567, 42 |

Таблиця 3.4 – Результати гри з ненульовою сумою для атакуючого Професіонал при $q = \$1500$

| | Професіонал D = 500 | <u>Професіонал</u> <u>D = 750</u> | Професіонал D = 1000 |
|---------------------------------|------------------------|--------------------------------------|-------------------------|
| $c = 0,05 * q$ | -1470, <u>895</u> | -1503, 678 | -1520, 445 |
| $c = 0,25 * q$ | <u>-896</u> , -87 | -1041, <u>-83</u> | -1149, -225 |
| <u>$c = 0,5 * q$</u> | -926, -514 | <u>-1000</u> , <u>-500</u> | <u>-1065</u> , -684 |
| $c = 0,75 * q$ | -1208, <u>-562</u> | -1247, -627 | -1283, -841 |
| $c = 0,95 * q$ | -1478, <u>-595</u> | -1503, -671 | -1528, -896 |

Таблиця 3.5 – Результати гри з ненульовою сумою для атакуючого Scriptkiddie при $q = \$1800$

| | <u>Scriptkiddie</u> <u>D = 0</u> | Scriptkiddie D = 50 | Scriptkiddie D = 100 |
|--------------------------------|-------------------------------------|------------------------|-------------------------|
| $c = 0,05*q$ | -1290, 1200 | -1290, 1150 | -1290, 1100 |
| <u>$c = 0,25*q$</u> | <u>-964, 514</u> | <u>-964, 464</u> | <u>-964, 414</u> |
| $c = 0,5*q$ | -1200, 300 | -1200, 250 | -1200, 200 |
| $c = 0,75*q$ | -1561, 211 | -1561, 161 | -1561, 111 |
| $c = 0,95*q$ | -1881, 171 | -1881, 121 | -1881, 71 |

Таблиця 3.6 – Результати гри з ненульовою сумою для атакуючого Професіоналу при $q = \$1800$

| | Професіонал D = 500 | <u>Професіонал</u> <u>D = 750</u> | Професіонал D = 1000 |
|-------------------------------|------------------------|--------------------------------------|-------------------------|
| $c = 0,05*q$ | -1741, <u>1151</u> | -1788, 948 | -1812, 722 |
| $c = 0,25*q$ | <u>-1003, 30</u> | -1170, <u>53</u> | -1297, -152 |
| <u>$c = 0,5*q$</u> | -1080, -392 | <u>-1157, -383</u> | <u>-1227, -672</u> |
| $c = 0,75*q$ | -1434, <u>-415</u> | -1474, -625 | -1511, -838 |
| $c = 0,95*q$ | -1763, <u>-446</u> | -1789, -670 | -1814, -895 |

Для вирішення гри було використано рівновагу Неша. Підкреслено стратегії, що є оптимальними за даною рівновагою. Отже, для потенційного атакуючого Scriptkiddie найбільш оптимальним є обсяг інвестицій до 25% від вартості активів, що підлягають захисту. Для професіоналу необхідний обсяг

інвестицій збільшується – до 50%. Також при проведенні розрахунків було виявлено, що при зростанні рівня зрілості організації до значень 40 балів та вище оптимальний обсяг інвестицій в СЗІ при потенційному атакуючому професіоналу зменшується майже до 25%.

Для отриманих результатів побудуємо гру з природою. Хоча вважається, що у даній грі природа не може виступати в якості зловмисника, проте для організацій, що будують систему захисту зовнішнє середовище (природа) генерує різні за ймовірністю ситуації. Так, наприклад, ситуація, в якій атакуючий – це Скриптікідді, виникає із ймовірністю 70% [20]. Для професіоналу та хактивісту ці ймовірності складають відповідно 29% та 1%. Серед стратегій сторони захисту виділемо найоптимальніші рівні інвестицій, отримані в попередній грі – 25% та 50%.

Таблиця 3.7 – Результати гри з природою ($q = \$1000$)

| | Scriptkiddie | Професіонал | Професіонал-виконавець |
|-------------|--------------|-------------|------------------------|
| $c = 0,25q$ | 536 | 865 | 1249 |
| $c = 0,5q$ | 667 | 786 | 1500 |

Наведені в таблиці 3.7 розрахунки отримано за формулами визначення ризиків в попередньому розділі (3.16), (3.17). Функція виграшу задається наступним чином:

$$\pi_A = qP_{\text{усп.}} + c \quad (3.18)$$

Значення D взято із [16]: для професіоналу \$1000, для професіоналу-виконавця \$100 000.

