Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Сінсевича Тараса Миколайовича*

академічної групи *125-18зск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка засобів підвищення ефективності системи захисту інформації провайдера доступу до мережі Інтернет*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Сінсевичу Тарасу Миколайовичу*** **академічної групи** ***125-18зск-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка засобів підвищення ефективності системи захисту інформації провайдера доступу до мережі Інтернет***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз основних методик оцінки ефективності СЗІ та загроз безпеки інформаційним ресурсам провайдера.	29.03.2021
Розділ 2	Аналіз механізмів захисту, які можуть використовуватися провайдерами. Розробка методика оцінки ефективності СЗІ та визначені вихідні дані для розрахунків за даною методикою. Розробка рекомендації щодо вибору ефективної СЗІ для провайдера доступу до мережі Інтернет.	24.05.2021
Розділ 3	Привести розрахунки збитків від реалізації загроз	14.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2021р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатка, __ джерел.

Об'єкт дослідження: методи оцінки ефективності системи захисту інформації провайдера доступу до мережі Інтернет.

Мета роботи: підвищення рівня безпеки ІС провайдера за рахунок застосування результатів оцінки ефективності СЗІ.

У розділі «Стан питання. Постановка задачі» проведено аналіз основних методик оцінки ефективності СЗІ та загроз безпеки інформаційним ресурсам провайдера.

У спеціальній частині був здійснений аналіз механізмів захисту, які можуть використовуватися провайдерами. Розроблена методика оцінки ефективності СЗІ та визначені вихідні дані для розрахунків за даною методикою. Розроблені рекомендації щодо вибору ефективної СЗІ для провайдера доступу до мережі Інтернет.

В економічному розділі приведені розрахунки збитків від реалізації загроз.

Новизна роботи полягає в удосконаленні методики оцінки СЗІ для провайдера.

Практична цінність роботи полягає у підвищенні рівня захищеності ІС провайдера за рахунок вибору СЗІ з найвищим коефіцієнтом ефективності шляхом застосування запропонованої методики.

КОЕФІЦІЄНТ ЕФЕКТИВНОСТІ, МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ СЗІ, ІНФОРМАЦІЙНА СИСТЕМА ПРОВАЙДЕРА, МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., _ приложений, __ источников.

Объект исследования: методы оценки эффективности системы защиты информации провайдера доступа в Интернет.

Цель работы: повышение уровня безопасности ИС провайдера за счет применения результатов оценки эффективности СЗИ.

В разделе «Состояние вопроса. Постановка задачи» проведен анализ основных методик оценки эффективности СЗИ и угроз безопасности информационным ресурсам провайдера.

В специальной части был осуществлен анализ механизмов защиты, которые могут использоваться провайдерами. Разработана методика оценки эффективности СЗИ и определены исходные данные для расчетов по данной методике. Разработаны рекомендации по выбору эффективной СЗИ для провайдера доступа к сети Интернет.

В экономическом разделе приведены расчеты ущерба от реализации угроз.

Новизна работы заключается в разработке методики оценки СЗИ для провайдера.

Практическая ценность работы заключается в повышении уровня защищенности ИС провайдера за счет выбора СЗИ с наивысшим коэффициентом эффективности путем применения предложенной методики.

КОЭФФИЦИЕНТ ЭФФЕКТИВНОСТИ, МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СЗИ, ИНФОРМАЦИОННАЯ СИСТЕМА ПРОВАЙДЕРА, МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ.

THE ABSTRACT

The explanatory note: ___ c., __ fig., __ table, _ additions, __ sources.

Object of research: The methods for evaluating the effectiveness of the protection provider of Internet access.

The purpose of degree project: improving the safety IS provider through the use of methods of evaluating the effectiveness of ISS.

In the «State of the question. Problems» analysis of existing security threats information resource provider, methods evaluation ISS.

In the special part was the analysis of mechanisms of protection that can be used by providers. The method evaluation and ISS source data for the calculations by this method. The calculation of performance indicators ISS according to the proposed methodology and recommendations for choosing an effective ISS.

In the economic section are estimates of losses from the sale of threats.

The scientific novelty of degree project is to develop methods of assessment for ISS provider.

The practical value of degree project is to raise the level of protection IS provider by selecting a ISS with the highest coefficient of efficiency by applying the proposed method.

EFFECTIVENESS RATIO, EFFECTIVENESS EVALUATION METHODOLOGY ISS, INFORMATION SYSTEM PROVIDERS, SECURITY MECHANISM.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

DoS – атака типу «відмова в обслуговуванні» (denial of service);

IDS – система виявлення вторгнень (Intrusion Detection System);

IP – інтернет протокол (Internet Protocol);

TCO – сукупна вартість володіння (Total cost of ownership);

TCP – протокол управління передачею (Transmission Control Protocol);

VPN – приватна віртуальна мережа (Virtual Private Network);

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІТ – інформаційні технології;

МЕ – мережевий екран;

ОС – обчислювальна система;

ПЗ – програмне забезпечення;

ПЕОМ – персональна електронно-обчислювальна машина;

ПК – персональний комп'ютер;

РС – робоча станція;

СЗІ – система захисту інформації.

ЗМІСТ

ВСТУП

Зараз Інтернетом користується майже кожна організація. При цьому за його допомогою компанія здійснює різноманітні операції та розміщує інформацію на своєму сайті, що дозволяє її клієнтам більш детальніше ознайомлюватися з умовами надання послуг, які пропонує компанія. Успішне та своєчасне здійснення операцій та забезпечення доступності та цілісності інформації визначає ефективне функціонування організації. Крім того необхідно, щоб під час обміну даними між організаціями існували процедури перевірки справжності відправника інформації і отримувача інформації. Забезпечення здійснення операцій такого роду можливе тільки завдяки наданню провайдерами Інтернет-послуг для організацій, які є клієнтами цих провайдерів. При цьому до останніх висувається ряд вимог з боку клієнтів та держави згідно нормативних документів.

Дотримуючись вимог щодо організації своєї діяльності, провайдери телекомунікацій повинні встановлювати не тільки комунікаційні засоби, але і технічні апаратні та програмні засоби, які забезпечують захист інформації під час її передачі каналом зв'язку. Також вони повинні отримати ліцензію на здійснення своєї діяльності, що забезпечує юридичні основи для надання Інтернет послуг.

При наданні послуг доступу до мережі Інтернет існує ряд загроз, які потрібно нейтралізувати. Зменшення впливу загроз можливе за рахунок створення системи захисту інформації.

До складу системи захисту інформації входять різні технічні засоби. Для того, щоб визначити, які технічні засоби та заходи захисту потрібно використовувати, проводиться оцінка ефективності нейтралізації даними засобами можливих загроз інформаційним ресурсам провайдера.

А постійна зміна загроз та відсутність єдиного підходу до оцінки ефективності системи захисту інформації роблять дану задачу необхідною та актуальною.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальна характеристика об’єкту досліджень-провайдера

Перш ніж працювати в Інтернеті, кожен вирішує питання, навіщо це потрібно. Звичайно, що цілі організацій та приватних користувачів переважно не співпадають, хоча і можуть мати спільні риси. Компанії намагаються організовувати власну рекламу в мережі, представити інформацію про себе та власну продукцію, знайти партнерів, запропонувати послуги тощо. Приватні особи хочуть мати свою візитну карточку, знайти друзів, познайомитись, знайти потрібну тематичну інформацію.

Зазначені потреби Інтернет-провайдери пропонують реалізувати клієнтам наступними способами: з наданням чи без надання онлайнових послуг по доступу до мережі, зі створенням поштової скриньки клієнта, зберіганням файлової інформації клієнта з метою доступу до неї через мережу Інтернет, розміщенням інформації клієнта в мережі. Остання послуга є найбільш популярною та оптимальною: клієнт стає повноправним членом мережі, і активно може проводити власну політику по залученню ділових партнерів, пошуку контактів тощо.

1.1.1 Визначення типу, до якого відноситься даний провайдер та особливості його діяльності

Відповідно до того, які функції виконують організації в сфері телекомунікаційних послуг, існують оператори і провайдери телекомунікацій.

В Законі України «Про телекомунцікації» приводяться наступні визначення оператора і провайдера телекомунікацій:

– оператор телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж;

– провайдер телекомунікацій - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне

обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку;

– провайдер доступу до Інтернет - суб'єкт господарської діяльності, який надає послуги доступу до Інтернет третім особам, не здійснюючи при цьому технічне обслуговування та експлуатацію мереж доступу до Інтернет телекомунікаційних мереж за винятком технічних засобів телекомунікацій, які визначені технічними умовами підключення провайдера до мережі оператора телекомунікацій.

В подальшому будемо розглядати суб'єкт господарської діяльності, який виступає в ролі провайдера доступу до мережі Інтернет та використовує телекомунікаційну мережу оператора, побудовану на основі кабельного з'єднання обладнання.

Даний провайдер надає послуги доступу до мережі Інтернет третім особам (надалі клієнтам). Він підписує з оператором телекомунікацій договір, на основі якого оператор телекомунікацій надає в оренду провайдеру доступу до мережі Інтернет власну телекомунікаційну мережу. Технічне обслуговування та експлуатацію мережі за цим договором здійснює оператор телекомунікацій, який має відповідну ліцензію на провадження даного виду діяльності. Оператор також здійснює встановлення клієнтського обладнання та його підключення до телекомунікаційної мережі, а також приймає претензії від клієнтів, які пов'язані із проблемами обслуговування телекомунікаційної мережі.

Технічне обслуговування включає в себе:

1) вимірювання та тестування абонентських ліній;
2) вимірювання та тестування з'єднувальних ліній та каналів;
3) діагностику та усунення пошкоджень;
4) обслуговування та профілактику апаратних засобів;
5) ведення документації про аварійні стани;
6) забезпечення надійного функціонування програмного забезпечення;
7) ведення баз даних.

Оператор телекомунікацій здійснює встановлення в межах своєї телекомунікаційної мережі автоматизованої системи розрахунків за послуги доступу до мережі Інтернет (білінгової системи) та створює умови для підключення провайдера доступу до власної телекомунікаційної мережі.

Провайдер доступу до мережі Інтернет, відповідно до умов договору, повинен видавати клієнту логіни, паролі (ідентифікатори користувача мережею) для доступу до мережі Інтернет. Також провайдер забезпечує захист інформації, що зберігається на сервері від загроз, що реалізуються зловмисником.

Відповідно до вимог, що зазначені в законах України у сфері телекомунікацій, провайдери доступу до мережі Інтернет повинні здійснювати технічне обслуговування обладнання, яким вони підключаються до телекомунікаційної мережі оператора телекомунікацій. До такого обладнання можна віднести сервер та центральний мережевий комутатор (свіч) , який ще називають агрегацією (технологією об'єднання декількох каналів передачі даних).

Провайдер доступу до мережі Інтернет повинен також оброблювати претензії, що надходять від клієнта та пов'язані із проблемами налаштування комп'ютера клієнта для доступу до мережі Інтернет.

Якщо клієнтом провайдера доступу до мережі Інтернет є державний орган, що оброблює інформацію, що є власністю держави, або інформацію з обмеженим доступом, вимоги щодо захисту якої встановлені чинним законодавством, то дані провайдери повинні додержуватись вимог Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

Провайдери доступу до мережі Інтернет повинні забороняти клієнтам, що є студентами або учнями доступ до інформаційних ресурсів аморального та протиправного характеру.

Даний провайдер отримує доступ до мережі Інтернет на основі договору, який він підписує із верхнім провайдером, та зобов'язується дотримуватись вимог, зазначених в даному договорі.

Підсумовуючи вищесказане, можна визначити ряд послуг, що надає провайдер доступу до мережі Інтернет.

1.1.2 Перелік послуг, що надає провайдер доступу до мережі Інтернет, та його організаційна структура

Провайдер доступу до мережі Інтернет надає наступні послуги:

1) надає кожному своєму клієнту ідентифікатори для підключення робочої станції до мережі на снові договору, який укладений між провайдером та клієнтом;

2) оброблює претензії, що надходять від клієнта щодо проблем використання логіна та пароля та усуває причину проблем;

3) здійснює технічне обслуговування обладнання, за допомогою якого провайдер доступу підключається до мережі оператора телекомунікацій;

4) забезпечує захист інформації, що розміщується на сервері;

5) контролює виконання клієнтами вимог, що зазначені в договорі на підключення клієнта до мережі Інтернет.

Всі перелічені вище послуги відносяться до основних телекомунікаційних послуг (основна телекомунікаційна послуга - послуга, що надається споживачу для задоволення його потреби при обміні інформацією з іншими споживачами або пунктами надання послуг), забезпечення яких потребує наявності певного обладнання та відповідних технічних потужностей.

Підключення до Інтернету може бути двох видів:

1) режим он-лайн, коли відповідь на ваш запит відправляється відразу. Так працюють з Web-серверами;

2) режим офф-лайн, коли запит клієнта буде очікувати деякий час на відповідь. Таким чином функціонує багато систем електронної пошти.

Клієнти можуть бути підключені по комутованій лінії (тобто звичайними телефонними лініями), коли для того, щоб одержати доступ до провайдера, доводиться дзвонити до нього звичайним способом. Такий спосіб з'єднання

називають dial up. Але ви також можете орендувати (придбати) і виділену лінію. В цьому випадку ви будете з'єднані з провайдером постійно.

Інформація може бути розміщена в Інтернеті трьома способами. Клієнт орендує простір на сервері провайдера, організовуючи таким чином свої сторінки в Інтернеті. Другим способом є досить розповсюджені віртуальні магазини, що представляють собою інтерактивні каталоги з великими об'ємами інформації про товари та послуги різних фірм. Третій спосіб є найбільш солідним і, відповідно, не самим дешевим: провайдер організовує для клієнта власний віртуальний сервер з унікальним іменем (що є ідентичним з іменем приватної особи або назвою організації). Також доцільно згадати про четвертий спосіб активної участі в розвитку мережі Інтернет - власний Web-вузол, але ця можливість сьогодні поза рамками фінансових можливостей багатьох користувачів.

Для надавання послуг доступу до Інтернету провайдеру потрібно співпрацювати з іншими організаціями.

Організації, з якими співпрацює даний провайдер:

1) Національна комісія з питань регулювання зв'язку - орган виконавчої влади, що здійснює регулювання у сфері телекомунікацій. Цей орган регламентує діяльність даного провайдера;

2) інші оператори телекомунікацій, які здійснюють технічне обслуговування деяких частин телекомунікаційної мережі даного провайдера, а також укладають договори з провайдером на отримання каналу електрозв'язку в оренду та на надання дозволу на експлуатацію власної телекомунікаційної мережі провайдером;

3) проектні відділи будівельних компаній, який надає дозвіл на реалізацію будівельних проектів, що дає змогу провайдеру прокласти провід, який буде з'єднувати його обладнання між собою;

4) інші організації, які виступають в ролі клієнтів даного провайдера.

Забезпечення послуг також неможливе без співробітників та клієнтів даного суб'єкту господарської діяльності.

Серед співробітників даного провайдера можна виділити наступних:

1) директор – особа, що керує даним суб'єктом господарської діяльності;

2) бухгалтер – особа, що здійснює фінансові операції та веде бухгалтерський облік;

3) водій;

4) охоронець;

5) монтажники – співробітники даного підприємства, які здійснюють встановлення та налаштування обладнання, яким провайдер підключається до телекомунікаційної мережі оператора;

6) системний адміністратор – особа, що здійснює технічне обслуговування систем обробки інформації;

7) секретар – особа, що приймає заяви від клієнтів на підключення до Інтернету та передає їх керівництву організації;

8) обслуговуючий персонал, який оброблює інформацію щодо претензії, що надходить від клієнта;

9) юрист – особа, що перевіряє правильність оформлення договору на підключення клієнта до мережі Інтернет.

Для надання послуг доступу до мережі Інтернет провайдер використовує певне обладнання. До обладнання, яке є власністю та обслуговується провайдером доступу до мережі Інтернет, відноситься:

1) сервер, на якому знаходиться база даних клієнтів з переліком ідентифікаторів доступу до мережі;

2) центральний мережевий комутатор;

3) робочі станції співробітників провайдера.

Технічні ресурси, які входять до телекомунікаційної мережі оператора, є власністю та обслуговуються оператором телекомунікацій.

На сервері розміщуються інформаційні ресурси, які потрібно захищати.

1.1.3 Інвентаризація інформаційних ресурсів провайдера та побудова схеми інформаційних потоків

Визначимо інформаційні ресурси провайдера, якими він володіє та до яких він має доступ.

Серед інформаційних ресурсів можна виділити наступні:

1) накази, статути, ліцензії, службові записки та самі документи, що знаходяться в друкованому вигляді в кабінеті директора.