Для вирішення використаємо критерій Баєса:

$$c = 0,25q : R = 536 \cdot 0,7 + 865 \cdot 0,29 + 1249 \cdot 0,01 = 638.$$

$$c = 0,5q : R = 667 \cdot 0,7 + 786 \cdot 0,29 + 1500 \cdot 0,01 = 709.$$

Отже, для заданих умов оптимальнішою є стратегія при інвестуванні 25% від вартості активу, що підлягає захисту. Проте при зміні вхідних даних про вартість активу, що підлягає захисту оптимальною може виявитися стратегія із меншим обсягом інвестицій, адже це призводить до відповідного зменшення втрат.

Варто зазначити, що такий розподіл імовірностей отримано за статистичними даними, тобто він характеризує загальну ситуацію в даній галузі. Проте для конкретної організації розподіл імовірностей може значно відрізнятись від статистичного. Так, наприклад, при більш імовірних атаках з боку професіоналу та професіоналу-виконавця можливі наступні результати:

$$c = 0,25q : R = 536 \cdot 0,01 + 865 \cdot 0,7 + 1249 \cdot 0,29 = 915.$$

$$c = 0,5q : R = 667 \cdot 0,01 + 786 \cdot 0,7 + 1500 \cdot 0,29 = 881.$$

Для зазначеного розподілу імовірностей найбільш оптимальною є стратегія інвестування 50% від вартості активу, що підлягає захисту. Таким чином, шляхом побудови гри з природою із відповідним розподілом імовірностей реалізації атак з боку потенційних зловмисників для окремої організації може бути визначено прийнятний рівень інвестицій в систему захисту інформації.

Висновки до розділу 3

В даному розділі розглянуто моделі потенційних зловмисників, на основі чого введено поняття «рівень адаптації». Для кожного типу потенційного зловмисника визначається відповідний рівень адаптації, для яких наведено орієнтовний перелік актуальних заходів захисту.

Запропоновано спосіб обчислення прийнятного (ефективного) обсягу інвестицій у СЗІ, структура і функції якої формуються виходячи із принципу адаптивного управління ІБ організації. В залежності від існуючих умов, для захисту від потенційного атакуючого, означеного як Scriptkiddie, найбільш прийнятними є інвестиції у СЗІ в обсязі до 25% від вартості активів, що

підлягають захисту, для професіонала цей обсяг збільшується до 50%. Аналізуючи отримані результати, приходимо до висновку, що, в залежності від цінності інформаційних активів організації, рівня її зрілості, характеристик потенційного атакуючого, можна розрахувати прийнятний обсяг інвестицій в СЗІ для будь-якої організації індивідуально. Отримані розрахунки дають можливість побудувати для організації найбільш ефективну та економічно виправдану стратегію захисту.

4 СТАРТАП-ПРОЕКТ

4.1 Ідея проекту

Таблиця 4.1 – Опис ідеї стартап-проекту

| <i>Зміст ідеї</i> | <i>Напрямки застосування</i> | <i>Вигоди для користувача</i> |
|---|--|--|
| Ідея проекту полягає в розробці десктопного застосунку, основною функцією якого є визначення оптимального рівня інвестиції в побудову системи захисту інформації для організації. | 1. Визначення ефективного рівня інвестицій в побудову СЗІ. | 1. Доступність отриманих результатів. |
| | 2. Аналіз ефективності дійсного рівня інвестицій з отриманням рекомендацій по необхідним коригуванням. | 2. Відсутність необхідності в спеціальних знаннях в теорії ігор. |
| | | 3. Економія часу при визначенні ефективного рівня інвестицій в СЗІ |

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

| № n/ n | Техніко- економічні характерис тики ідеї | (потенційні) товари/концепції конкурентів | | | W (слабка сторона) | N (нейтр альна сторо на) | S (сильна сторона) |
|--------------|--|---|--|---|--|--------------------------------------|---|
| | | Мій проект | РОП | Традиційн ий підхід | | | |
| 1. | Рівень складності проведення оцінки прийнятного рівня інвестицій в СЗІ | Низький, об умовлени й рівнем складності користування застосунком | Високий, обумовлений рівнем складності розрахунку інтегрального ризику | Високий, обумовлений рівнем складності розрахунку вартості повного перекриття | Обмеження закладеними можливостями продукту | - | Доступність |
| 2. | Час затрачений на проведення оцінки | Мінімальний | Максимальний | Максимальний | - | - | Висока швидкість проведення необхідного процесу |
| 3. | Точність отриманих результатів | Середня | Низька | Низька | Точність залежить від вірного визначення моделі потенційного зловмисника | - | Точність вища ніж у конкурентів |
| 4. | Ціна проведення процедури | Середня | Висока | Висока | - | - | Нижча ціна ніж у конкурентів |