2) трудові договори, що знаходиться в електронному та друкованому вигляді в кабінеті у юриста;

3) інформація про заяви від клієнтів та самі заяви, що знаходяться в електронному вигляді в кабінеті у секретаря провайдера;

4) електронна база даних клієнтів, що знаходиться на сервері та включає в себе імена, паролі користувачів, IP-адреси комп'ютерів, MAC-адреси модемів, адреси проживання, швидкість, з якою користувач може передавати дані через Інтернет, мітки Онлайн, які визначають, чи має клієнт доступ до Інтернету та чи підключений комп'ютер до мережі та ін.;

5) інформація про статистику перебоїв та атак на мережу, знаходиться в електронному вигляді на робочій станції системного адміністратора та на персональному комп'ютері обслуговуючого персоналу, доступ до неї має тільки адміністратор та обслуговуючий персонал;

6) інформація про фінансові операції, що пов'язані із нарахуванням заробітної плати співробітникам провайдера та оплатою послуг доступу до мережі Інтернет, знаходиться в електронному вигляді на персональному комп'ютері бухгалтера та сервері. Доступ до неї має бухгалтер, а доступ тільки до інформації, що пов'язана з оплатою послуг, має системний адміністратор;

7) інформація про особистий кабінет – інформація, що доступна для кожного клієнта та включає в себе дані про залишок коштів на рахунку та швидкість обробки та передачі даних через Інтернет. Для входу в особистий кабінет необхідно ввести свій логін та пароль;

8) договір на підключення клієнта до мережі Інтернет, знаходиться в друкованому вигляді в кабінеті у директора організації. Правильність оформлення цього договору перевіряється юристом при його укладанні та передається керівництву організації;

9) персональні дані клієнтів вказуються в договорі на підключення клієнта до мережі Інтернет та знаходяться в електронному вигляді на сервері провайдера;

10) інформація про верхнього провайдера, який надає доступ даному провайдеру до мережі Інтернет, знаходиться в електронному вигляді на сервері провайдера. Частина цих даних (ПІБ, телефон, адреса), які необхідні для усунення проблем доступу до мережі даного провайдера, використовується системним адміністратором;

11) інформація про оператора телекомунікацій, який надає в оренду провайдеру доступу до мережі Інтернет свою телекомунікаційну мережу та здійснює її технічне обслуговування. Відповідні дані знаходяться в електронному вигляді на сервері. Частина цих даних (ПІБ, телефон, адреса), які необхідні для усунення проблем технічного обслуговування телекомунікаційної мережі, використовується обслуговуючим персоналом;

12) інформація, пов'язана із діяльністю клієнтів даного провайдера та має ознайомчий характер. Знаходиться в електронного вигляді на сервері провайдера.

Аналізуючи вищенаведену інформацію, можна визначити інформаційні потоки, які дозволять нам детальніше розглянути які співробітники до якої інформації мають доступ.

Таблиця 1.1 – Інформаційні потоки провайдера доступу до мережі Інтернет

Інформація	Режим доступу	Властивості інформації, що забезпечуються	Хто має доступ
1	2	3	4
Накази, службові записки, звіти по заходам (знаходиться в кабінеті директора та у друкованому вигляді)	З обмеженим доступом	Конфіденційність, цілісність, доступність	Директор, системний адміністратор.

Продовження таблиці 1.1

1	2	3	4
Заяви від клієнтів на підключення до мережі Інтернет	Відкрита для співробітників провайдера	Цілісність	Працівники провайдера
Інформація про статистику перебоїв та атак на мережу	З обмеженим доступом	Конфіденційність	Системний адміністратор та обслуговуючий персонал
Інформація про фінансові розрахунки	З обмеженим доступом	Конфіденційність, цілісність	Директор, бухгалтери.
Інформація про особистий кабінет	Відкрита для клієнтів	Доступність	Тільки клієнт до свого особистого кабінету
Договір на підключення клієнта до мережі Інтернет	З обмеженим доступом	Конфіденційність, цілісність	Юрист, директор
Інформація про працівників і клієнтів	З обмеженим доступом	Конфіденційність, цілісність	Директор, системний адміністратор, юрист при підписанні договору
Електронна база даних клієнтів	З обмеженим доступом	Конфіденційність, цілісність	Системний адміністратор
Інформація про верхнього провайдера	З обмеженим доступом	Конфіденційність	Системний адміністратор
Дані про оператора телекомунікацій	З обмеженим доступом	Конфіденційність	Обслуговуючий персонал
Інформація, пов’язана з діяльністю клієнтів та має ознайомчий характер	Відкрита для клієнтів	Доступність	Всі клієнти та співробітники
Статутні документи підприємства, ліцензії (знаходиться в кабінеті директора та у друкованому вигляді)	Відкрита для робітників та клієнтів	Цілісність, доступність	Весь персонал та клієнти
Трудові договори	Відкрита для робітників	Цілісність, доступність	Весь персонал

Після того, як визначили, які інформаційні ресурси циркулюють в провайдера доступу до мережі Інтернет, можна побудувати моделі інформаційних

потоків. Розглянемо декілька інформаційних процесів, які характерні для провайдера доступу до мережі Інтернет.

Одним із перших процесів, які будуть розглядатися в даній роботі, буде процес приймання та обробки заяви клієнта на підключення до мережі Інтернет, який зображений на рисунку 1.1.

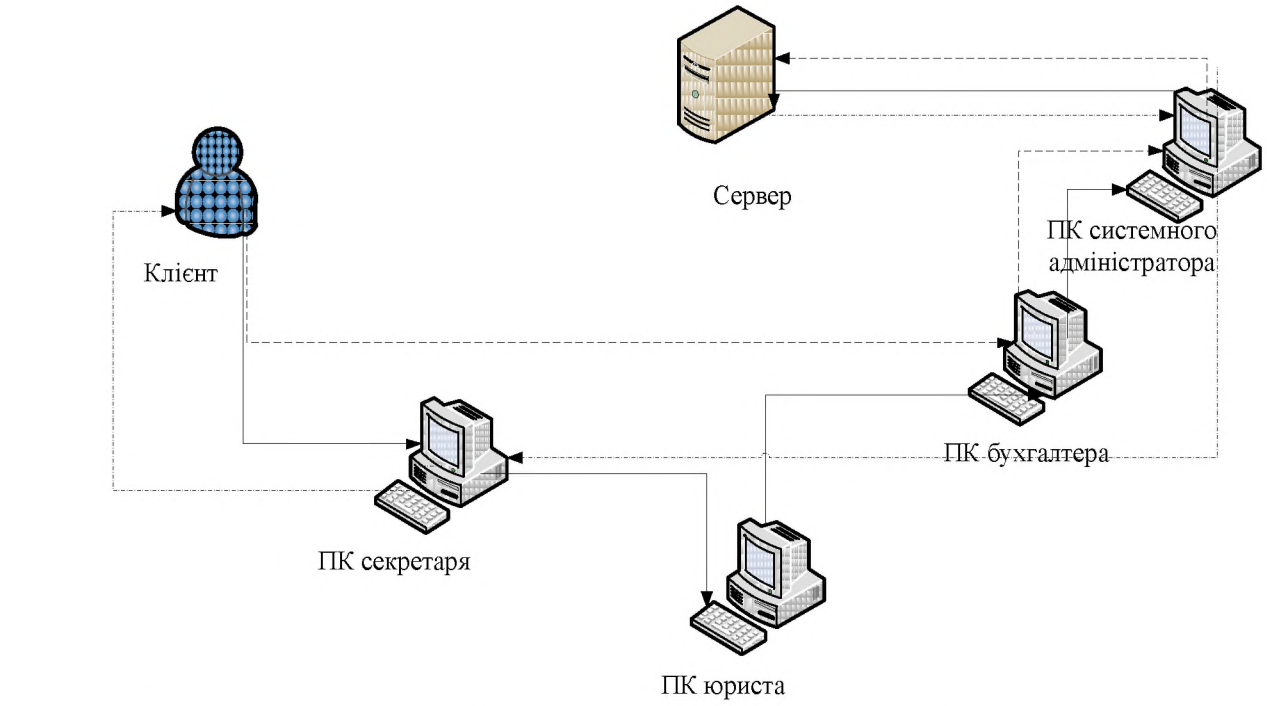

Рисунок 1.1 - Інформаційний процес приймання та обробки заяви клієнта на підключення до мережі Інтернет

Відповідно до рисунку 1.1, клієнт заповнює заяву на підключення до мережі Інтернет, в якій він вказує свої прізвище, ім’я та по-батькові, номер телефону, вибраний тарифний план, адресу проживання. Вид тарифного плану визначається двома способами: в залежності від об’єму трафіку та від швидкості передачі даних. Далі заяву від клієнта приймає секретар, який перевіряє правильність її

оформлення та передає дані про клієнта юристу. Юрист, в свою чергу, перевіряє отриману інформацію та укладає з клієнтом договір на отримання послуги доступу до мережі Інтернет, проставляє номер договору та передає дані про клієнта бухгалтеру. Бухгалтер вносить суму коштів, яка визначається відповідно до тарифного плану, проставляє дату оплати послуг та передає дані про клієнта системному адміністратору. Адміністратор на основі даних про клієнта та про умови оплати послуг доступу до мережі Інтернет, робить запит до сервера на створення в базі даних нового облікового запису користувача, що містить логін, IP-адрес та пароль клієнта. Потім він відправляє ці дані секретарю, який, в свою чергу, видає їх клієнту. А щоб користуватися мережею Інтернет, клієнт повинен здійснити налаштування мережі в себе на комп'ютері. В разі виникнення проблем із налаштуванням, він може зателефонувати обслуговуючому персоналу провайдера.

Здійснення підключення співробітників провайдера до мережі Інтернет здійснюється за рахунок створення в базі даних на сервері облікового запису для конкретного співробітника. Після чого системний адміністратор видає логін, пароль кожному користувачу мережею окремо та налаштовує на персональному комп'ютері підключення до мережі Інтернет.

Далі розглянемо процес здійснення оплати послуг доступу до мережі Інтернет.

Для того, щоб клієнту здійснити оплату послуг, що надаються даним провайдером, необхідно придбати картку поповнення, потім зайти на сайт провайдера та ввести номер картки, логін та пароль. Всі введені дані передаються на робочу станцію системного адміністратора. Системний адміністратор, в свою чергу, перевіряє правильність вводу даних та відправляє запит на сервер на внесення даних про оплату послуги відповідним користувачем. Якщо введена інформація та інформація, що міститься на сервері, збігаються, то на рахунок клієнта нараховуються кошти і він отримує можливість користуватися мережею

Інтернет. Визначимо також, як здійснюється обробка претензій, які надходять від клієнта. Процес обробки претензій зображений на рисунку1.2

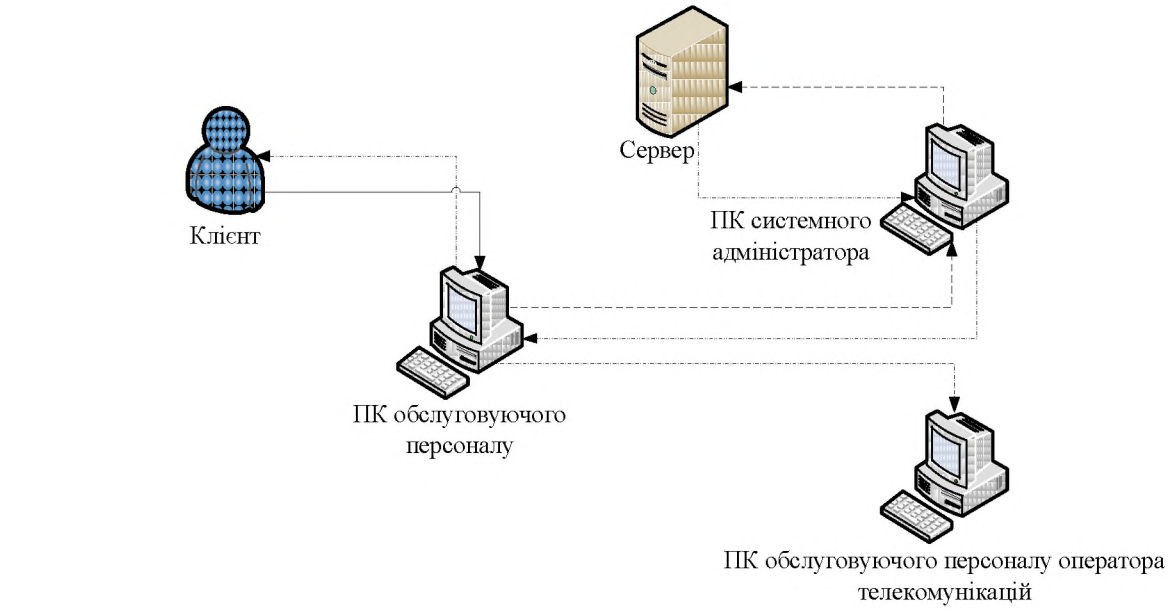

Рисунок 1.2 - Інформаційний процес обробки претензій, що надходять від клієнта

Відповідно до рисунку 1.2, від клієнта на робочу станцію обслуговуючого персоналу провайдера доступу до мережі Інтернет надходить інформація щодо претензії, пов’язаної із проблемами надання доступу до мережі та ідентифікаторів користувача мережею. Обслуговуючий персонал, в свою чергу, оброблює отриману інформацію та вирішує, з якими проблемами пов’язана дана претензія. Якщо претензія пов’язана із проблемами технічного обслуговування мережі, то даний персонал відправляє дані щодо відповідного клієнта та існуючої проблеми на робочу станцію обслуговуючого персоналу оператора телекомунікацій. Якщо ж претензія пов’язана із проблемами налаштування доступу персонального комп’ютера клієнта до мережі Інтернет, тоді

обслуговуючий персонал відправляє дані про клієнта та існуючу проблему на робочу станцію системного адміністратора. Останній робить запит до сервера на встановлення відповідності між даними, отриманими від клієнта, та даними, що зберігаються в базі даних на сервері, аналізує наявність доступу комп'ютера клієнта до мережі Інтернет, встановлює причину виникнення існуючої проблеми та приймає рішення щодо ліквідації причини. Потім адміністратор відправляє інформацію щодо успішного усунення неполадок обслуговуючому персоналу, а останній – клієнту.

Також даний провайдер отримує доступ до мережі Інтернет від верхнього провайдера та є його клієнтом. Тому процес обробки претензій та обробки заяви даного провайдера на підключення до мережі Інтернет здійснюється за аналогічними схемами (рисунок 1. 1 та рисунок 1.2)

Інформаційні процеси, пов'язані із технічним обслуговуванням мережі, не розглядаємо, так як вони характерні для діяльності оператора телекомунікацій, а в даній роботі описуються особливості діяльності провайдера доступу до мережі Інтернет.

Розглянемо процес обміну інформацією між співробітниками провайдера, який зображений на рисунку 1.3.

Відповідно до рисунку 1.3, існує декілька потоків інформації. Розглянемо один із них. Секретар визначає умови укладення договору з клієнтом на підключення до мережі Інтернет, заповнює форму та відправляє юристу. Юрист перевіряє правильність оформлення договору та відправляє його директору. Директор підписує цей договір.

Розглянемо потік інформації від обслуговуючого персоналу до сервера. Обслуговуючий персонал отримує від клієнта інформацію щодо претензій, пов'язаних із проблемами доступу до мережі Інтернет та його дані для підключення до мережі, відправляє їх адміністратору. Адміністратор, в свою чергу, оброблює інформацію та встановлює відповідність між отриманими даними та даними, що містяться на сервері.

На сервер провайдера доступу до мережі Інтернет також відправляється інформація про фінансові розрахунки від бухгалтера. Бухгалтер відправляє дану інформацію системному адміністратору. Адміністратор оброблює її та вносить дані в базу даних, що розміщена на сервері.

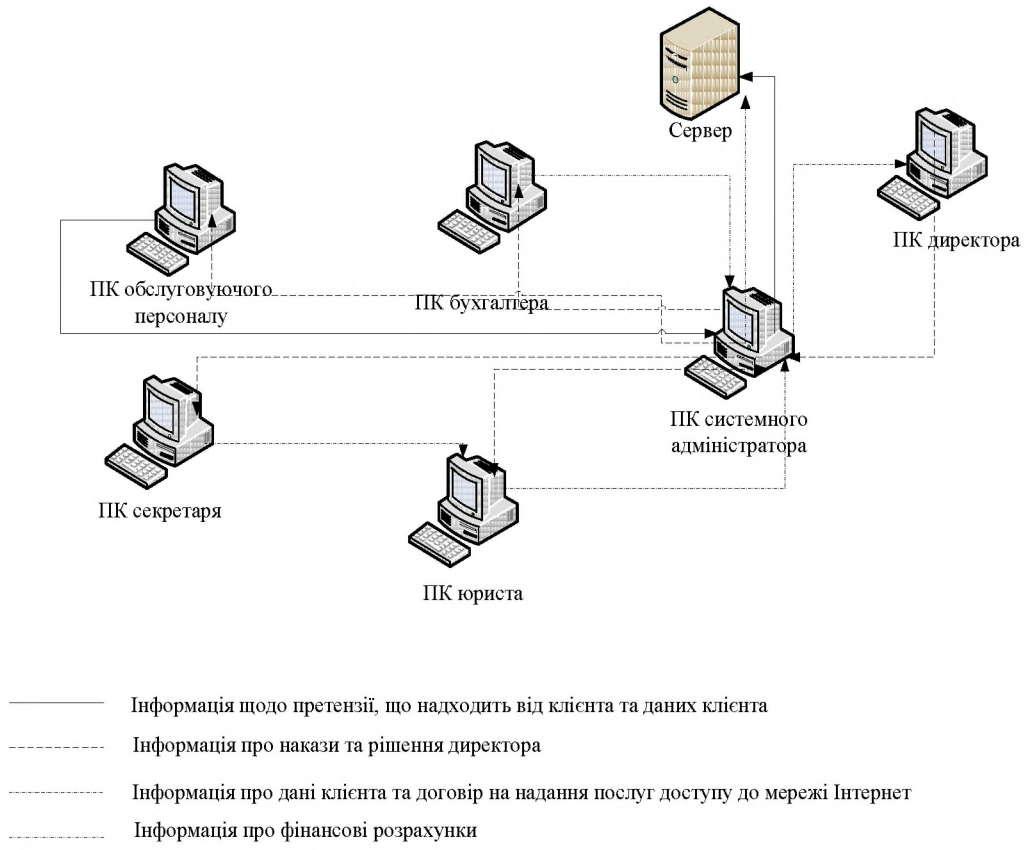

Рисунок 1.3 - Процес обміну інформацією між співробітниками провайдера доступу до мережі Інтернет

Розглянемо останній потік інформації, що зображений на рисунку 1.3. Директор даної організації відправляє інформацію про накази та рішення системному адміністратору, а він, в свою чергу, відправляє її іншим співробітникам провайдера.