4.2 Потенційні техніко-економічні переваги

Таблиця 4.3 – Технологічна здійсненність проекту

| № n/n | Ідея проекту | Технології реалізації | Наявність технологій | Доступність технологій |
|---|---|---------------------------------|-------------------------|---------------------------|
| 1 | Визначення прийняттого рівня інвестицій | Побудова гри з ненульовою сумою | Наявна | Доступна |
| 2 | Автоматизація процесу розрахунків та побудови гри | Мова програмування Java | Наявна | Доступна |
| Обрана технологія реалізації ідеї проекту: Для оцінки обрано метод теорії ігор – гра з ненульовою сумою, для автоматизації процесу – мова програмування Java. | | | | |

4.3 Ринкові можливості запуску стартап-проекту

Таблиця 4.4 – Попередня характеристика потенційного ринку стартап-проекту

| № n/ n | Показники стану ринку (найменування) | Характеристика |
|--------------|--|-----------------------------|
| 1 | Кількість головних гравців, од | 3 |
| 2 | Загальний обсяг продаж, грн/ум.од | - |
| 3 | Динаміка ринку (якісна оцінка) | Зростає |
| 4 | Наявність обмежень для входу (вказати характер обмежень) | Істотні обмеження відсутні |
| 5 | Специфічні вимоги до стандартизації та сертифікації | ISO/IEC 9001, ISO/IEC 27001 |
| 6 | Середня норма рентабельності в галузі (або по ринку), % | - |

За попереднім оцінюванням ринок є привабливим для входження.

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

| <i>№ n/n</i> | <i>Потреба, що формує ринок</i> | <i>Цільова аудиторія (цільові сегменти ринку)</i> | <i>Відмінності у поведінці різних потенційних цільових груп клієнтів</i> | <i>Вимоги споживачів до товару</i> |
|------------------|--|---|---|---|
| 1 | Потреба побудови надійного захисту інформаційних активів організації | Організації, що володіють конфіденційною інформацією | Рівень обізнаності у існуючих вразливостях та рівнях впливу захищеності активів на діяльність усієї організації | - до продукції: точність, конфіденційність введених даних - до компанії-постачальника: вигідна цінова пропозиція, підтримка продукту |

Таблиця 4.6 – Фактори загроз

| <i>№ n/n</i> | <i>Фактор</i> | <i>Зміст загрози</i> | <i>Можлива реакція компанії</i> |
|------------------|--|--|--|
| 1 | Неточність введених даних | Від коректності введених даних залежить точність оцінки | Наведення рекомендацій та правил визначення вхідних даних |
| 2 | Фізична крадіжка машини на якій проводилися обчислення | Крадіжка машини означатиме доступ зловмисника до отриманих оцінок та вхідних даних про організацію | Захист доступу до даних застосунку шляхом встановлення двухфакторної аутентифікації, можливість видалення вхідних та вихідних даних одразу після одержання необхідних результатів (відсутність зберігання даних) |

Таблиця 4.7 – Фактори можливостей

| <i>№ n/n</i> | <i>Фактор</i> | <i>Зміст можливості</i> | <i>Можлива реакція компанії</i> |
|------------------|--------------------------------|--|--|
| 1 | Поширення програмного продукту | Подання рішення на ринок у вигляді готового програмного продукту | Одноразова розробка продукту та підтримка забезпечують однакову кількість витрат на розробку, незалежно від кількості користувачів. Тобто витрати стабільні, дохід - зростає |