Для наведеної вище інформації існують певні загрози, які можуть реалізовуватись зловмисниками.

1.1.4 Визначення загроз інформаційній безпеці провайдера та побудова моделі загроз

Загрози, які повинні нейтралізуватися оператором телекомунікацій, не розглядаються.

Серед загроз безпеці інформаційних ресурсів провайдера можна виділити наступні:

1 Комп'ютерні віруси. Найбільш ймовірними причинами створення і розповсюдження шкідливого програмного забезпечення є наступні:

1) шахрайство з метою привласнення ресурсів жертви: непомітне управління ураженим комп'ютером, підміна паролів доступу в Інтернет;

2) шпигунство - як правило, це проникнення в мережу з метою привласнення конфіденційної інформації, що представляє фінансову цінність.

2 Незаконне втручання у роботу мережі даного провайдера з боку конкурентів та зловмисників. Цю загрозу можна послабити (але не усунути) за допомогою використання криптографічних засобів захисту інформації, що розміщується на сервері.

3 Посередництво в обміні незашифрованими ключами (атака Man-in-the-Middle) - для проведення цієї атаки зловмисникові потрібен доступ до пакетів, що передаються мережею. Такий доступ до всіх пакетів, що передаються від провайдера доступу в будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Ефективно боротися з атаками типу Man-in-the-Middle можна тільки за допомогою криптографії. Після отримання доступу до мережі у атакуючого зловмисника з'являються великі можливості. Він може посилати некоректні дані додатків і мережевих службам, що призводить до аварійного завершення програми або неправильного функціонування; він може також наповнити комп'ютер або всю мережу трафіком, поки не відбудеться зупинка системи у зв'язку з перевантаженням; нарешті, атакуючий може блокувати трафік, що призведе до втрати доступу авторизованих користувачів до мережевих ресурсів.

4 Відмова в обслуговуванні (Denial of Service, DoS) - ця атака відрізняється від атак інших типів. Вона не направлена на отримання доступу до

вашої мережі або на витяг з цієї мережі будь-якої інформації. Атака DoS робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми. Дана атака позбавляє звичайних користувачів доступу до ресурсів або комп'ютерам мережі провайдера.

5 Підбір паролів і логінів, використовуючи для цього численні спроби доступу. Такий підхід носить назву повного перебору (brute force attack). Для цієї атаки використовується спеціальна програма, яка намагається отримати доступ до ресурсу загального користування (наприклад, до сервера). Якщо в результаті зловмисникові вдається підібрати пароль, він отримує доступ до ресурсів на правах звичайного користувача. Якщо цей користувач має значні привілеї доступу, зловмисник може створити для себе «прохід» для майбутнього доступу, який буде діяти, навіть якщо користувач змінить свій пароль і логін. Парольних атак можна уникнути, якщо не користуватися паролями в текстовій формі. Використання одноразових паролів та криптографічного аутентифікації можуть практично звести нанівець загрозу таких атак.

6 Загрози технологій спаму інформаційні безпеці провайдера проявляються в наступному:

1) ускладнення роботи інформаційних систем і ресурсів через непотрібне інформаційне навантаження;

2) витрачання великої кількості часу на перегляд спаму та психологічний дискомфорт, пов'язаний з подальшим видаленням численних повідомлень;

3) ризик видалення потрібної кореспонденції разом із спамом, що може привести до різного роду неприємних наслідків ;

4) висока вірогідність реалізації різних шахрайських схем, жертвами яких можуть ставати як приватні, так і юридичні особи;

5) одержувач спаму оплачує інтернет-провайдеру час чи трафік, витрачений на одержання непрошеної кореспонденції з поштового сервера.

7 Отримання незаконного доступу до Інтернету через використання логінів та паролів других користувачів та підміна IP-адресу комп'ютера, що призведе до того, що легальний користувач не зможе отримати доступ до Інтернету в потрібний для нього час.

8 Поширення неправдивої інформації про даного провайдера, що впливає на репутацію останнього.

9 Переманювання клієнтів конкурентами даного провайдера;

10 Збої в роботі систем оброблювання даних, які є однією з причин відсутності доступу до Інтернету та можуть породжуватися комп'ютерними вірусами, перепадами напруги в електромережі та ін.

Аналізуючи загрози та механізми їх реалізації, можна побудувати наступну модель загроз.

В приведеній нижче моделі загроз (таблиця 1.2) описуються види загроз телекомунікаційній мережі провайдера та механізми їх реалізації

Надалі для кожної із можливих загроз шляхом їх аналізу (можливо і методом експертних оцінок) необхідно визначити:

1) ймовірність виникнення таких загроз. Як перший крок визначення такої ймовірності можна використати її якісні оцінки. В таблиці використовуються наступні якісні оцінки ймовірності реалізації загроз – неприпустимо висока, дуже висока, висока, значна, середня, низька, знехтувано низька (стовпчик 3);

2) на порушення яких функціональних властивостей захищеності інформації (стовпчик 4) вона спрямована (порушення конфіденційності – к, цілісності – ц, доступності – д);

3) можливий (такий, що очікується) рівень ризику (стовпчик 5). Приклад цієї оцінки наведено також за якісною шкалою (відсутня, низька, середня, висока, неприпустимо висока). Наявність таких оцінок, навіть за якісною шкалою, дозволяє обґрунтувати необхідність забезпечення засобами захисту кожної з властивостей захищеності інформації;

4) механізми реалізації (можливі шляхи здійснення) загроз (стовпчик 6).

Таблиця 1.2- Модель загроз інформаційній безпеці провайдера доступу до мережі Інтернет

№	Вид загроз	Ймовір-ність	Що пору-шує	Рівень ризику	Механізм реалізації
1	2	3	4	5	6
1	Розвідка, аналіз трафіка	висока	к, ц, д	середній	Перехоплення інформації, що пересилаються у незашифрованому вигляді, відсутність виділеного каналу зв'язку між провайдерами, клієнтеми провайдерів, провайдерами та віддаленими співробітниками даного провайдера, між провайдером та оператором теле-комунікацій
2	Підміна (імітація) довіреного об'єкта або суб'єкта мережі з підробленням мережних адрес тих об'єктів, що атакують	висока	к, ц, д	середній	Фальсифікація (підроблення мережних адрес IP-адреси, повторне відтворення повідомлень при відсутності віртуального каналу, недостатні

					ідентифікації та автентифікації при наявності віртуального каналу)

Продовження таблиці 1.2

1	2	3	4	5	6
3	Подолання систем адміністрування доступом до робочих станцій, локальних мереж та захищеного інформаційного об'єкту, заснованих на атрибутах робочих станцій чи засобів управління доступом та маршрутизації (маскування) відповідних мереж – (файрволів, проксі – серверів та ін..)	висока	к, ц, д	високий	Використання недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, та ін.). Недостатні ідентифікації та автентифікації об'єктів РОМ, зокрема адреси відправника
4	Подолання криптографічної захищеності інформаційних об'єктів робочих станцій співробітників провайдера	низька	к	високий	Несанкціонований доступ до інформаційних об'єктів із використанням недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача із розкриттям ключових наборів

Продовження таблиці 1.2

1	2	3	4	5	6
5	Модифікація даних чи програмного коду, що зберігаються на сервері.	висока	ц, д	високий	Модифікація чи підміна інформаційних об'єктів (програмних кодів) чи їх частин шляхом впровадження руйнуючих програмних засобів чи зміни логіки роботи програмного файлу із використанням спеціальних типів вірусних атак,
					Зміна певної кількості символів інформаційного об'єкту із використанням спеціальних впливів на інформацію технічними каналами в локальній мережі чи в елементах розподіленої мережі

Продовження таблиці 1.2

1	2	3	4	5	6
6	Блокування сервісу чи перевантаження запитами системи управління доступом (відмова в обслуговуванні)	висока	д	високий	Використання атак типу “спрямований штурм” (Syn Flood), передачі на об’єкт, що атакується, не коректних запитів
					Використання анонімних запитів на обслуговування типу електронної пошти (spam) чи вірусних атак спеціального типу

Механізми та засоби захисту інформації від існуючих загроз використовуються відповідно до вимог до захищеності інформації, що знаходиться на сервері провайдера доступу до мережі Інтернет.

1.1.5 Вимоги до захищеності інформації провайдера

Згідно рішення НКРЗ №512 від 11.11.2010 «Умови здійснення діяльності у сфері телекомунікацій з надання послуг доступу до інтернет» до системи захисту інформації, що проходить через провайдера доступу до мережі Інтернет, висуваються наступні вимоги:

Організаційно-правова складова

Організаційні заходи є однією з найважливіших складових комплексної системи захисту інформації в організації:

1) перелік конфіденційних відомостей повинен відповідати реальному стану організації і вимогам законодавства;

2) повинен бути забезпечений повний пакет документів, пов'язаних із забезпеченням інформаційної безпеки в організації;

3) організаційними заходами забезпечити конфіденційність інформації при проведенні конфіденційних нарад і переговорів;

4) повинен бути підготовлений пакет документів, що регламентують правила поводження з конфіденційною інформацією;

5) розмежування прав користувачів на доступ як до локальних, так і до мережевих ресурсів повинно бути контрольованим і документованим процесом.

Інженерно-технічна складова:

1) повинні застосовуватися технічні засоби контролю доступу в приміщення;

2) для захисту серверної кімнати повинні застосовуватися додаткові технічні засоби контролю доступу;

3) повинні застосовуватися технічні засоби захисту акусто-мовної інформації при проведенні конфіденційних нарад і переговорів у тому випадку, якщо неможливо забезпечити конфіденційність переговорів за допомогою

організаційних заходів;

4) за допомогою технічних засобів повинна забезпечуватися захист від витоку конфіденційної інформації через канал ПЕМВН;

5) повинна бути забезпечена безперебійна робота ПК співробітників у випадку відключення електрики не менше, ніж на 10 хвилин;

6) повинна забезпечуватися безперебійна робота основного устаткування і технічних засобів, встановлених в серверній на весь термін відсутності основного енергопостачання.

Програмно-апаратна складова:

1) вміст веб-сайтів, що знаходяться на сервері провайдера, повинен відповідати таким вимогам:

а) не повинно містити матеріалів, заборонених законодавством;

б) повинен бути безпечним (не містити віруси, шкідливі скрипти);

в) не повинен містити матеріали, що не відносяться до робочого процесу;

2) обмін інформацією за допомогою різних програмних засобів не повинен завдавати шкоди конфіденційності, цілісності, доступності інформації;

3) за допомогою програмно-апаратних засобів повинна забезпечуватися захист від НСД до конфіденційної інформації, що зберігається на АРМ співробітників і на сервері.

Реалізація даних вимог можлива за рахунок застосування системи захисту інформації. А здійснити перевірку виконання вимог щодо захищеності інформації під час розробки та експлуатації СЗІ можливо за допомогою застосування методів оцінки ефективності СЗІ, які приведені нижче.

1.2 Оцінка ефективності систем захисту інформації. Загальна характеристика

Ефективність заходів захисту зазвичай оцінюється за трьома напрямками:

1) достатність;

2) адекватність отриманому ефекту;

3) якість реалізації.

Вжиті заходи визнаються достатніми, якщо вони повністю усувають заявлені загрози або створюють умови, при яких потенційний збиток від загрози стає прийнятним для власника. Достатність, мабуть, складніше за все піддається оцінці, і цьому є декілька причин. По-перше, помилка може бути закладена вже у самій моделі загроз.

Інша проблема полягає в тому, що кожна міра захисту лише частково сприяє усуненню загрози. Антивірусні засоби захищають від відомих вірусів, але не захищають від нових їхніх різновидів, що використовують ті ж вразливості. Управління оновленнями усуває такі вразливості, але не дає змоги уникнути помилок в налаштуванні засобів захисту і т.д. Оцінити, наскільки ці заходи в сукупності сприяють забезпеченню доступності ресурсу, що захищається - завдання для кваліфікованого експерта.

По-третє, доводиться враховувати взаємозв'язки інформаційних ресурсів. Якщо кілька програм становлять загальну систему управління базами даних, то

помилка в одній програмі може дозволити порушникові отримати доступ до інформації, що захищається, всіх інших додатків, як би добре вони не були б захищені.

Адекватність характеризує співвідношення витрат на реалізацію механізму захисту та отриманого ефекту. Ефект від впровадження рішень, запропонованих системними інтеграторами, не можна порівняти з витратами на експлуатацію (не кажучи вже про вартість самого рішення). Дуже показовий приклад з системами запобігання вторгнень (IPS). Розгорнувши подібну систему, компанії зазвичай стикаються з тим, що потік повідомлень від сенсорів настільки великий, що для його обробки потрібно впровадження дорогих засобів кореляції. Впровадивши і налаштувавши засобів кореляції, компанія переконується, що мережеві атаки успішно блокуються мережевими екранами без додаткового втручання модулів IPS.

В результаті ефект від впровадження системи можна вважати нульовим.

Інколи впровадження механізмів захисту призводить до негативного ефекту.

Наприклад, блокування користувачам доступу до мережі Інтернет або введення жорсткої фільтрації призводить до того, що співробітники починають шукати способи обійти заборону. В результаті зростає число інцидентів, пов'язаних з використанням чужих облікових записів, загальнодоступних бездротових точок доступу.

Якість механізму захисту залежить також від якості контролю. Наприклад, контроль доступу повинен супроводжуватися документуванням заявок на надання доступу та проведенням вибіркових перевірок, управлінням оновленнями - вибірковою перевіркою серверів і робочих станцій, мережевим екрануванням. Всі дії щодо контролю повинні бути задокументовані. В середньому періодичний контроль механізмів захисту з циклом в шість місяців в компанії з 500 чоловік забезпечує повне завантаження одного внутрішнього аудитора.

Адекватність заходів захисту зазвичай оцінюється методами аналізу ризиків, описаними в стандарті ISO 13335. Цей підхід критикується - адже оцінка ризиків так чи інакше базується на суб'єктивній думці експерта. Однак, зіставлення суб'єктивної оцінки потенційної загрози з об'єктивним розрахунком витрат на впровадження механізму захисту - основний метод оцінки адекватності застосовуваних заходів.

Найчастіше оцінка ризиків ґрунтується на суб'єктивній думці експерта, і три групи експертів можуть надати три різних результати.

Найскладніше оцінюється достатність заходів захисту, і для визначення даного параметру використовується комбінація з декількох методів. Стандарти в галузі управління інформаційної безпеки, такі як ISO 27001 та ін.. містять досить докладні каталоги механізмів безпеки, реалізація яких забезпечує достатній захист інформаційних ресурсів більшості компаній. Але вони не є універсальними для кожної організації.

Методика, запропонована в стандарті ISO 15408 , припускає, що для заданих власником цілей можна підібрати набір вимог безпеки так, що їх реалізація в інформаційній системі призведе до досягнення поставлених цілей. Практика показала, що розробити за допомогою цієї методики систему вимог для складної системи неможливо: формалізований відповідно до стандарту документ не можливо прочитати. Зараз стандарт використовується тільки для сертифікації програмних продуктів.

Ще один підхід - розрахунок метрик, коли окремі аспекти безпеки інформаційної системи можна охарактеризувати одним або кількома чисельними показниками. Наприклад, якість антиспамових фільтрів характеризується кількістю пропущеного спаму і кількістю помилково відфільтрованих повідомлень, а ефективність його застосування - середньою кількістю спаму, що отримується одним користувачем за умови, що кількість помилково відфільтрованих повідомлень близька до нуля. Для багатьох процесів за допомогою подібних показників можна зручно, наочно, а головне - однозначно

оцінювати достатність застосовуваних механізмів захисту. Наприклад, послідовне зростання кількості виявлених в мережі організації вірусів свідчить про недостатність застосовуваних в ній заходів антивірусного захисту. Останній з методів - тестування на проникнення. Якщо попередні методи дозволяють оцінити достатність механізмів захисту теоретично, то тестування на проникнення передбачає практичне виявлення методів реалізації атаки, з якими не вдається впоратися застосовуваними на момент оцінки заходами захисту. Тестування на проникнення може включати в себе як автоматизоване сканування, так і практичну реалізацію атак, в тому числі за допомогою таких методів, що погано піддаються оцінці, як соціальна інженерія.

Для більш детального розгляду методів оцінки ефективності, їх порівняльного аналізу, необхідно визначити критерії ефективності СЗІ, які описані нижче.

1.2.1 Визначення критеріїв ефективності

Ефективність СЗІ можна охарактеризувати як здатність системи протистояти несанкціонованим діям порушника. Таким чином, ефективність

СЗІ і характеризує рівень захищеності об'єкта. Існують якісні та кількісні методи аналізу ефективності СЗІ. У багатьох випадках якісних оцінок не достатньо, щоб визначити, наскільки надійний захист об'єкта. Більш точні кількісні методи. Однак для того, щоб «виміряти» ефективність, необхідно мати обґрунтований критерій (показник оцінки ефективності системи). На практиці зустрічаються такі типи критеріїв:

1) критерії типу «ефект-витрати», що дозволяють оцінювати досягнення цілей функціонування СЗІ при заданих витратах (так звана економічна ефективність);

2) критерії, що дозволяють оцінити якість СЗІ за заданими показниками і виключити ті варіанти, які не задовольняють заданим обмеженням. При цьому використовуються методи багатокритеріальної оптимізації, відновлення функцій і функціоналів, методи дискретного програмування;

3) критерії, що дозволяють оцінювати інтегральний ефект (наприклад, методи теорії нечітких множин).