Таблиця 4.8 – Ступеневий аналіз конкуренції на ринку

| <i>Особливості конкурентного середовища</i> | <i>В чому проявляється дана характеристика</i> | <i>Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)</i> |
|--|--|---|
| 1. Вказати тип конкуренції - монополія/олігополія/ монополістична/чиста | Чиста | Підтримувати якісний рівень продукції |
| 2. За рівнем конкурентної боротьби - локальний/національний/... | Міжнародний | Унікальність у рішеннях та пропозиціях |
| 3. За галузевою ознакою - міжгалузева/ внутрішньогалузева | Внутрішньогалузева | Підтримувати високий рівень обізнаності в ситуації в галузі, пропонувати більш гнучкі рішення |
| 4. Конкуренція за видами товарів: - товарно-родова - товарно-видова - між бажаннями | - | - |
| 5. За характером конкурентних переваг - цінова / нецінова | Цінова, нецінова | Нижча ціна на проведення процесу оцінки, вища точність результатів |
| 6. За інтенсивністю - марочна/не марочна | Немарочна | - |

Таблиця 4.9 – Аналіз конкуренції в галузі за М. Портером

| | <i>Прямі конкуренти в галузі</i> | <i>Потенційні конкуренти</i> | <i>Постачальники</i> | <i>Клієнти</i> | <i>Товари-замінники</i> |
|-------------------------|--|--|---|--|--|
| <i>Складові аналізу</i> | <i>В даній галузі ринок ще не сформований, прямі конкуренти відсутні</i> | <i>Конкурентами могли б стати продукти, що втілювали б концепції інших підходів до УІБ</i> | <i>Постачальниками є команда розробки застосунку, тому фактори сили полягають у керуванні процесом розробки</i> | <i>Полягають у зацікавленості пропонування можливостей</i> | <i>Товарамі-замінниками можна вважати РОП та традиційний підходи до УІБ</i> |
| Висновки: | Практично відсутня | Можливості входу досить високі Потенційні конкуренти поки не вийшли на ринок | Можливі додаткові стягнення компаніями-розповсюджувачами застосунку | Усі умови обумовлені недостатньою поширеністю знань про адаптивний підхід та відсутністю готовності інвестувати в додаткове програмне забезпечення | Такі підходи є більш поширеними на сьогодні, тому важливою умовою успішного виходу на ринок є достатня поінформованість потенційних споживачів у перевагах пропонованого підходу |

4.4 Фактори конкурентоспроможності

Таблиця 4.10 – Обґрунтування факторів конкурентоспроможності

| № n/n | Фактор конкурентоспроможності | Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим) |
|----------|--|--|
| 1 | Визначення ефективного рівня інвестицій | Наявні підходи до управління інформаційною безпекою не надають можливості оцінки прийнятного рівня інвестицій в СЗІ |
| 2 | Швидкість процедури | Для інших підходів характерна довготривалість проведення оцінки необхідного рівня інвестицій |
| 3 | Рівень трудозатратності | У порівнянні з іншими підходами рівень трудозатратності для адаптивного підходу на порядок менший |
| 4 | Зацікавленість потенційних споживачів | Потенційні споживачі продукції – організації, що будують систему захисту інформації зацікавлені у винайденні нових, більш ефективних підходів |

4.5 Сильні та слабкі сторони стартапу

Таблиця 4.11 – Порівняльний аналіз сильних та слабких сторін «назва проекту»

| № n/ n | Фактор конкурентоспроможності | Бали 1-20 | Рейтинг товарів-конкурентів у порівнянні з ... (назва підприємства) | | | | | | |
|--------------|--|--------------|---|----|----|---|----|----|----|
| | | | -3 | -2 | -1 | 0 | +1 | +2 | +3 |
| 1 | Визначення ефективного рівня інвестицій | 23 | | | | | | | + |
| 2 | Швидкість процедури | 22 | | | | | | + | |
| 3 | Рівень трудозатратності | 22 | | | | | | + | |
| 4 | Зацікавленість потенційних споживачів | 21 | | | | | + | | |

Результативна сума дає можливість зробити висновок про високий рівень конкурентоспроможності товару.

Таблиця 4.12 – SWOT - аналіз стартап-проекту

| | |
|--|--|
| Сильні сторони: Визначення ефективного рівня інвестицій, Швидкість процедури, Рівень трудозатратності, Зацікавленість потенційних споживачів | Слабкі сторони: необхідний час на встановлення на ринку |
| Можливості: Подання рішення на ринок у вигляді готового програмного продукту | Загрози: Неточність введених даних, Фізична крадіжка машини на якій проводилися обчислення |

4.6 Альтернативи ринкової поведінки

Таблиця 4.13 – Альтернативи ринкового впровадження стартап-проекту

| <i>№ п/п</i> | <i>Альтернатива (орієнтовний комплекс заходів) ринкової поведінки</i> | <i>Ймовірність отримання ресурсів</i> | <i>Строки реалізації</i> |
|------------------|---|---|--------------------------|
| 1 | Акцент реалізації маркетингових стратегій на розробці сайту | Висока 80% | Місяць |
| 2 | Знаходження потенційних споживачів на конференціях, ярмарках, воркшопах | Висока 70% | 3 місяці |
| 3 | Орієнтація у реалізації маркетингових стратегій на корпоративні мережі | Середня 50 % | 7 місяців |
| 4 | Рекламні кампанії: листівки, банери, контекста реклама | Нижча середньої 40% | Рік |
| 5 | Виявлення потенційних організацій-споживачів та реалізація націленої реклами | Висока 70% | Пів року |

4.7 Визначення стратегії охоплення ринку

Таблиця 5.1 – Вибір цільових груп потенційних споживачів

| <i>№ n/n</i> | <i>Опис профілю цільової групи потенційних клієнтів</i> | <i>Готовність споживачів сприйняти продукт</i> | <i>Орієнтовний попит в межах цільової групи (сегменту)</i> | <i>Інтенсивність конкуренції в сегменті</i> | <i>Простота входу у сегмент</i> |
|--|---|--|--|---|---|
| 1 | Державні установи | Середня | Невисокий | Невисока | Середня |
| 2 | Приватні невеликі організації | Низька | Низький | Низька | Низька |
| 3 | Середні приватні організації | Висока | Високий | Висока | Висока |
| 4 | Великі приватні організації | Висока | Високий | Висока | Середня |
| 5 | Установи, що володіють державною таємницею | Висока | Висока | Низька | Середня |
| Які цільові групи обрано: За результатами аналізу обрано середні та великі приватні організації | | | | | |

Побудуємо наступну таблицю для визначення найбільш підходящої базової стратегії розвитку

Таблиця 5.2 – Визначення базової стратегії розвитку

| <i>№ п/ п</i> | <i>Обрана альтернатива розвитку проекту</i> | <i>Стратегія охоплення ринку</i> | <i>Ключові конкурентоспромо жні позиції відповідно до обраної альтернативи</i> | <i>Базова стратегія розвитку*</i> |
|-----------------------|---|---|--|---------------------------------------|
| 1 | Акцент реалізації маркетингових стратегій на розробці сайту | Розробка власного сайту, що повно представлятиме усі переваги та можливості використання пропонованого продукту | Доступність для потенційного споживача, легкість сприйняття, повнота передаваної інформації | Стратегія лідерства по витратах |
| 2 | Знаходження потенційних споживачів на конференціях, ярмарках, воркшопах | Пошук потенційних споживачів та ознайомлення їх з пропозицією на тематичних заходах | Висока ймовірність знаходження зацікавлених людей, низький рівень витратності | Стратегія спеціалізації |

4.8 Стратегія конкурентної поведінки

Таблиця 5.3 – Визначення базової стратегії конкурентної поведінки

| <i>№ n/n</i> | <i>Чи є проект «першопрохідцем» на ринку?</i> | <i>Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?</i> | <i>Чи буде компанія копіювати основні характеристики товару конкурента, і які?</i> | <i>Стратегія конкурентної поведінки*</i> |
|------------------|---|---|--|--|
| 1 | Так | Компанія буде і забирати існуючих споживачів у конкурентів і шукати нових споживачів | Ні | Стратегія лідера |

4.9 Стратегія позиціонування

Таблиця 5.4 – Визначення стратегії позиціонування

| <i>№ n/ n</i> | <i>Вимоги до товару цільової аудиторії</i> | <i>Базова стратегія розвитку</i> | <i>Ключові конкурентоспромо жні позиції власного стартап- проекту</i> | <i>Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)</i> |
|-----------------------|--|--|---|---|
| 1 | Точність визначення оцінки | спеціалізація | Точність | Точність, безпека, надійність |
| 2 | Конфіденційність даних | Лідерства по витратах | Конфіденційність | Конфіденційність, надійність, безпечність |
| 3 | Підтримка | спеціалізація | Надійність | Надійність, підтримка |