Для оцінки якості системи захисту може бути використаний міжнародний стандарт ISO / IEC 27001. У першому з них пропонується розширений перелік аспектів інформаційної безпеки. Він починається з принципів розробки політики безпеки, включає основи перевірки системи на відповідність вимогам інформаційної безпеки, містить практичні рекомендації.

Стандарт ISO / IEC 15408 визначає критерії безпеки інформаційних технологій. У ньому не наводиться список вимог з безпеки, але положення стандарту дозволяють сформулювати цілі безпеки, спрямовані на забезпечення протистояння загрозам і виконання політики безпеки, тобто ті цілі, які повинні використовуватися як основа для оцінки властивостей безпеки продуктів, систем та інформаційних технологій. Стандарт описує інфраструктуру, в якій користувачі системи можуть сформулювати вимоги, а експерти з безпеки визначити, чи володіє продукт заявленими властивостями.

Ефективність функціонування СЗІ залежить від безлічі діючих взаємопов'язаних між собою елементів і, як правило, оцінюється сукупністю критеріїв, що знаходяться в складних конфліктних взаєминах. Відсутність на сьогоднішній день загального підходу до вирішення завдань даного класу вимагає використання різних не пов'язаних між собою методів оцінки якості.

1.3 Аналіз методів та методик оцінки ефективності СЗІ

В таблиці 1.3 наведені умовні назви використовуваних підходів до вибору критеріїв та оцінці параметрів, показники ефективності систем захисту та методики їх розрахунку.

Зокрема, відома методика сукупної вартості володіння (ТСО) була спочатку запропонована аналітичною компанією Gartner Group в кінці 80-х років (1986-1987) для оцінки витрат на інформаційні технології. Методика Gartner Group дозволяє розрахувати вартість інформаційних активів компанії, включаючи прямі і непрямі

витрати на апаратно-програмні засоби, організаційні заходи, навчання і підвищення кваліфікації співробітників компанії, реорганізацію, реструктуризацію бізнесу та т. ін.

Таблиця 1.3 - Підходи до оцінки СЗІ

№	Підхід до оцінки СЗІ	Показники оцінки ефективності СЗІ	Спосіб розрахунку показників
1	2	3	4
1	Статистичний	Загроза і-го виду виникає в середньому за період часу T_i	Статистична обробка потенційних загроз та їх наслідків
2	Ймовірнісний	Сумарні середні збитки $\mathbf{R} = \sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{P}\left(\frac{\vec{\gamma}}{\vec{s}}\right)\mathbf{P(s)}\prod(\vec{\gamma},\vec{s}) + \mathbf{m}$ $\mathbf{P}\left(\frac{\vec{\gamma}}{\vec{s}}\right)$- ймовірність усунення; $\mathbf{P(s)}$- апріорна ймовірність стану об'єкта контролю; $\prod(\vec{\gamma},\vec{s})$ – збитки при прийнятті рішення $\boldsymbol{\gamma}$ при стані об'єкта s; m - кількість загроз, які можна розпізнати	Визначається ймовірність відмови системи від обробки даних в результаті реалізації загроз
3	Частотний	Очікуваний збиток від і-ої загрози $\mathbf{R_i = F(S,V)}$, де $\mathbf{S}$ – показник частоти виникнення загрози, $\mathbf{V}$ – умовний показник збитку	На основі аналізу статистичного матеріалу задається значення $\mathbf{S}$, величина $\mathbf{V}$ вибирається рівною від 1 до max можливової суми збитку, розраховується значення показника $\mathbf{R_i}$ як функції параметрів V та S
4	Експертне оцінювання	Ступінь забезпечення безпеки SR системи S $\mathbf{SR_{(s,r)}} = \frac{\mathbf{1}}{\mathbf{n_{i=1}^{n}}}\mathbf{W_i G_i}$	Визначається кількість (n) та перелік параметрів (i), що характеризують СЗІ. Задаються значення суб'єктивних коефіцієнтів

			важливості ($\mathbf{W_i}$) кожної із характеристик $\mathbf{G_i}$. Розраховується значення **SR**

Продовження таблиці 1.3

1	2	3	4
5	Інформаційно-ентропійний	Величина інформаційної ентропії Шенона $\Psi(t) = (\int_0^t S_n(t-\tau) \dots (\int_0^t S_3 \left(\int_0^t S_1(\tau) S_2(t-\tau) d\tau \right) d\tau \dots) d\tau)$ $S_1, \dots S_n$ – значення інформаційних ентропій різних підсистем	Проводиться аналітичне обчислення інформаційної ентропії системи. При лінійній залежності ефективність підсистеми в інформаційному плані вважають задовільною. В протилежному випадку – неефективною.
6	Матричний (формальні моделі захисту)	Стан системи захисту описується трьома параметрами, наприклад: (S,O,M) – множини S – суб'єктів, O – об'єктів, M – об'єктів; або (O,H,M) – O – основі та складові системи (нормативно-правова, організаційна, інформаційна та ін..), H – напрям захисту, M – етап створення СЗІ	Визначення параметрів. Побудова трьохмірної матриці відносин. Перетворення матриці відносин у двохмірну матрицю. Визначення кількісних та якісних значень показників
7	Багаторівневий підхід	Стан системи захисту описується сукупністю рівнів конфіденційності та набору категорій конфіденційності	Модель кінцевих станів Бела Ла-Падули, решіткова модель Д. Денінга
8	Оптимізаційний	Вирішується задача дискретного програмування виду: максимізувати	Методи Балаша для змінних цілого типу,

	(комбінаторний)	$\sum_{j=1}^{n} C_j X_j$ за умов $\sum_{j=1}^{n} a_{ij} x_j \leq b_i$, $i = \overline{1,m}$; $x_j \in \{0,1\}$, $j = \overline{1,n}$	гілок та меж, виключення групи невідомих, методи лінійного та параметричного програмування.

1.3.1 Методика сукупної вартості володіння (ТСО)

Методика ТСО може бути використана для обґрунтування економічної ефективності існуючих систем захисту інформації. Вона дозволяє керівникам служб інформаційної безпеки (CISO) обґрунтовувати бюджет на ІБ, а також визначити ефективність роботи співробітників служби ІБ. Крім того, оперативно вирішується завдання контролю і корекції показників економічної ефективності і зокрема показника ТСО. Таким чином, показник ТСО можна використовувати як інструмент для оптимізації витрат на забезпечення необхідного рівня захищеності ІС та обґрунтування бюджету на ІБ.

Показник ТСО може застосовуватися практично на всіх основних етапах життєвого циклу системи захисту інформації та дозволяє визначити існуючі та заплановані витрати на ІБ. Тому показник ТСО дозволяє об'єктивно і незалежно обґрунтувати економічну доцільність впровадження та використання конкретних організаційних і технічних заходів і засобів захисту інформації. При цьому для об'єктивності рішення необхідно додатково враховувати і стан зовнішнього і внутрішнього середовища підприємства, наприклад показники технологічного, кадрового та фінансового розвитку підприємства.

Якісне управління ТСО дозволяє раціонально і економно реалізовувати кошти бюджету на ІБ, досягаючи при цьому прийнятного рівня захищеності компанії, адекватного поточним цілям і завданням бізнесу. Істотно, що порівняння певного показника ТСО з аналогічними показниками ТСО в галузі (аналогічними компаніями) дозволяє об'єктивно і незалежно обґрунтувати витрати компанії на ІБ. Адже часто виявляється досить важко або навіть практично неможливо оцінити прямий економічний ефект від витрат на ІБ.

В цілому методика ТСО компанії Gartner Group дозволяє:

1) одержати адекватну інформацію про рівень захищеності ІС та сукупної вартості володіння системи захисту інформації;

2) порівняти підрозділи служби ІБ компанії, як між собою, так і з аналогічними підрозділами інших підприємств у даній галузі;

3) оптимізувати інвестиції на ІБ компанії з урахуванням реального значення показника ТСО.

Під показником ТСО розуміється сума прямих і непрямих витрат на організацію (реорганізацію), експлуатацію та супроводження системи захисту інформації за рік. ТСО може розглядатися як ключовий кількісний показник ефективності організації ІБ в компанії, так як дозволяє не тільки оцінити сукупні витрати на ІБ, але й керувати цими витратами для досягнення необхідного рівня захищеності ІС.

При цьому прямі витрати включають як капітальні компоненти витрат (асоційовані з фіксованими активами або "власністю"), так і трудовитрати, які враховуються в категоріях операцій та адміністративного управління. Сюди ж відносять витрати на послуги віддалених користувачів, аутсорсинг і ін, пов'язані з підтримкою діяльності організації.

Непрямі витрати відображають вплив ІС і підсистеми захисту інформації на співробітників компанії за допомогою таких вимірних показників як простої системи захисту інформації та ІС в цілому, витрати на операції та підтримку (не пов'язані з прямими витратами). Дуже часто непрямі витрати відіграють значну роль, так як вони зазвичай спочатку не відображаються в бюджеті на ІБ, а виявляються явно при аналізі витрат надалі, що в кінцевому рахунку призводить до зростання "прихованих" витрат компанії на ІБ.

Підхід до оцінки ТСО базується на результатах аудиту структури і поведінки системи захисту інформації та ІС в цілому, включаючи дії співробітників служб автоматизації, інформаційної безпеки та користувачів ІС. Збір та аналіз статистики по структурі прямих (HW / SW, операції, адміністративне управління) і непрямих витрат (на кінцевих користувачів і

простої) проводиться, як правило, протягом 12 місяців. Отримані дані оцінюються по ряду критеріїв з урахуванням порівняння з аналогічними компаніями в галузі.

В методиці ТСО в якості бази для порівняння використовуються дані і показники ТСО для західних компаній. Проте дана методика здатна враховувати специфіку українських компаній за допомогою так званих поправочних коефіцієнтів, наприклад:

1) за вартістю основних компонентів системи захисту інформації та ІС, інформаційних активів компанії (профілі вартості) з урахуванням даних по кількості і типам серверів, персональних комп'ютерів, периферії і мережевого обладнання;

2) за заробленими коштами співробітників з урахуванням доходу компанії, географічного положення, типу виробництва та розміщення організації у великому місті;

3) за кінцевими користувачами IT (End Користувач скаляри) з урахуванням типів користувачів і їх розміщення (для кожного типу користувачів потрібна різна організація служби підтримки та інформаційної системи);

4) з використання методів так званої кращої практики в галузі управління ІБ (Best Practices), з урахуванням реального стану справ з управління змінами, операціями, активами, сервісного обслуговування, навчання, планування та управління процесами;

5) за рівнем складності організації (рівень складності), з урахуванням стану організації кінцевих користувачів (відсоток впливу - 40%).

В цілому, визначення витрат компанії на ІБ передбачає вирішення наступних трьох задач:

1) оцінка поточного рівня ТСО системи захисту інформації та ІС в цілому;

2) аудит ІБ компанії на основі порівняння рівня захищеності компанії та рекомендованого (краща світова практика) рівня ТСО;

3) формування цільової моделі ТСО.

Розглянемо кожне з перерахованих завдань.

Оцінка поточного рівня ТСО. У ході робіт з оцінки ТСО проводиться збір інформації та розрахунок показників ТСО організації за такими напрямами:

1) існуючі компоненти ІС (включаючи систему захисту інформації) та інформаційні активи компанії (сервери, клієнтські комп'ютери, периферійні пристрої, мережеві пристрої);

2) існуючі витрати на апаратні і програмні засоби захисту інформації (витратні матеріали, амортизація);

3) існуючі витрати на організацію ІБ в компанії (обслуговування СЗІ, а також штатних засобів захисту периферійних пристроїв, серверів, мережевих пристроїв, планування і управління процесами захисту інформації, розробку концепції та політики безпеки тощо);

4) існуючі витрати на організаційні заходи захисту інформації;

5)існуючі непрямі витрати на організацію ІБ в компанії і зокрема забезпечення безперервності або стійкості бізнесу компанії Аудит ІБ компанії. За результатами співбесіди з ТОР-менеджерами компанії і проведення інструментальних перевірок рівня захищеності організації проводиться аналіз наступних основних аспектів:

1) політика безпеки;

2) організація захисту;

3) класифікація та управління інформаційними ресурсами;

4)управління персоналом;

5)фізична безпека;

6) адміністрування комп'ютерних систем і мереж;

7) управління доступом до систем;

8) розробки і супровід систем;

9) планування безперебійної роботи організації;

10) перевірки системи на відповідність вимогам ІБ.

На основі проведеного аналізу вибирається модель ТСО, порівнянна з середніми і оптимальними значеннями для групи аналогічних організацій, що

мають схожі з розглянутої організацією показники за обсягом бізнесу. Така група вибирається з бази даних за ефективністю витрат на ІБ та ефективністю відповідних профілів захисту аналогічних компаній.

Порівняння поточного показника ТСО перевіряється з базовим значенням показника ТСО дозволяє провести аналіз ефективності організації ІБ компанії, результатом якого є визначення "вузьких" місць в організації, причин їх появи і вироблення подальших кроків щодо реорганізації системи захисту інформації та забезпечення необхідного рівня захищеності ІС.

Формування цільової моделі ТСО. За результатами проведеного аудиту моделюється цільова (бажана) модель, що враховує перспективи розвитку

бізнесу та системи захисту інформації (активи, складність, методи кращої практики, типи СЗІ, кваліфікація співробітників компанії і т. ін.). Крім того, розглядаються капітальні витрати і трудовитрати, необхідні для проведення перетворень поточного середовища в цільове. В трудовитрати на впровадження включаються витрати на планування, розгортання, навчання і розробку. Сюди ж входять можливі тимчасові збільшення витрат на управління і підтримку.

Для обґрунтування ефекту від впровадження нової системи захисту інформації (ROI) можуть бути використані модельні характеристики зниження сукупних витрат (ТСО), що відображають можливі зміни в системі захисту інформації.

1.3.2 Оптимізаційний підхід до оцінки ефективності

При цьому підході вирішується завдання оптимізації виду: максимізувати якусь функцію при заданих обмеженнях.

Вид функції мети і система обмежень будуються в залежності від поставленого завдання. Так, якщо ввести нижченаведені позначення, то можна розглянути кілька варіантів постановки.

Отже, нехай:

$U = \{u_j\}$ - безліч загроз безпеки, $j = 1, \ldots m$;

A = {a_i} - безліч механізмів безпеки, i = 1, ... n;

C = {c_i} - допустимі витрати на створення захисту (загальний обсяг витрат), причому c_i - це витрати на придбання і-го засобу захисту;

d (i, j) - ефективність нейтралізації і-м механізмом безпеки j-ї загрози.

Для побудови математичної моделі введемо змінну p (i, j) рівну 1, якщо j-а загроза усувається за допомогою і-го механізму, і нулю - в іншому випадку і q, таку, що:

$$\mathbf{q(i,j)} = \begin{cases} \mathbf{1} - \text{якщо } \mathbf{i} - \text{й механізм безпеки використовується для усунення } \mathbf{j} - \text{ї загрози} \\ \mathbf{0} - \text{в протилежному випадку} \end{cases}$$

Спочатку вважаємо, що інформаційні загрози між собою не пов'язані.

Перше завдання - знайти максимальний ефект від нейтралізації безлічі інформаційних загроз U за допомогою задекларованих в системі засобів захисту A при обмеженнях на загальний обсяг витрат C.

$$\sum_{\mathbf{j=1}}^{\mathbf{m}} \sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{d(i,j)p(i,j)} \rightarrow \mathbf{max}, \qquad (1.1)$$

при обмеженнях:

$$\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{c(i)} * \mathbf{sign} \sum_{\mathbf{uj} \in \mathbf{U}}^{\mathbf{n}} \mathbf{p(i,j)} \leq \mathbf{C}, \qquad (1.2)$$

$$\mathbf{p(i,j)} \in \mathbf{(1,0), j = 1, \dots m; i = 1, \dots n}. \qquad (1.3)$$

Друге завдання - варіант, коли рівень інформаційної безпеки визначається СЗІ з найменшою ефективністю. В цьому випадку функція мети у формальній постановці задачі має вигляд:

$$\min \sum_{i=1}^{n} d(i,j)p(i,j) \rightarrow \max, \qquad (1.4)$$

а обмеження (1.2) і (1.3) залишаються тими ж.

Третє завдання - випадок, коли поява однієї загрози є джерелом для іншої, тобто інформаційні загрози не є незалежними. В цьому випадку функція мети має вигляд (1.1), але обмеження змінюються - по першому це перелік основних, а по другому – породжених загроз. Замість функції p (i, j) використовується q (i, j).

Четверта задача - це задача мінімізації витрат на СЗІ при обмеженні на заданий рівень ефективності. При цьому алгоритм рішення доповнюється процедурою пошуку максимальних елементів в кожному стовпці матриці

q(i, j) і розрахунком найвищого рівня ефективності P, що дорівнює сумі знайдених максимальних елементів:

$$\sum_{i=1}^{n} c_i * \operatorname{sign} \sum_{j=1}^{m} p(i,j) \rightarrow \min , \quad (1.5)$$

$$\sum_{j=1}^{m} \sum_{i=1}^{n} d(i,j)p(i,j) / \sum_{i=1}^{n} (\max_j d(i,j)) \leq P , \quad (1.6)$$

$$p(i,j) \in (1,0), j = 1, \dots m; i = 1, \dots n. \quad (1.7)$$

Для вирішення завдань зазначеного типу можуть бути використані методи Балаша для змінних цілого типу, гілок і меж, виключення групи невідомих, елементи теорії двоїстості, інструментарій лінійного і параметричного програмування.