4.10 Маркетингова концепція товару

Таблиця 5.5 – Визначення ключових переваг концепції потенційного товару

| <i>№ n/n</i> | <i>Потреба</i> | <i>Вигода, яку пропонує товар</i> | <i>Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)</i> |
|------------------|---|---|---|
| 1 | Визначення оцінки інвестицій | Можливість самостійного визначення прийнятного рівня інвестицій в СЗІ | Низька витратність процедури, Низький рівень трудовитрат, точність процедури |
| 2 | Новий підхід до управління інформаційною безпекою | Новий підхід до управління інформаційною безпекою | Низька витратність процедури, Низький рівень трудовитрат, точність процедури |

4.11 Маркетингова модель товару

Таблиця 5.6 – Опис трьох рівнів моделі товару

| <i>Рівні товару</i> | <i>Сутність та складові</i> |
|--|--|
| I. Товар за задумом | Можливість оцінки прийнятного рівня інвестицій в СЗІ |
| II. Товар у реальному виконанні | Властивості/характеристики |
| | 1. Оцінка прийнятного обсягу інвестицій |
| | 2. Аналіз існуючого підходу та рекомендації по його покращенню |
| | Якість: Стандарти ISO/IEC 9001, ISO/IEC 27001 |
| | Пакування: відсутнє оскільки це застосунок |
| III. Товар із підкріпленням | Марка: назва організації-розробника «Adaptive security» + назва товару InvestmentAppraiser |
| | До продажу Надання рекомендацій по зміні рівня інвестицій без оцінки прийнятного рівня |
| | Після продажу Оцінка прийнятного рівня інвестицій |
| За рахунок чого потенційний товар буде захищено від копіювання: Патент | |

4.12 Цінові межі

Таблиця 5.7 – Визначення меж встановлення ціни

| <i>№ п/п</i> | <i>Рівень цін на товари замінни ки</i> | <i>Рівень цін на товари-аналоги</i> | <i>Рівень доходів цільової групи споживачів</i> | <i>Верхня та нижня межі встановлення ціни на товар/послугу</i> |
|------------------|--|---|---|--|
| 1 | - | до 2000 грн. | 3000-8000 грн. | Верхня -2000 грн. ; нижня – 100 грн. |
| 2 | - | 2000-8000 грн. | 8000-10000 грн. | |
| 3 | - | 8000-10000 грн. | 10000-12000 грн. | |
| 4 | - | від 10000 грн. | від 12000 грн. | |

4.13 Оптимальна система збуту

Таблиця 5.8 – Формування системи збуту

| <i>№ п/п</i> | <i>Специфіка закупівельної поведінки цільових клієнтів</i> | <i>Функції збуту, які має виконувати постачальник товару</i> | <i>Глибина каналу збуту</i> | <i>Оптимальна система збуту</i> |
|------------------|--|--|---------------------------------|--|
| | - | Підтримка споживачів, конфіденційність даних | Міжнародна | Розміщення установовчого файлу на сайті організації для скачування |

4.14 Концепція маркетингових комунікацій

Визначимо концепцію маркетингових комунікацій за допомогою побудови наступної таблиці.

Таблиця 5.9 - Концепція маркетингових комунікацій

| <i>№ п/п</i> | <i>Специфіка поведінки цільових клієнтів</i> | <i>Канали комунікацій, якими користуються цільові клієнти</i> | <i>Ключові позиції, обрані для позиціонування</i> | <i>Завдання реklamного повідомлення</i> | <i>Концепція реklamного звернення</i> |
|------------------|---|---|---|--|---|
| | Мінімізація необхідних ресурсів на побудову СЗІ | Інтернет, конференції, соціальні мережі, засоби масової інформації | Точність, доступність, швидкість, конфіденційність | Надання якогого повної інформації про можливості та переваги застосунку | Можливість пробної версії |

Висновки до розділу 4

В межах даного розділу було описано ідею проекту та проаналізовано ситуацію на ринку. Визначено потенційних споживачів пропонованого продукту, його сильні та слабкі сторони. Було описано потреби, що формують ринок, потенційних конкурентів та переваги над ними. Також було визначено основні шляхи задоволення потреб споживачів та альтернативні ринкові поведінки. Аналізуючи отримані результати можна дійти висновку про високу імовірність виходу на ринок та зайняття на ньому успішних позицій.

В розділі також було розглянуто можливі ринкові стратегії для стартапу та обрано найперспективнішу. Було описано стратегії конкурентної поведінки та стратегії позиціонування. На основі отриманих результатів було побудовано маркетингову модель товару, визначено цінові межі, оптимальну систему збуту та концепцію маркетингових комунікацій.