Підвищення швидкості розрахунку при використанні розглянутих алгоритмів є актуальним завданням, тому що між часом виконання обчислень і розміром задачі існує експоненціальна залежність. А розмірність задачі, в свою чергу, залежить від складності СЗІ, яка зростає в міру появи нових загроз безпеки, і ускладненням, пов'язаним з розвитком самої інформаційної системи, для якої створено систему захисту.

Відомо, що в алгоритмі Балаша потрібне виконання лише операцій додавання і віднімання, щоб знайти часткове вирішення задачі але також при заданому частковому рішення не завжди вдається визначити, яке значення повинна мати вільна змінна при будь-якому допустимому обмеженні.

Метод гілок і меж відноситься до комбінаторним методам. До переваг методу слід віднести гнучкість побудови, що дозволяє ефективно використовувати специфіку розв'язуваної задачі. Проте дослідники відзначають залежність обсягу обчислень, необхідних для виконання завдання, від обраного способу обчислення оцінок.

Обидва методи ґрунтуються на послідовному аналізі варіантів, але використовують різні підходи для відбору підмножин, що не містять оптимальних рішень.

У методі Балаша відбір проводиться на підставі принципу оптимальності. У методі гілок і меж відбір проводиться із застосуванням нижніх оцінок в підмножинах.

Враховуючи сказане, сформулюємо наступне твердження: алгоритм, який поєднує позитивні якості цих алгоритмів є ефективним в порівнянні з вихідними з точки зору теорії обчислювальної складності.

Сутність алгоритму

1 Задається значення цільової функції мети так, щоб воно відповідало рішенням, при якому всі p (i, j) = 0 (поточна нижня оцінка оптимального рішення дорівнює $0(z_0 = 0)$. Можливо знаходження нижньої оцінки оптимального значення цієї функції за допомогою методу гілок і меж.

2 Перевіряється основний список завдань і закінчити обчислення, якщо він порожній. В іншому випадку вибрати чергову задачу з основного списку і викреслити її з нього. При цьому на безлічі отриманих оцінок виділяють «кращу» і найближчу до неї.

3 Встановлюється, чи існує припустиме додаткове рішення, за яким значення цільової функції перевершує поточну нижню оцінку оптимального рішення. Якщо можна встановити, що не існує допустимого доповнення, у якого значення цільової функції перевершує значення поточної нижньої оцінки оптимального рішення, то покласти $z_0^{(k+1)} = z_0^k$ і повернутися до другого кроку. В іншому випадку перейти до четвертого кроку.

4 Якщо часткове рішення містить всі n змінних (тобто є повним), то зафіксувати його і повернутися до другого кроку. В іншому випадку перейти до п'ятого кроку.

5 Вибирається будь-яка вільна змінна, яка не входить в часткове вирішення. Використовуються елементи методу гілок і меж. Вводяться два нових завдання в основний список. В одному з них покласти p(i,j) = 0 в частковому рішенні, а в іншому - p(i,j) = 1. Покласти $z_0^{(k+1)} = z_0^k$ і повернутися до другого кроку.

6 Якщо зафіксовано допустиме рішення, при якому цільова функція не змінилася, це рішення оптимальне. Зменшення кількості операцій порівнянь досягається завдяки вибору «кращого» на другому кроці кожної ітерації.. Таким чином, запропонований ефективний алгоритм вирішення задачі визначення ефективності функціонування складної системи.

Приведемо алгоритм методики оцінки якості СЗІ з використанням оптимізаційного підходу:

1 Складається сценарій розвитку небезпеки (граф виду «дерево»), що становить собою логіко-імовірнісну модель функціонування СЗІ. Це двочастковий граф G (A, U) такий, що вершини множин в A відповідають апаратним і програмним засобам захисту, а вершини множин в U - відповідним інформаційним загрозам. Кожен елемент (вершина) характеризується ціною і ефективністю з нейтралізації інформаційних загроз. Кожній вершині безлічі U присвоюється коефіцієнт, рівний вартості, що відповідає СЗІ, а кожній дузі, вага p (I, J) = {1,0}. Кінцева подія описує небезпечний стан системи.

2 Аналітично граф описується за допомогою цільової функції небезпеки системи і системи обмежень.

3 За допомогою логіко-імовірнісних перетворень функція небезпеки системи приводиться до однієї з канонічних форм і замінюється ймовірнісною функцією p (i, j). При цьому необхідно мати ймовірності подій, плановані витрати на створення захисту і задати ефективність нейтралізації загрози. Значення

ймовірнісної функції p, при якій значення функції небезпеки і дорівнює одиниці, визначає ступінь ризику, присутнього в системі.

4 Застосовуючи лише операції додавання і віднімання (алгоритм Балаша) знаходять часткові рішення, при цьому вибір на другому та п'ятому кроки може ґрунтуватися на інформації, отриманої за допомогою методу гілок і меж.

Застосовуючи ефективні правила вибору на другому та п'ятому кроки, можна знайти допустиме по всім обмеженням і близьке до оптимального рішення вже на початкових ітераціях.

Обчислювальна складність алгоритму тісно пов'язана з числом змінних цілого типу. В даному алгоритмі обсяг обчислень визначається насамперед числом завдань, що входять в основний список.

1.3.3 Теоретико-графовий підхід до оцінки ефективності СЗІ

Велика кількість методів і механізмів забезпечення комп'ютерної безпеки, принцип розумної достатності при забезпеченні комп'ютерної безпеки зумовлюють необхідність формальних моделей і методик аналізу ефективності систем захисту. У літературі і практиці дані питання характеризуються терміном "комплексні оцінки захищеності", включаючи оцінку ефективності методів і механізмів як програмно-технічного, так і нормативно-організаційного характеру для захисту активів організації.

Рішення подібних завдань ґрунтується на теоретико-графовому підході, запропонованому ще на початку 70-х рр.. у вигляді т.зв. "Моделі систем з повним перекриттям загроз безпеки".

Система захисту в рамках даної формалізації представляється графом, варіант якого представлений на рисунку 1.4

Кожне ребро графа G (P, O, Z, E, H) визначає вплив конкретної загрози на конкретний актив (об'єкт) або усунення (нейтралізацію) певним захисним механізмом загрози безпеки. При цьому від кожної загрози може бути кілька впливів на різні об'єкти і кожен об'єкт може зазнавати впливу кількох загроз.

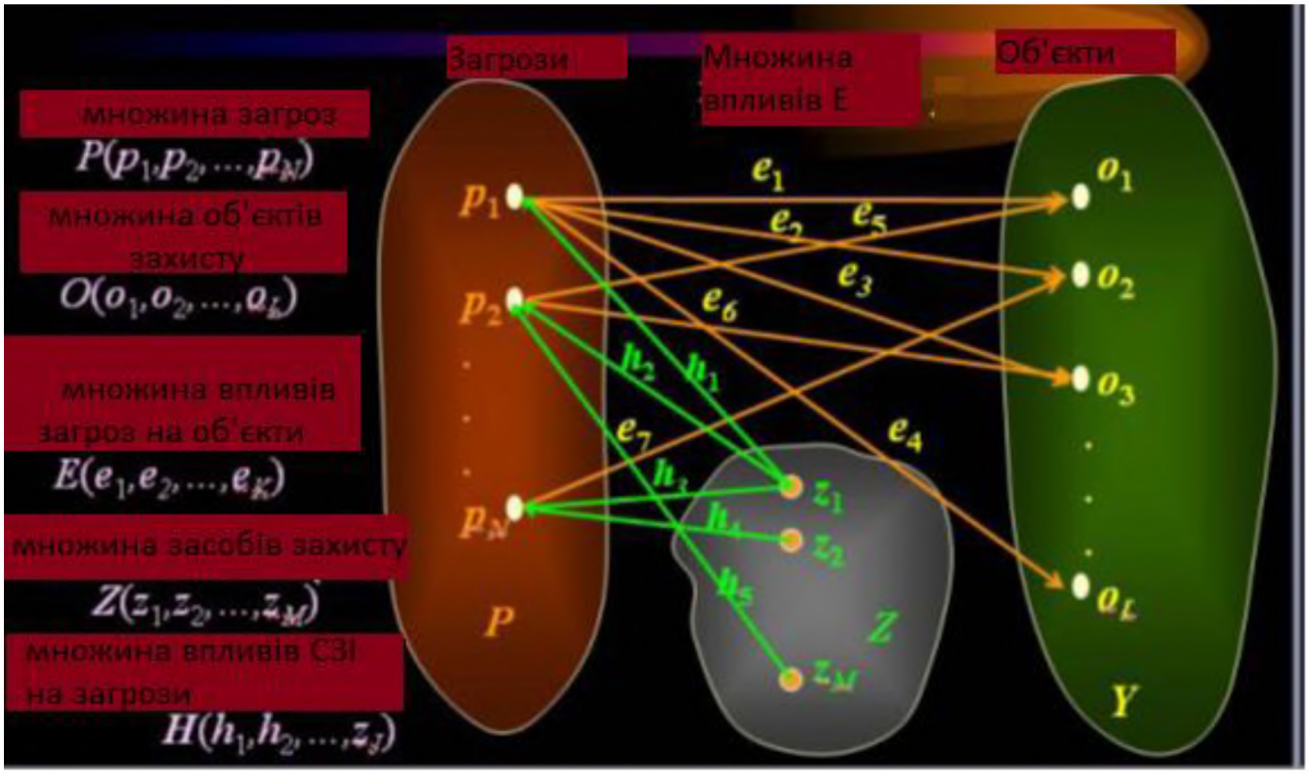

Рисунок 1.4 - Модель системи захисту у вигляді графа

Для отримання та оперування кількісними параметрами граф G (P, O, Z, E, H) зважується і еквівалентно представляється наступної сукупністю векторів і матриць:

1) вектор P (p_1, p_2, ..., p_N), де p_j - ймовірність здійснення відповідної загрози;

2) вектор O (o_1, o_2, ..., o_L), де o_i - вартість відповідного об'єкта захисту;

3) NxL матриця E $\{e_{ij}\}$, де $e_{ij} = 1$ при впливі i-ї загрози на j-й об'єкт, і $e_{ij} = 0$ в іншому випадку;

4) вектор Z (z_1, z_2, ..., z_M), де $z_к$ - вартість відповідного засобу захисту;

5) NxM матриця H $\{h_{ij}\}$, де $h_{iк}$ - ймовірність усунення i-ї загрози при застосуванні j-го засобу захисту.

В рамках даної формалізації можливе вирішення таких важливих практичних завдань, як аналіз техніко-економічної чи тактико-технічної ефективності систем захисту.

Аналіз техніко-економічної ефективності системи захисту ґрунтується на визначенні кількісного критерію, що відображає вплив реалізованої системи захисту (прийнятих) на зниження небезпеки від впливу загроз, або інакше на величину збитку від загроз безпеки.

В якості такого критерію техніко-економічної ефективності можна використовувати наступний показник:

$$Э = \frac{U - U'}{\sum_{i=1}^{L} o_i + \sum_{k=1}^{M} z_k}, \tag{1.8}$$

де U - оцінка величини збитку від загроз безпеки при відсутності захисних заходів і механізмів;

U '- оцінка величини залишкового збитку при реалізації захисних заходів і механізмів.

Розрахунок величин U і U 'здійснюється за наступними співвідношеннями:

$$U = \sum_{i=1}^{L} O_i\left(1 - \prod_{j=1}^{N} e_{ij}(1 - p_j)\right), \tag{1.9}$$

$$U' = \sum_{i=1}^{L} o_i\left(1 - \prod_{j=1}^{N} e_{ij}\left(1 - p_j\left(1 - \prod_{k=1}^{M}(1 - h_{jk})\right)\right)\right). \tag{1.10}$$

Завдання тактико-технічного аналізу ефективності систем захисту полягають у визначенні залишкової ймовірності реалізації всіх можливих загроз без урахування вартості об'єктів та заходів захисту, що може бути обчислено за наступним співвідношенням:

$$P'_{под} = \left(1 - \prod_{j=1}^{N}\left(1 - p_j\left(1 - \prod_{k=1}^{M}(1 - h_{ik})\right)\right)\right). \tag{1.11}$$

Відзначаючи практичну значимість наведених співвідношень, слід зауважити, що їх використання потребує застосування методів оцінювання загроз безпеки, зокрема методів експертних оцінок ймовірності реалізації загроз та величин h_{ij} ступеня (ймовірності) усунення загроз в залежності від прийнятих заходів і механізмів захисту.

Внаслідок проведеного аналізу підходів та методів оцінки ефективності СЗІ були виявлені їх переваги та недоліки, що зазначені в таблиці 1.4

В даній таблиці недоліки методу або підходу позначені мінусом, а їх переваги – плюсом.

Таблиця 1.4 – Порівняльна характеристика методів оцінки

Характеристика методики	Назва методики		
	Методика сукупної вартості володіння (ТСО)	Методика оцінки якості СЗІ з використанням оптимізаційного підходу	Теоретико-графовий метод оцінки ефективності СЗІ
Залежність тривалості розрахунку від кількості загроз	-	+	+
Аналіз збитків від реалізації загроз	+	_	+
Наявність обмежень	-	+	_
Швидкий процес розрахунку	_	-	+
Аналіз витрат на ІБ	+	+	+
Зручність в застосуванні	-	-	-
Швидкий процес отримання вихідних даних	-	+	-

Відповідно до табл.1.4, методи та підходи до оцінки ефективності СЗІ порівнюються за наступними показниками:

1 Вплив повноти переліку загроз на тривалість розрахунку. Повнота переліку загроз прямо пропорційна точності розрахунку рівня ефективності СЗІ.

Але при збільшенні кількості загроз, що враховуються при проведенні оцінки, збільшується час, що відводиться на виконання розрахунків. Ефективні методи та підходи характеризуються слабкою залежністю тривалості розрахунку від кількості загроз.

2 Аналіз збитків від реалізації загроз. Визначення доцільності впровадження СЗІ неможливе без аналізу збитків. Якщо величина збитку значно перевищує величину витрат на забезпечення ІБ, то впровадження СЗІ є економічно доцільним для відповідної організації.

3 Наявність обмежень. Ефективність СЗІ в більшості випадків визначається за критерієм «ефект-затрати». Збільшення рівня ефективності СЗІ передбачає збільшення величини затрат на забезпечення ІБ. Тому використання ефективних методів оцінки повинно передбачати вирішення одного із завдань: мінімізувати затрати при обмеженні на заданий рівень ефективності СЗІ, або знайти максимальний ефект від впровадження СЗІ при обмеженні на обсяг затрат.

4 Швидкість розрахунку. Ефективність використання методів напряму залежить від швидкості розрахунків, при чому точність розрахунків повинна залишатися незмінною.

5 Аналіз витрат на ІБ. При розрахунку ефективності СЗІ потрібно враховувати капітані та експлуатаційні витрати на впровадження СЗІ, та порівнювати їх з величиною збитків від реалізації загроз. Аналіз витрат на ІБ також дозволяє заздалегідь планувати бюджет компанії.

6 Зручність в застосуванні. Більшість методів передбачає розрахунок вартості інформаційних ресурсів, а для деяких організації визначення цінності інформації є досить складним завданням, тому дані методи не завжди зручно використовувати на практиці.

7 Швидкість отримання вихідних даних. Більшість методів передбачає отримання вихідних параметрів за допомогою обробки статистичних відомостей. А сам процес обробки є досить тривалим.

1.4 Висновок. Постановка задачі

В даному розділі визначені особливості діяльності провайдера, побудовані моделі інформаційних потоків для кожного процесу. Визначені загрози, що характерні для провайдера та побудована модель загроз. Також здійснений аналіз існуючих методів оцінки ефективності систем захисту інформації. В результаті аналізу було визначено, що жоден з методів не позбавлений недоліків. Для підвищення ефективності оцінки СЗІ та рівня захищеності інформаційної системи провайдера, необхідно вирішити наступні задачі:

1) визначити критерії оцінки ефективності системи захисту інформації;
2) розробити методику, яка б враховувала всі переваги існуючих методів оцінки та специфіку провайдера доступу до мережі Інтернет;
3) визначити вихідні дані, необхідні для проведення оцінки;
4) вибрати для оцінки механізми та заходи захисту інформації;
5) визначити загрози, які будуть враховуватись при виконанні оцінки;
6) провести розрахунок показників ефективності СЗІ за допомогою методики оцінки.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Розробка методики оцінки ефективності системи захисту інформації

В результаті аналізу існуючих методів оцінки ефективності СЗІ, який був приведений в першому розділі, було визначено, що для проведення оцінки за більшістю методів необхідно визначити вартість інформаційних ресурсів організації, яка враховується при визначенні величини збитку від реалізації загроз. Для організацій, які мають велику кількість співробітників, клієнтів та володіють великою кількістю інформації, визначити вартість інформаційних ресурсів та величини збитків досить складно. Тому потрібно розробити методику, яка б передбачала розрахунок збитків, які пов'язані із витратами на відновлення роботи інформаційної системи, не враховуючи вартість інформації. Також методика повинна застосовуватися і при наявності великої кількості загроз, характерних для відповідної організації.

В даному розділі запропонована методика, враховує специфіку провайдера, зокрема кількість його клієнтів, при визначення збитків, яких зазнає дана організація внаслідок успішної реалізації атак.