ВИСНОВКИ

Існуючі стандарти у сфері інформаційної безпеки можна розділити на дві групи. Першу започатковано від найстарішого стандарту в галузі інформаційної безпеки - «Помаранчевої книги». Сюди також належать розроблені пізніше «Федеральні критерії», «Канадські критерії», а сучасним представником даної гілки виступають «Загальні критерії оцінки безпеки інформаційних технологій» - ISO/IEC 15408. Ключовою ідеєю стандартів цієї гілки є так званий захист «із повним перекриттям», орієнтація здійснюється на статичні, замкнуті системи, що у загальному випадку характерні для військової сфери та дуже рідко – для комерційної.

До другої ж групи можна віднести документи, що за основу взяли стандарти серії BS 7799 (British Standards) і за своїм змістом інтегруються із стандартами якості менеджменту серії ISO 900X. Саме з даної групи стандартів беруть початок основні принципи управління інформаційною безпекою. Сучасними представниками документів цієї групи є серія стандартів ISO/IEC 2700X. Важливою відмінністю даних стандартів від першої групи є регламентування ризик-орієнтованого підходу до управління інформаційною безпекою (УІБ). Проте застосування даного підходу на практиці викликає певну кількість запитань. Зокрема для великих організацій із складною ієрархічною структурою розрахунок їх інтегральних ризиків являє трудомістку довготривалу процедуру, результати якої виявляються приблизними та неоднозначними. Крім того, вельми суб'єктивним є формування переліку адекватних загроз: перестраховка, намагання не пропустити істотної загрози призводить до невиправданого розширення складу переліку загроз, що у свою чергу тягне за собою надлишкові інвестиції у створення системи захисту інформації (СЗІ).

Це питання є дуже болісним і важливим для комерційних організацій, виникає потреба у перегляді використовуваних підходів до формування базових принципів побудови СЗІ та політик УІБ в цілому, підсиленні в них ваги економічної складової, формування цих політик залежно від потенціалу та

спроможності атакуючої сторони, адаптуючись до особливостей її поведінки, ймовірних намірів та можливостей.

В роботі розглянуто адаптивний підхід до управління інформаційною безпекою. В даний час існує декілька підходів до застосування адаптації у сфері інформаційної безпеки. Найбільш відомі з них мають такі компоненти: технологію аналізу захищеності (security assessment) або пошуку вразливостей (vulnerabilities assessment); технологію виявлення атак (intrusion detection); адаптивний компонент, який включає в себе і розширює дві перші технології; керуючий компонент. Проте такі підходи не відповідають на одне з найважливіших питань управління інформаційною безпекою – визначення прийняттого рівня інвестицій в побудову системи захисту інформації.

В роботі розглянуто моделі потенційних зловмисників, на основі чого введено поняття «рівень адаптації». Для кожного типу потенційного зловмисника визначено відповідний рівень адаптації, для яких наведено орієнтовний перелік актуальних заходів захисту.

Запропоновано спосіб обчислення прийняттого (ефективного) обсягу інвестицій у СЗІ, структура і функції якої формуються виходячи із принципу адаптивного управління ІБ організації. В залежності від існуючих умов, для захисту від потенційного атакуючого, означеного як Scriptkiddie, найбільш прийнятними є інвестиції у СЗІ в обсязі до 25% від вартості активів, що підлягають захисту, для професіонала цей обсяг збільшується до 50%. Аналізуючи отримані результати, приходимо до висновку, що, в залежності від цінності інформаційних активів організації, рівня її зрілості, характеристик потенційного атакуючого, можна розрахувати прийнятний обсяг інвестицій в СЗІ для будь-якої організації індивідуально. Отримані розрахунки дають можливість побудувати для організації найбільш ефективну та економічно виправдану стратегію захисту.