Оцінка ефективності системи захисту інформації і вибір оптимального варіанту системи захисту (необхідного набору механізмів захисту) здійснюється наступним чином:

1) розрахунок параметру P (ймовірності нейтралізації загроз системою захисту інформації) для оцінки ефективності системи за вихідними даними, отриманими статистичним або, в разі нестачі статистики, одним з методів або підходів (оптимістично-песимістичний підхід, метод експертної оцінки);

2) розрахунок параметру C (величини збитку внаслідок успішної реалізації загроз), враховуючи час простою системи $t_п$ та час відновлення інформації системним адміністратором $t_в$;

3) розрахунок критеріїв ефективності D (коефіцієнту ефективності), $Ц_{СЗІ}$ (вартості СЗІ), $П_{СЗІ}$ ($dП_{СЗІ}$) – продуктивності СЗІ для кожного варіанту системи захисту (набору механізмів та засобів захисту);

4) вибір системи захисту (набору механізмів та засобівзахисту при розробці системи) з максимальним коефіцієнтом ефективності D, що задовольняє обмеженням по вартості $Ц_{СЗІ}$ і продуктивності $П_{СЗІ}$.

5) аналіз зміни коефіцієнта ефективності dD при заданому прирості критеріїв $Ц_{СЗІ}$ і $dП_{СЗІ}$ методом послідовного вибору поступок з оцінкою доцільності вибору системи, що задовольняє новим обмеженням.

Для отримання більш точних даних, наближених до реальності і відповідності специфіці провайдера, на першому етапі (підготовчому), що передує етапу розрахунку параметрів, потрібно провести ретельний опис системи. Цей пункт є невід'ємною частиною вимог багатьох міжнародних стандартів у галузі інформаційної безпеки. Його значимість велика, тому що чим краще фахівець знає об'єкт, який йому належить захищати, тим більш точну оцінку він зможе отримати.

2.1.1 Розрахунок ймовірності нейтралізації загроз системою захисту інформації

Основною проблемою проведення кількісної оцінки рівня ефективності є визначення вихідних параметрів для системи захисту - ймовірності та інтенсивності загроз. Розглянемо можливі методи визначення ймовірності та інтенсивності загроз.

1 Метод статистичної оцінки інтенсивності потоків загроз λ і ймовірності атак p_i.

Основним способом завдання інтенсивності потоків загроз λ і ймовірності атак p є отримання цих значень на основі наявної статистики загроз безпеки інформаційних систем, в яких реалізується система захисту. Якщо існує статистика для аналогічної інформаційної системи, то задавати вихідні

параметри для оцінки захищеності можна на її основі. При цьому бажано, щоб подібні інформаційні системи експлуатувалася провайдерами з подібною специфікою діяльності.

Однак при практичній реалізації такого підходу виникають наступні складності. По-перше повинен бути зібраний дуже великий матеріал про події в

цій галузі. По-друге даний підхід виправданий далеко не завжди. Якщо інформаційна система досить велика (містить багато елементів, розташована на великій території), має давню історію, то застосовується подібний підхід. Якщо ж система порівняно невелика і експлуатує новітні елементи технології (для яких поки немає достовірної статистики), оцінки загроз можуть виявитися недостовірними.

Статистика загроз періодично публікується досить авторитетними виданнями, тобто завжди існують вихідні дані для використання даного підходу для більшості додатків засобів захисту інформації. Зазвичай ця статистика доступна в Інтернеті на сайтах спеціалізованих організацій. Якщо ж необхідна статистика по загрозам безпеки відсутня, то можна скористатися одним з інших підходів.

2 Оптимістично-песимістичний підхід. В рамках даного підходу передбачено два різні способи.

Перший спосіб - це спосіб рівних інтенсивностей $\forall\ \lambda_i = \alpha$, $\alpha = const$. При цьому способі для розрахунку ефективності константа α може бути обрана будь-яка. У формулі (2) вона буде винесена за дужки і в кінцевому підсумку скоротиться, так що захищеність в даному випадку буде залежати тільки від збитків:

$$D = 1 - \frac{\sum_1^w (C_i * \lambda_i * (1 - p_i))}{\sum_1^w (C_i * \lambda_i)} = 1 - \frac{\sum_1^w (C_i * \alpha * (1 - p_i))}{\sum_1^w (C_i * \alpha)} = 1 - \frac{\alpha \sum_1^w (C_i * (1 - p_i))}{\alpha \sum_1^w C_i} = \quad (2.1)$$

$$= 1 - \frac{\sum_1^w (C_i * (1 - p_i))}{\sum_1^w C_i}.$$

Другий спосіб – це спосіб пропорційності збиткам $\lambda_i = \alpha * C_i$, $\alpha = const$. При цьому способі передбачається, що чим більше збитки від злому, тим частіше здійснюються спроби несанкціонованого доступу до цієї

інформації. Тобто інтенсивності потоків загроз прямо пропорційні збиткам. В цьому випадку захищеність буде залежати від квадрата збитків:

$$D = 1 - \frac{\sum_{1}^{w}(C_i * \lambda_i * (1 - p_i))}{\sum_{1}^{w}(C_i * \lambda_i)} = 1 - \frac{\sum_{1}^{w}(C_i * \alpha * C_i * (1 - p_i))}{\sum_{1}^{w}(C_i * \alpha * C_i)} = 1 - \frac{\alpha\sum_{1}^{w}(C_i^2 * (1 - p_i))}{\alpha\sum_{1}^{w}C_i^2}$$
$$= 1 - \frac{\sum_{1}^{w}(C_i^2 * (1 - p_i))}{\sum_{1}^{w}C_i^2}. \qquad (2.2)$$

3 Метод експертної оцінки.

Експертна оцінка вихідних параметрів для розрахунку захищеності може здійснюватися з використанням так званої дельфійскої групи. Дельфійська група - це група експертів, створена з метою збору інформації з певних джерел з визначеної проблеми.

При цьому необхідно задати лінгвістичний словник можливих оцінок експертів, визначити набір питань і умовних значень кваліфікацій окремих експертів. Після визначення всіх вхідних змінних здійснюється почергове опитування кожного експерта. Після опитування всіх експертів з урахуванням їхньої кваліфікації визначається загальна оцінка групи та узгодженість (достовірність) відповідей для кожного питання.

Експерт оцінює ефективність (ймовірність) нейтралізації загрози елементами захисту p_i і ймовірність появи загроз Q_i. Ймовірності експерт задає лінгвістичними оцінками: відмінно, добре, задовільно, погано, не відображає; ймовірно, близько до нуля, близько до одиниці, досить імовірно і т.п. Потім ці лінгвістичні оцінки за допомогою словника перекладаються в числа p_i і Q_i в діапазоні [0; 1].

Для визначення ймовірності появи загрози можлива оцінка ймовірності появи загрози і-того виду в загальному потоці загроз:

$$Q_i = \frac{\lambda_i}{\sum \lambda_i}. \qquad (2.3)$$

Виходячи із заданої кваліфікації експертів, розраховується їх вага (значимість) в групі за формулою:

$$\kappa_e = \frac{S_e}{\sum S_e}, \qquad (2.4)$$

де S_e - кваліфікація експерта, що задається в деякому діапазоні, наприклад, від 0 до 10 в залежності від досвіду, освіти та інших якостей експерта. Потім оцінки підсумовуються з урахуванням ваги експертів:

$$p_i = \sum p_{ie} * k_e,$$
$$Q_i = \sum Q_{ie} * k_e, \qquad (2.5)$$

де p_{ie} і Q_{ie} - оцінка ймовірностей відображення і появи загроз, зроблені одним експертом;

k_e - вага експерта в групі.

Після розрахунку загальної оцінки всієї групи розраховується узгодженість відповідей, яка може використовуватися для оцінки достовірності результатів. Узгодженість розраховується за допомогою середньоквадратичного відхилення і виражається у відсотках.

Максимальна узгодженість досягається при однакових значеннях оцінок експертів і в цьому випадку дорівнює 100%. Мінімальна узгодженість досяжна при максимальному розкиді оцінок експертів.

При визначенні відповідності між інтенсивністю загроз і ймовірністю їх нейтралізації потрібно враховувати, що, якщо в системі реалізовано декілька механізмів, які захищають ІС від певної атаки, ймовірність подолання захисту розраховується наступним чином.

Якщо $p_к$ є ймовірність нейтралізації і-тої загрози кожним засобом захисту, то ймовірність злому системи буде:

$$\overline{p}_i = \prod_k (1 - p_k) \tag{2.6}$$

а ймовірність нейтралізації загрози системою захисту

$$p_i = 1 - \overline{p}_i \tag{2.7}$$

На даному кроці описуються цілі створення інформаційної системи, її межі, інформаційні ресурси, вимоги в області ІБ та компонентів управління інформаційною системою і режимом ІБ.

2.1.2 Розрахунок величини збитків від успішної реалізації загроз

Найважливішою характеристикою об'єкта, що захищається (як наслідок, і системи захисту) є вартість збитків від злому. Розглянемо можливі методи

визначення збитків. Метод дозволяє встановити цінність ресурсів. Цінність фізичних ресурсів в даному методі залежить від ціни їх відновлення в разі руйнування. Цінність даних та програмного забезпечення визначається в наступних ситуаціях:

1) недоступність ресурсу протягом певного періоду часу;

2) руйнування ресурсу - втрата інформації, отриманої з часу останнього резервного копіювання, або її повне руйнування;

3) порушення конфіденційності у випадках несанкціонованого доступу штатних співробітників або сторонніх осіб;

4) модифікація даних - розглядається для випадків дрібних помилок персоналу (помилки вводу), програмних помилок, навмисних помилок;

5) наявність помилок, пов'язаних з передачею інформації: відмова від доставки, недоставляння інформації, доставка за неправильною адресою. Для оцінки можливого збитку рекомендується скористатися деякими з перерахованих критеріїв:

1) шкоди репутації організації;
2) порушення чинного законодавства;
3) шкоди для здоров'ю персоналу;
4) збитки, пов'язані з розголошенням персональних даних окремих осіб;
5) фінансові втрати від розголошення інформації;
6) фінансові втрати, пов'язані з відновленням ресурсів;
7) втрати, пов'язані з неможливістю виконання зобов'язань;
8) дезорганізація діяльності.

Вартість втрати інформації C_i:

$$C_i = \min(c_i * v * t_j , c_i * V_i), \quad (2.8)$$

де c_i -питома ціна інформації;

v - швидкість отримання / спотворення / знищення інформації;

t - час знаходження суб'єкта в системі;

V_i - обсяг інформації.

Витрати від неможливості отримання доступу до інформації:

$$C_i = c_i * t , \quad (2.9)$$

де c_i -питома ціна недоступності інформації;

t - час відновлення системи.

Щоб точніше визначити збиток в результаті реалізації загроз інформації необхідно використовувати різні принципи класифікації загроз і виділити той принцип класифікації який більшою мірою характеризує величину збитків.

Існують різні класифікації загроз:

1) за принципами і характером впливу на систему;
2) за використовуваними технічними засобами;
3) за цілями атаки і т.ін.

Очевидно, що величину збитків C_i зручніше задавати для загроз, класифікованих за цілями атаки. Що стосується характеристики інтенсивності загроз, то вона визначається за допомогою засобів аудиту та моніторингу мережі, які розрізняють загрози за принципами і характером впливу на систему (механізму атаки, способом проникнення). Ймовірність відображення загрози засобами захисту p_i визначається у відповідності з тими механізмами, які реалізовані в кожному засобі. Причому кожен із механізмів в загальному випадку може відображати кілька видів атак.

Завдання відповідності між вартістю втрат і інтенсивністю загроз можна здійснювати таким чином:

1 Статистичний підхід. З аналізу статистики можна виявити ймовірності нанесення певних видів збитку при певних видах зломів. Однак на практиці далеко не завжди подібна статистика існує, зокрема, при впровадженні нових технологій захисту інформації, нових версій ОС або додатків і т.д., тому що для її збору потрібен якийсь час. У цьому випадку може використовуватися песимістичний підхід.

2) Песимістичний підхід. Якщо немає достатньої статистики, можна скористатися іншим способом. Будемо вважати, що при проникненні в систему зловмисник завдає найбільшої шкоди, якої він тільки може заподіяти.

Саме цей підхід використовується для визначення величини збитків у випадку реалізації хоча б однієї із загроз. До того ж, як показує практика, при подоланні зловмисником хоча б одного з бар'єрів захисту, загальний рівень захищеності всієї системи різко знижується, що може привести до її повної компрометації. Виходячи з цих переконань наш підхід до оцінки збитку цілком обґрунтований, і рівень втрат дорівнюватиме максимальному за будь-яких видів атак і порушень.

На другому кроці при оцінці вартості СЗІ може використовуватися 2 підходи:

1) Перший підхід - назвемо його наукоподібним - полягає в тому, щоб освоїти, а потім застосувати на практиці заходи безпеки, а для цього залучити

керівництво організації до оцінки вартості інформації, що захищається, визначення ймовірностей потенційних загроз і вразливостей, а також потенційного збитку. Якщо інформація не коштує нічого, істотних загроз для інформаційних активів провайдера немає, а потенційний збиток мінімальний - і керівництво це підтверджує - проблемою ІБ можна не займатися. Якщо ж інформація коштує певних грошей, загрози і потенційний збиток відомі, то зрозумілі і рамки бюджету на систему ІБ. При цьому можна залучити керівництво провайдера до усвідомлення проблем ІБ та побудови системи захисту інформації, заручитися його підтримкою. В якості такого підходу для оцінки вартості системи захисту може використовуватися дана методика без введення обмежень на параметр $Ц_{СЗІ}$, а орієнтуватися тільки на необхідний рівень ефективності;

2) Другий підхід (назвемо його практичним) полягає в наступному: можна знайти варіант доцільної вартості системи захисту інформації. Адже існують аналогічні варіанти в інших областях, де значимі для бізнесу події носять імовірнісний характер. Тому експерти-практики в галузі захисту інформації знайшли якийсь оптимум, вартість системи ІБ повинна становити приблизно 10-20% від вартості ІС - залежно від рівня конфіденційності інформації. Це і є та сама оцінка на основі практичного досвіду (best practice), на яку можна покластися. Очевидно, що другий підхід не позбавлений недоліків. Проте за допомогою цього підходу можна заздалегідь прогнозувати обсяг бюджету на ІБ і знизити витрати на послуги зовнішніх консультантів.

2.1.3 Розрахунок коефіцієнтів ефективності та вибір СЗІ

Розглянемо ефективність системи захисту інформації з точки зору ризику. Зауважимо, що використання теорії ризиків для оцінки рівня ефективності на сьогоднішній день є найбільш часто використовуваним на практиці підходом. Ризик (R) - це потенційні втрати від загроз захищеності інформації:

$$R(p) = C_{інф} * p_{зл.} \qquad (2.10)$$

З іншого боку, можна розглядати ризик як втрати в одиницю часу:

$$R(\lambda)=C_{інф}*\lambda_{зл}\ , \tag{2.11}$$

де $\lambda_{взл}$ - інтенсивність потоку зломів (під зломом будемо розуміти вдалу спробу реалізації загрози інформації).

Ці дві формули пов'язані наступним співвідношенням:

$$p_{ЗЛ}=\frac{\lambda_{зл}}{\Lambda}\ , \tag{2.12}$$

де Λ - загальна інтенсивність потоку несанкціонованих спроб порушення основних властивостей інформації зловмисниками.

В якості основного критерію захищеності будемо використовувати коефіцієнт ефективності системи захисту інформації (D), що показує відносне зменшення ризику в захищеній інформаційній системі провайдера в порівнянні з незахищеною системою.

$$D\%=\left(1-\frac{R_{зах}}{R_{нез}}\right)*100\%\ , \tag{2.13}$$

де $R_{зах}$ - ризик в захищеній системі;

$R_{нез}$ - ризик в незахищеній системі.

Таким чином, в даному випадку завдання оптимізації виглядає наступним чином:

$$\begin{cases} D(C_{інф}, p_{зл}) \to \max; \\ Ц_{сзі} \to \min; \\ П_{сзі} \to \min\ . \end{cases} \tag{2.14}$$

Для вирішення цього завдання зведемо її до однокритеріальної за допомогою введення обмежень. В результаті отримаємо:

$$\begin{cases} D(C_{інф}, p_{зл}) \to \max; \\ Ц_{сзі} \le Ц_{зад}; \\ П_{сзі} \ge П_{зад}. \end{cases}, \qquad (2.15)$$

де $Ц_{зад}$ і $П_{зад}$ - задані обмеження на вартість системи захисту і продуктивність системи.

Цільова функція обрана виходячи з того, що саме вона відображає основне функціональне призначення системи захисту - забезпечення безпеки інформації.

Продуктивність системи $П_{СЗІ}$ розраховується із застосуванням моделей і методів теорії масового обслуговування і теорії розкладів (в залежності від того, захищається чи система оперативної обробки, або реального часу). На практиці можливе завдання обмеження за продуктивністю (вплив на завантаження обчислювального ресурсу системи, що захищається). В цьому випадку завдання оптимізації буде виглядати наступним чином:

$$\begin{cases} D(C_{інф}, p_{зл}) \to \max; \\ Ц_{сзі} \to \min; \\ dП_{сзі} \to \min, \end{cases} \qquad (2.16)$$

і після її зведення до однокритеріальної:

$$\begin{cases} D(C_{інф}, p_{зл}) \to \max; \\ Ц_{сзі} \le Ц_{зад}; \\ dП_{сзі} \le dП_{зад}. \end{cases} \qquad (2.17)$$

де $Ц_{зад}$ і $dП_{зад}$ – задані обмеження на вартість системи захисту і зниження продуктивності.