ПЕРЕЛІК ДЖЕРЕЛ, ПОСИЛАНЬ

1. Архипов О.Є., Теплицька Т.П. Еволюція методології захисту інформації на прикладі аналізу стандартів безпеки [Текст] / О.Є. Архипов, Т.П. Теплицька // Матеріали XVI Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених. «Теоретичні і прикладні проблеми фізики, математики та інформатики», т.ІІ (26 – 27 квіт. 2018 р., м. Київ). – К.: КПІ ім.. Ігоря Сікорського, Видавництво «Політехніка», 2018. – 144 с., С. 130-132.
2. Information technology — Security techniques — Information security management systems — Requirements: ISO/IEC 27001:2005. — [Чинний від 15-10-2005]. — Женева: [б.в.], 2005. — 42 с. — (Міжнародні стандарти ISO/IEC).
3. Information technology — Security techniques — Information security risk management: ISO/IEC 27005:2008. — [Чинний від 15-06-2008]. — Женева: [б.в.], 2008. — 64 с. — (Міжнародні стандарти ISO/IEC).
4. econ.wikireading.ru [Електронний ресурс] : [Інтернет-портал]. — Електронні дані. — Режим доступа: <https://econ.wikireading.ru/25702> (дата звернення 14.05.2019). — Риск-ориентированный подход к обеспечению ИБ.
5. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность [Текст] Москва: Компания АйТи; ДМК Пресс, 2004. 47 с.
6. cfin.ru [Електронний ресурс] : [Інтернет-портал]. — Електронні дані. — Режим доступа: <http://www.cfin.ru/finanalysis/risk/stages.shtml> (дата звернення 26.10.2019). — Левченко В.Н. Этапы анализа рисков.
7. technet.microsoft.com [Електронний ресурс] : [Інтернет-портал]. — Електронні дані. — Режим доступа: <http://technet.microsoft.com/ru-ru/security/cc185712.aspx> (дата звернення 18.09.2019). — Средство оценки безопасности Microsoft Security Assessment Tool (MSAT).

8. uio.no [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим
доступа: <https://www.uio.no/studier/emner/matnat/ifi/INF5150/h06/undervisningsmateriale/060930.CORAS-handbook-v1.0.pdf> (дата звернення 16.08.2019). – The CORAS Model-based Method for Security Risk Analysis.
9. Карпов Л. Е., Юдин В. Н. Адаптивное управление по прецедентам, основанное на классификации состояний управляемых объектов. URL: http://citforum.ru/consulting/BI/karpov/#ref_1 (Дата звернення: 20 листопада 2019).
10. compress.ru [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступа: <https://compress.ru/article.aspx?id=11449> (дата звернення 26.10.2019). – Адаптивная безопасность сети.
11. researchgate.net/ [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим
доступа: https://www.researchgate.net/publication/257307356_Comparison_of_Adaptive_Information_Security_Approaches (дата звернення 23.10.2019). – Comparison of Adaptive Information Security Approaches.
12. securelist.ru/ [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим
доступа: <https://securelist.ru/proaktivnaya-zashhita-kak-ona-est/698/#ways> (дата звернення 10.10.2019). – Проактивная защита как она есть.
13. Архипов А.Е. Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации [Текст] // Захист інформації. – 2015. - Том 17, №3. – С.211-218.
14. Архипов А.Е. Экономические аспекты информационной безопасности. [Текст] // Матеріали міжнародної наукової конференції. ISBN 978-617-7273-36-2 – Херсон: Видавництво ПП Вишемирський В.С., ХНТУ, 2016. – 382 с., С.23-25.

15. Саймон В., Митник К. Искусство вторжения [Текст] Москва: ДМК-Пресс, Компания АйТи, 2005. 282 с.
16. Вахний Т. В., Гуц А. К. Теория игр и защита компьютерных систем [Текст] – Омск: Издательство ОмГУ, 2013. – 160 с.
17. Dorothy E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy: Global Problem Solving Information Technology and Tools, 1999. [Electronic resource]. Access mode: <https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/>. (Дата доступу: 29 жовтня 2019).
18. Руководство по управлению рисками безопасности. Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам и Центр Microsoft security center of excellence, [Электронный ресурс]. Режим доступа: <http://infoeto.ru/download/rukovodstvo-po-upravleniyu-riskami-bezopasnosti.doc> (Дата звернення: 28 жовтня 2019).
19. Лукацкий А.В. Обнаружение атак [Текст] – СПб.: БХВ – Петербург, 2003. – 608 с.
20. zapdoc.site / [Электронный ресурс] // : [Интернет-портал]. – Електронні дані. – Режим доступа: <https://zapdoc.site/corporate.html> (дата звернення 12.10.2019). – Угрозы будущего: будьте к ним готовы. Специальный отчет о стратегиях борьбы со сложными угрозами