Такий принцип зведення задачі до однокрітеріальної доцільний, тому що в будь-якому технічному завданні на розробку системи захисту вказується, якою мірою система захисту повинна впливати на продуктивність системи. Як правило, впровадження системи захисту не повинно знижувати продуктивність системи більш ніж на 10%. Крім того, зазвичай вводиться обмеження на вартість системи захисту.

Якщо розраховане значення коефіцієнта захищеності (D) не задовольняє вимогам до системи захисту, то в допустимих межах можна змінювати задані обмеження і вирішити задачу методом послідовного вибору поступок, приклад якого буде розглянуто нижче. При цьому задається приріст вартості і зниження продуктивності:

$$Ц^*_{зад} = Ц_{зад} + \Delta Ц\,, \qquad (2.18)$$

$$П^*_{зад} = П_{зад} - \Delta П \text{ або } dП^*зад = dП_{зад} + \Delta dП. \qquad (2.19)$$

У такому вигляді задача вирішується в результаті реалізації ітераційної процедури шляхом відсіювання варіантів, що не задовольняють обмеження, і подальшого вибору з решти варіанта з максимальним коефіцієнтом ефективності.

Тепер виразимо коефіцієнт захищеності через параметри загроз. У загальному випадку в системі присутні безліч видів загроз. В цих умовах задамо наступні величини:

W – кількість видів загроз, що впливають на систему;

$C_i (i = \overline{1,w})$ - вартість (збитки) від злому і-того виду;

$\lambda_i (i = \overline{1,w})$ - інтенсивність потоку зломів і-того виду;

$Q_i (i = \overline{1,w})$ - ймовірність появи загроз і-того виду в загальному потоці спроб реалізації загроз;

$p_i (i = \overline{1,w})$ - ймовірність нейтралізації загроз і-того виду системою захисту.

Відповідно, для коефіцієнта втрат від зломів системи захисту маємо:

$$R(p) = \sum R_i(p) = \sum C_i * p_{зл\_i}, \tag{2.20}$$

де R_i (p) - коефіцієнт втрат від злому і-того типу; показує, які в середньому втрати припадають на один злом і-того типу. Для незахищеної системи $P_{загрози\_i}=Q_i$, для захищеної системи:

$$P_{загрози\_i} = Q_i*(1-p_i). \tag{2.21}$$

Відповідно, для коефіцієнта збитків від зломів системи захисту в одиницю часу маємо:

$$R(\lambda) = \sum_1^w R_i(\lambda) = \sum_1^w C_i * \lambda_{загрози\_i}, \tag{2.22}$$

де $R_i(\lambda)$ - коефіцієнт збитків від зломів і-того типу в одиницю часу.

Для незахищеної системи:

$$\lambda_{загрози\_i} = \lambda_i, \tag{2.23}$$

для захищеної системи

$$\lambda_{загрози\_i} = \lambda_i * (1 - p_i). \tag{2.24}$$

Відповідно, із (2.1) маємо:

$$D = 1 - \frac{\sum_1^w (C_i * Q_i * (1 - p_i))}{\sum_1^w (C_i * Q_i)} = 1 - \frac{\sum_1^w (C_i * \lambda_i * (1 - p_i))}{\sum_1^w (C_i * \lambda_i)} \tag{2.25}$$

Якщо в якості вихідних параметрів задані ймовірності появи загроз Q_i то коефіцієнт ефективності системи захисту зручно розраховувати через ймовірності появи загроз. Якщо ж в якості вихідних параметрів задані інтенсивності потоків загроз λ_i, то, коефіцієнт ефективності розраховується через інтенсивність.

Тому при використанні будь-якого математичного методу проектування системи захисту необхідно задавати певні вихідні параметри для оцінки її ефективності. Однак саме з цим пов'язані основні проблеми формалізації задачі синтезу системи захисту.

2.1.4 Використання методу поступок при виборі оптимального варіанту захисту

Проаналізувавши характер залежностей основних параметрів, що характеризують систему захисту, від складності системи, визначили, що вартість системи захисту зростає необмежено, а продуктивність знижується до нуля.

Отже, при проектуванні системи захисту доцільно дослідити можливість використання менш складних систем захисту і, задавши певний проміжок зниження коефіцієнта ефективності (dD), вибрати систему, рівень ефективності якої задовольняє отриманим (D-dD). Звичайно, якщо такі є. При цьому може бути отриманий відчутний виграш у ціні і продуктивності.
У цьому й полягає застосування відомого методу послідовних поступок при виборі оптимальної системи захисту.

Метод послідовних поступок являє собою процедуру, використовуючи яку розробник, даючи допустимі збільшення одним параметрам (зокрема, задаючи зниження коефіцієнта захищеності), аналізує зміну інших, приймаючи рішення про допустимість поступок.

Таким чином, весь процес аналізу рівня безпеки умовно можна розділити на етапи збору та аналізу отриманих даних і модифікації параметрів системи захисту.

2.2 Впровадження запропонованої методики для оцінки ефективності системи захисту інформації провайдера доступу до мережі Інтернет

2.2.1 Загальна характеристика інформаційної системи провайдера

Дана методика дозволяє оцінити ефективність системи захисту інформації. Ця система використовується провайдером доступу для захисту його мережі та інформації, що циркулює в цій мережі, від загроз зі сторони зловмисників. Методика оцінює ефективність СЗІ в аспекті мережевого захисту, так як основою діяльності провайдера є надання послуг доступу до мережі Інтернет і мережевий захист є важливим для даного типу організацій.

Інформаційна система провайдера, що зображена на рисунку 2.1, представляє собою мережу невеликої організації, з декількома відділами, співробітниками та клієнтами, що можуть віддалено підключатись до мережі провайдера.

Система складається з наступних елементів:

1) точка доступу VPN для віддаленого підключення до мережі провайдера клієнтів;

2) мережевий екран з підтримкою proxy та NAT;

3) IDS-система виявлення вторгнень;

4) сервер оновлень ПЗ, клієнтських ОС;

5) сервер антивірусного захисту;

6) сервер баз даних;

7) внутрішня локальна мережа з робочими станціями співробітників провайдера;

8) файл-сервер, на якому зберігаються документи відділів та інформація загального користування;

9) веб – сервер, який приймає HTTP-запити від клієнтів, зазвичай веб-браузерів, і видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом або іншими даними.

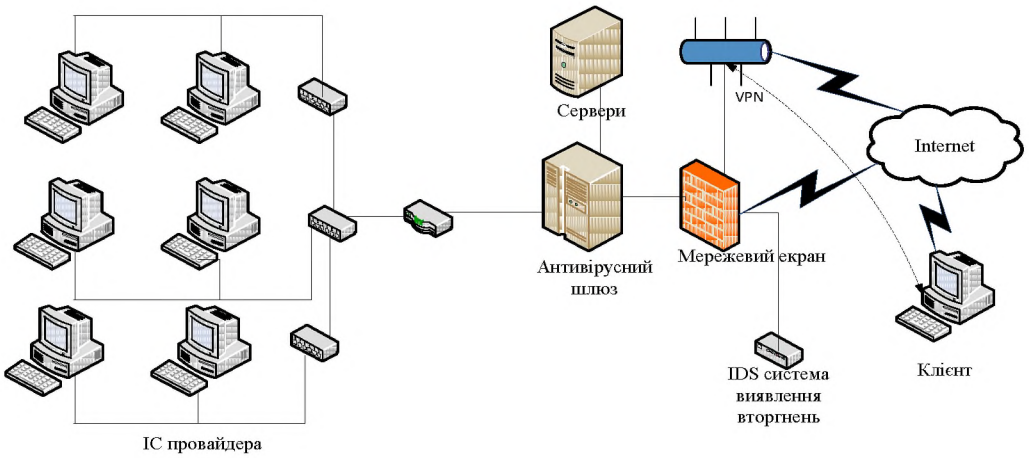

Рисунок 2.1 - Інформаційна система провайдера

На комп'ютерах співробітників встановлена операційна система MS Windows 2012 з останнім набором оновлень і стандартним ПЗ від Microsoft, що входять в комплект поставки ОС. На серверах встановлена ОС Linux.

Для даної мережі інформація, що захищається, зберігається як на локальних комп'ютерах співробітників, так і на серверах. Клієнти провайдера мають віддалений доступ до даної мережі. Будемо вважати, що кількість клієнтів для даного провайдера складає 2000 чоловік.

В даному прикладі оцінка захищеності СЗІ буде здійснюватися тільки в мережевому аспекті, із захистом як від зовнішнього так і від внутрішнього зловмисника. Розглянемо загрози зі сторони зловмисника.

2.2.2 Визначення переліку загроз, які враховуються при розрахунку

В першу чергу нам потрібно оцінити інформаційні загрози, ймовірності їх нейтралізації СЗІ, а також величину втрат у результаті реалізації загроз. Для

отримання точних оцінок потрібно найбільш повно перерахувати загрози мережевої безпеки для описаної мережі. Важливо виявити та ідентифікувати

повний список загроз, так як саме в цьому випадку буде отримана точна оцінка. Для переліку загроз можна використовувати як стандарти в галузі безпеки, які містять в собі списки загроз і контрзаходів щодо захисту від них, так і особистий досвід із захисту в даній області.

Загрози, які властиві мережі провайдера в області мережевого захисту, наступні:

1) недоступність даних;
2) неавторизоване використання ІТ системи;
3) порушення конфіденційності даних;
4) зловживання правами користувачів та адміністраторів;
5) віруси;
6) DoS атаки;
7) підбір паролів;
8) IP Spoofing;
9) захват мережних підключень;
10) різні види сканування мережі.

2.2.3 Аналіз механізмів захисту інформації.

2.2.3.1 Мережеві екрани

Провайдер доступу до мережі Інтернет надає доступ до мережі своїм клієнтам, при цьому він повинен забезпечувати можливість використання всіх привілеїв і вигод мережі Internet з мінімальним ризиком для своєї діяльності. Тому на перший план виходить проблема забезпечення безпеки в ІС провайдера з боку мережевого впливу.

Основними засобами захисту ІС провайдера є міжмережеві екрани. У літературі можна зустріти їх синоніми такі як: брандмауер, firewall, фільтруючий маршрутизатор тощо. Мережеві екрани є лише інструментом системи безпеки. Вони надають певний рівень захисту і є засобом реалізації політики безпеки на мережевому рівні. Рівень безпеки, який надає мережевий екран, може змінюватись в залежності від вимог безпеки. Мережевий екран є одним з декількох механізмів, використовуваних для управління і спостереження за доступом до і з мережі з метою її захисту.

Система firewall заміняє маршрутизатор або зовнішній шлюз мережі (gateway).

Захищена частина мережі розміщується за ним. Пакети, адресовані Firewall, обробляються локально, а не тільки переадресовуються. Пакети ж, які адресовані

об'єктам, розташованим за Firewall, не доставляються. Схема взаємодії Firewall з локальною мережею і зовнішньою мережею Інтернет відображена на рисунку 2.2

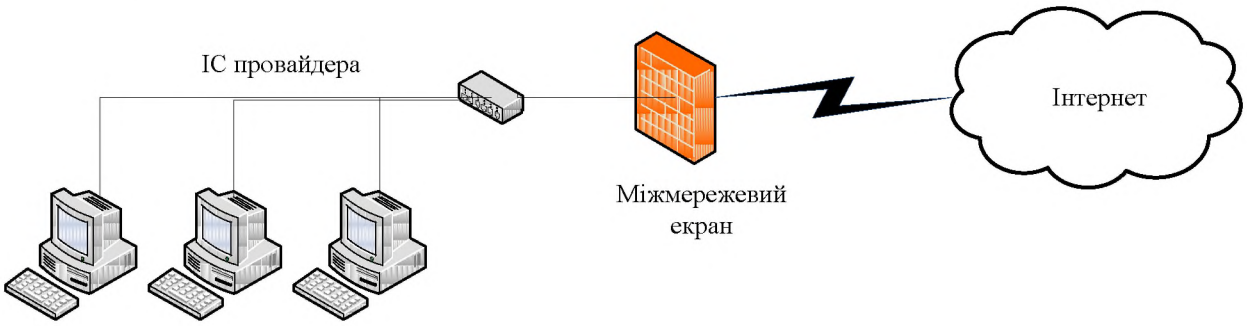

Рисунок 2.2- Схема Firewall

Найчастіше МЕ являє собою мережеву станцію з двома і більше мережевими інтерфейсами. При цьому через один інтерфейс здійснюється зв'язок з Інтернет, а через другий - із захищеною мережею. МЕ поєднує функції маршрутизатора-шлюзу, екрана та управління екраном.

Недоліки програми FireWall походять від її переваг, ускладнюючи доступ ззовні, система робить важким і доступ назовні. Для багатьох програм, які працюють на нестандартних портах і не підтримують проксі-сервера, для установки з'єднання доведеться або відкривати порти, або відмовитися від їх використання. В цілях безпеки інформації захищена мережа не може мати виходів у зовнішній світ окрім системи МЕ, в тому числі і через модеми. Для користувачів захищеної мережі створюються спеціальні входи для FTP, telnet та інших послуг. При цьому не вводяться обмеження по транспортуванню файлів в захищену мережу і блокується передача будь-яких файлів із цієї мережі.

У більшості випадків до МЕ висувається ряд вимог :

1) фільтрація пакетів на мережевому рівні;
2) фільтрація пакетів на прикладному рівні;
3) налаштування правил фільтрації і адміністрування;
4) використання стійких протоколів для аутентифікації по мережі;
5) ведення журналів аудиту.

Для виконання перших трьох вимог в МЕ використовуються наступні складові:

1) фільтруючі маршрутизатори;

2) шлюзи мережевого рівня;

3) шлюзи прикладного рівня(проксі-сервери).

Фільтруючі маршрутизатори є найпростішим компонентом мережевого екрану. Маршрутизатор передає дані в обох напрямках між двома (або більше) різними мережами. Звичайний маршрутизатор приймає пакет з мережі А і "переадресує" його до місця призначення в мережі В. Фільтруючий маршрутизатор робить те ж саме, але вирішує не тільки як пересилати пакет, але також чи потрібно цей пакет посилати. Це робиться шляхом встановлення фільтрів, за допомогою яких маршрутизатор вирішує, що робити конкретно з даним пакетом.

При підготовці маршрутизатора для фільтрації пакетів, важливі такі критерії політики відбору: IP-адреси відправника та одержувача, номера TCP-портів відправника і одержувача, і напрям передачі пакетів (т. е., A-> B або B-> A). Якщо маршрутизатор фільтрує тільки вихідні пакети, тоді він є зовнішнім по відношенню своїх фільтрів і може бути більш вразливим для атак. Процес формування фільтра може бути дуже важким і вимагати знання типу послуг (протоколів), які будуть фільтруватися.

Шлюзи мережевого рівня є пристроєм або ПЗ, що реалізує технологію NAT – це механізм в мережах TCP / IP, що дозволяє перетворювати IP-адреси транзитних пакетів. Перетворення адрес методом NAT може проводитися майже будь-яким маршрутизуючим пристроєм – маршрутизатором, сервером доступу, міжмережевим екраном. Суть механізму полягає в заміні зворотньої (source) адреси при проходженні пакета в одну сторону і зворотної заміні адреси призначення (destination) у відповідному пакеті.

Переваги NAT:

1) дозволяє використовувати меншу кількість IP-адрес, транслюючи декілька внутрішніх приватних IP-адрес в один зовнішній публічний IP-адрес;

2) дозволяє запобігти зверненню ззовні до внутрішніх хостів, залишаючи можливість звернення зсередини назовні. При ініціалізації з'єднання зсередини мережі створюється трансляція. Відповідні пакети, що надходять ззовні, відповідають створеній трансляції і тому пропускаються. Для решти пакетів, що надходять ззовні, відповідної трансляції не існує, тому вони не пропускаються.

Недоліки NAT:

1) не всі протоколи можуть «подолати» NAT. Деякі (наприклад, IPSec) не в змозі працювати, якщо на шляху між взаємодіючими хостами є трансляція адрес;

2) через трансляції адрес «багато в один» з'являються додаткові труднощі з ідентифікацією користувачів. Необхідно зберігати повні журнали аудиту трансляцій.

Проксі-сервер є засобом переадресації прикладних послуг через одну машину. Замість безпосереднього з'єднання із зовнішнім сервером, клієнт підключається до проксі-сервера, який в свою чергу ініціює з'єднання із зовнішнім сервером. Залежно від використовуваного проксі-сервера можна конфігурувати внутрішніх клієнтів так, щоб вони здійснювали це перенаправлення автоматично, без інформування користувача.

Застосування проксі-сервера надає суттєві переваги в забезпеченні безпеки. Є можливість додавання списків доступу для протоколів, що вимагають від користувачів або систем забезпечення певного рівня аутентифікації перш ніж доступ буде наданий. Проксі-сервери можуть також конфігуруватися для шифрування потоків даних на основі різноманітних параметрів. Провайдер може використовувати цю особливість, щоб дозволити криптографічні з'єднання між двома вузлами, один з яких розміщений в Інтернет. Мережеві екрани зазвичай розглядаються як засіб блокування доступу для зловмисників, але вони часто використовуються в якості способу доступу авторизованих користувачів до вузла.

Найкращим варіантом мережевого екрану вважається комбінація двох екрануючих маршрутизаторів і одного або більше проксі-серверів в мережі між маршрутизаторами. Така схема дозволяє зовнішньому маршрутизатору блокувати будь-які спроби використання нижчого IP-рівня для порушення безпеки (IP-

spoofing), в той же час проксі-сервер захищає уразливості на рівні верхніх протоколів. Метою внутрішнього маршрутизатора є блокування всього трафіку крім спрямованого на вхід проксі-сервера. Якщо реалізована ця схема, може бути забезпечений високий рівень безпеки.

2.2.3.2 Системи IDS

Системи виявлення атак IDS вирішують задачу моніторингу інформаційної системи на мережевому, системному і прикладному рівнях з метою виявлення порушень безпеки та оперативного реагування на них. Мережеві IDS є джерелом даних для аналізу мережевих пакетів, а IDS системного рівня (хостової - host based) аналізують записи журналів аудиту безпеки ОС і додатків. При цьому методи аналізу (виявлення атак) залишаються загальними для всіх класів IDS.

Існуючі IDS можна розділити на два основні класи: одні застосовують статистичний аналіз, інші - сигнатурний аналіз. Статистичні методи базуються на припущенні про те, що активність зловмисника завжди супроводжується зміною поведінки користувачів, програм і апаратури.

Основний принцип функціонування IDS, що застосовують сигнатурний аналіз - порівняння відбуваються в системі / мережі подій з сигнатурами відомих атак - той же, що використовується в антивірусному ПЗ.

Сучасні IDS починають відчувати серйозні проблеми з продуктивністю вже при швидкості 100 Мб / с в мережах. Тому в більшості випадків доцільно вдаватися для виявлення атак до аналізу мережевого трафіку.

Відповідні продукти діляться на системи IDS на базі мережі та на базі хоста. Обидві системи намагаються виявити вторгнення, але оброблюють абсолютно різні дані. Система IDS на базі мережі для розпізнання атаки зчитує потік даних, подібно аналізатору. Вона складається головним чином з реєструючих всі мережеві пакети сенсорів, інтерфейс яких підключено до призначеного для аналізу або копіювання порту комутатора.

Система IDS на базі хоста використовує агентів. Вони працюють як невелике додаткове програмне забезпечення на контрольованих серверах або

робочих місцях і аналізують активність зловмисника на підставі даних журналів реєстрацій та аудиту в пошуках ознак небезпечних подій.

Ефективність системи IDS на базі мережі багато в чому залежить від актуальності шаблону. Оскільки нові вразливі місця виявляються щодня і зловмисники можуть ними скористатися, система IDS повинна бути завжди актуальною. Якщо її шаблони оновлюються тільки раз на місяць, то потрібно враховувати, що в проміжку між оновленнями можуть з'явитися нові атаки, що не будуть розпізнаватись системою. Найбільша проблема систем виявлення атак полягає у високих операційних витратах через велику кількість помилкових сигналів тривоги. Вони виникають, якщо шаблон зі списку зустрічається в звичайному потоці даних, навіть при відсутності атаки, або коли звичайні додатки використовують незначні модифікації стандартних протоколів, що в кінцевому підсумку призводить до подачі системою IDS сигналу тривоги. Щоб уникнути хибних сигналів тривоги застосовуються різні підходи. Перш за все можна використовувати комплексні шаблони: вірогідність того, що вони з'являться в звичайному трафіку, дуже мала. Однак комплексні шаблони погіршують продуктивність сенсора, і навряд чи цей шлях є перспективним - адже виробники постійно намагаються перевершити і так вже досить високу максимальну пропускну здатність сенсорів.

Важливими ознаками якісної системи виявлення атак є не тільки те, який обсяг трафіку вона здатна контролювати і аналізувати, а, перш за все, точність виявлення та наявні інструменти в адміністратора для додаткового спостереження та аналізу вручну.

При проектуванні СЗІ із застосуванням IDS, повинні враховуватися обмеження наявних систем. Найчастіше виробники вказують граничні значення: число відомих шаблонів або максимально аналізовану пропускну здатність. Проте зазвичай вони не вказують, як багато або які саме вторгнення система IDS не може виявити. Проблема знову полягає в технології виявлення, оскільки і при аналізі протоколів вона частково базується на шаблонах. Коли в потоці даних присутній певний шаблон, атака розпізнається. Але якщо атака відбувається, а

шаблон при цьому не з'являється, то система її не виявляє. Часто системи виявляють вторгнення за характерною послідовності байтів при атаці за допомогою відомого автоматизованого інструменту вторгнення, так званого експлоїта. Якщо зловмисник має достатній досвід, він може створити такий інструмент і провести атаку так, щоб вона залишилася непоміченою з боку системи IDS на базі шаблонів.

Багато вторгнення відбуваються на рівні програми і, хоча вони використовують загальний основний принцип, є ще й дуже індивідуальними. Немає жодних шаблонів, які можна було б розпізнати на мережевому рівні. Відповідно потрібно з обережністю користуватися статистичними даними та дослідженнями, де дається оцінка системи IDS на базі глобально розподілених сенсорів. Висловлювання про атаки переважно через порт 80 дійсні тільки щодо деяких з них - на базі готових експлоітів, але не стосуються індивідуальних атак, специфічних для додатків. Такі атаки сенсори системи IDS виявляють лише у виняткових випадках.

IDS починають все ширше впроваджуватися в практику забезпечення безпеки провайдерів. Проте є ряд проблем, з якими неминуче стикаються провайдери, які створюють у себе систему виявлення атак. Ці проблеми істотно ускладнюють, а часом і зупиняють процес впровадження IDS. Наведемо деякі з них:

1) велика вартість комерційних IDS;

2) мала ефективність сучасних IDS, що характеризуються великою кількістю помилкових спрацьовувань і неспрацьовування (false positives and false negatives);

3) вимогливість до ресурсів і незадовільна продуктивність IDS вже на швидкості 100 Мбіт / с в мережах;

4) недооцінка ризиків, пов'язаних з мережевими атаками;

5) відсутність в провайдера методики аналізу ризиків та управління ними, що першкоджає керівництву адекватно оцінювати величину ризику і обгрунтовувати вартість реалізації контрзаходів;

6) необхідність у високій кваліфікації експертів з виявлення атак, без якої неможливо впровадження і розгортання IDS.

Рівень захищеності, що забезпечується IDS, на 80 відсотків залежить від компетентності адміністраторів і виходу оновлень сигнатур. Є випадки коли системи IDS не діяли через відсутність відповідного налаштування під конкретну систему, знижуючи тим самим доцільність свого застосування фактично до нуля.

2.2.3.3 Антивірусні засоби захисту

Зі звіту за підсумками 2019 року, наведеного на рисунку 2.3 - дослідження (опитування) компанії Ernst & Young, явно видно, що більшість опитаних фахівців, проблему вірусної небезпеки поставили саме на перше місце.

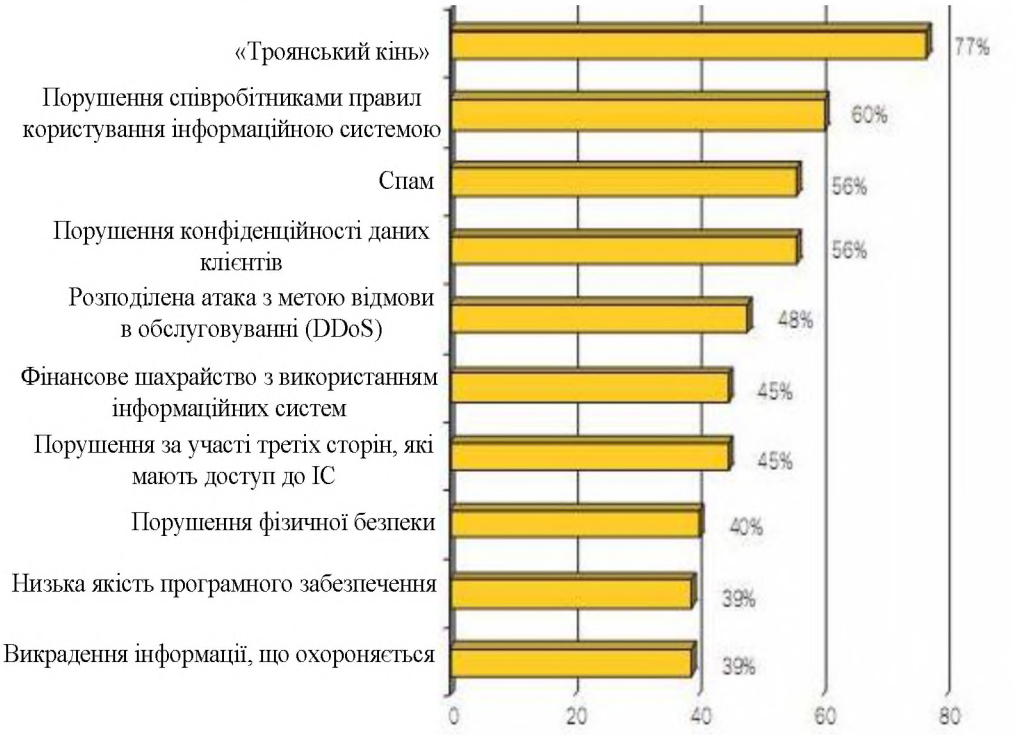

Рисунок 2.3 – Основні загрози для діяльності провайдера

Мережі провайдерів доступу до мережі Інтернет знаходяться в постійному розвитку, відповідно зростає і число точок проникнення вірусів в їх мережі. Основними точками проникнення є, в першу чергу – електронна пошта, шлюзи (центральна точка входу в мережу провайдера) і сервери Інтернету (Web browsing - різні CGI скрипти та інший шкідливий код, який скачується користувачем).

Одночасно з розвитком мережі провайдера, необхідно, щоб система антивірусного захисту випереджала її розвиток на крок або ж змінювалася

одночасно і відповідно з розширенням кількості та якості послуг, що надаються клієнтам даної мережі.

Ідеальним вирішенням проблеми вірусів є запобігання інфікування: не слід допускати початкового проникнення вірусу в комп'ютерну систему провайдера. Цій меті в загальному досягти неможливо, хоча зроблені заходи можуть знизити кількість успішно завершених вірусами атак. Майже ідеальний підхід повинен забезпечувати виконання наступних вимог.

Виявлення. Якщо зараження відбулося, воно має бути негайно виявлено з встановленням місця знаходження вірусу.

Ідентифікація. Як тільки зараження вірусом виявлено, необхідно ідентифікувати тип вірусу, інфікованих програм.

Видалення. Як тільки вірус ідентифікований, слід видалити всі сліди вірусу з інфікованих програм і відновити програми до їх початкового вигляду. Важливо видалити вірус з усіх інфікованих систем, щоб вірус не поширювався далі.

Якщо вірус виявлений, але його не вдається ідентифікувати або видалити із системи, альтернативою є видалення інфікованої програми з наступним її новим завантаженням з резервної копії.

Всі антивірусні програми поділяються на чотири покоління:

1) перше покоління: звичайні сканери.

2) друге покоління: евристичні аналізатори.

3) третє покоління: монітори.

4) четверте покоління: повнофункціональні системи захисту.

Антивірусні програми-сканери першого покоління для ідентифікації вірусів використовують характерні для відповідних вірусів сигнатури. Такі програми-сканери, що використовують сигнатури, можуть виявляти лише відомі віруси.

Сканери другого покоління вже не орієнтовані на конкретні сигнатури. Замість цього в них застосовується евристичний аналіз, за допомогою якого робиться висновок про можливу наявність у програмі вірусу. Одна з різновидів таких сканерів передбачає пошук в програмі фрагментів коду, характерного для вірусів.

Іншим підходом, що застосовується в антивірусних програмах другого покоління, є перевірка цілісності. З кожною програмою можна пов'язати контрольну суму. Якщо вірус інфікує програму, не змінюючи при цьому контрольної суми, то перевірка цілісності це виявить. Щоб протистояти вірусам, які при зараженні можуть змінювати відповідну контрольну суму, можна використовувати деяку функцію хешування з шифруванням. Ключ шифру зберігається окремо від програми, щоб вірус не зміг згенерувати новий хеш-код і зашифрувати його. Використання функції хешування з шифруванням замість звичайної контрольної суми не дає вірусу можливості модифікувати програму таким чином, щоб результат хешування після інфікування не змінювався.

Програми третього покоління представляють собою резидентні програми, що виявляють віруси по виконуваними ними діями, а не по їх структурі в інфікованої програмі. Перевагою таких програм є те, що для них не потрібно постійно оновлювати базу даних сигнатур для більшого числа вірусів. Замість цього достатньо визначити відносно невеликий набір дій, які характеризують можливі прояви вірусу.

Продукти четвертого покоління представляють собою пакети, які об'єднують в єдине ціле всі існуючі антивірусні технології. Такий підхід, крім виконання сканування і наявності компонентів, що дозволяють реєструвати певні дії вірусів, передбачає наявність засобів управління доступом, за допомогою яких можна обмежити можливості вірусів по проникненню в систему і по внесенню змін у файли з метою поширення вірусів під виглядом оновлення. З появою продуктів четвертого покоління з'явилася можливість побудови стратегії антивірусного захисту, яка є невід'ємною частиною загальних заходів щодо забезпечення захисту комп'ютерної системи провайдера.

Звичайна мережа провайдера включає в себе сотні робочих станцій, десятки серверів, активне і пасивне телекомунікаційне обладнання і, як правило, має дуже складну структуру. При цьому вартість обслуговування такої мережі катастрофічно зростає разом із збільшенням числа об'єктів мережі. Очевидно, витрати на антивірусний захист є не останнім пунктом у списку загальних витрат.

Однак існує принципова можливість їх зниження шляхом реалізації централізованої установки, управління і оновлення антивірусного комплексу захисту мережі провайдера.

Для того, щоб остаточно визначитися - якою має бути система антивірусного захисту ІС провайдера доступу до мережі Інтернет, необхідно визначити, що має в ходити в її функціональність. Для початку використовуються ті вимоги, які пред'являє до подібних систем міжнародний, найбільш авторитетний, стандарт в галузі управління інформаційною безпекою ISO 27001.

Якщо проаналізувати даний стандарт, то можна виділити ряд вимог, що пред'являються до самої системи антивірусної безпеки і до необхідних можливостей з управління даною системою:

1) відмовостійкість;

2) масштабованість, інтегрованість і можливість централізованого управління і оновлення;

3) робота антивірусних засобів в режимі реального часу і за розкладом;

4) оцінка нанесеного збитку і відновлення системи;

5) контроль над життєвим циклом вірусу і своєчасне інформування персоналу;

6) здатність перекривати всі потенційні канали проникнення вірусів в мережу провайдера;

Є також вимоги, які не описані стандартами, але на них завжди звертають увагу провайдери при побудові інформаційної системи. У першу чергу йдеться, наприклад, про продуктивність і зручність експлуатації антивірусних рішень. Список і розкриття цих вимог перераховані нижче.

Вартість рішення

Звичайно, вартість враховується при виборі рішення, адже це прямі витрати, які повинні забезпечити надійне функціонування всієї мережі провайдера. При цьому потрібно враховувати, що всі антивірусні рішення продаються на обмежений період часу, потім необхідно або оновлювати ліцензії, або продовжувати технічну підтримку.

Ліцензійна політика виробника

Потрібно відразу звернути увагу на ліцензійну політику виробника. Не існує гарантій, що, купивши ряд ліцензій, антивірус не відмовиться захищати всі об'єкти мережі провайдера, тому що їх виявиться значно більше, внаслідок використання будь-яких службових поштових скриньок.

Ефективність виявлення вірусів

Ефективність виявлення вірусів виправдовує фінансові витрати на придбання та експлуатацію антивірусного ПЗ.

Продуктивність

Якщо антивірусний захист «конфліктує» з продуктивністю системи, доставкою пошти або іншими ключовими аспектами сучасного процесу ділового спілкування, у кінцевого користувача з'являється бажання її відключити. Внаслідок чого, в будь-якому випадку рекомендується перед повноцінним впровадженням антивірусної системи виконати тестування на невеликій ділянці мережі.

Керованість всім антивірусним комплексом

Можливість централізованого адміністрування антивірусного програмного забезпечення надзвичайно актуальна, тому що не можна покладатися на те, що кінцеві користувачі будуть підтримувати працездатність та оновлення антивірусного захисту на своїх робочих станціях. При цьому буває так, що в результаті системного збою (не обов'язково самого антивірусного ПЗ) відбувається збій системи оновлення. Навіть подібні поодинокі випадки, серед сотень захищених об'єктів можуть призвести до непоправних наслідків.

Централізоване повідомлення та оповіщення

Якщо адміністратор антивірусної системи не зможе отримати єдину картину всіх вразливих точок мережі, то вони можуть випустити з уваги потенційну і, як правило, реальну вірусну атаку.

Таким чином на сьогоднішній день вірусні загрози становлять для ІС провайдера найбільшу небезпеку. Про це свідчить статистика порушень і

дослідження експертів в цій галузі. З цього можна зробити висновок, що забезпечення належного рівня антивірусного захисту в ІС провайдера має бути невід'ємною частиною загальної програми захисту, і проблеми вірусної активності повинні вирішуватися в першу чергу для забезпечення належного рівня гарантій безпеки.

2.2.3.4 VPN рішення

Для вирішення проблеми передачі інформації через відкриті канали Інтернет використовують VPN рішення. VPN-це об'єднання ряду локальних мереж, підключених до мережі загального призначення, в єдину віртуальну (логічно виділену) мережу.

При використанні VPN ресурси провайдера можуть бути легко об’єднані і використані з більшою ефективністю. Через те, що VPN може працювати через мережу Інтернет, у провайдера не виникає значних витрат, пов'язаних з купівлею додаткового обладнання та орендою ліній зв'язку. Використання виділених (орендованих) ліній зв'язку може призвести до підвищення витрат до сотень тисяч доларів, а такі витрати дуже складно виправдати.

До того ж головною перевагою VPN є можливість забезпечення безпеки безлічі комунікаційних потоків за допомогою одного механізму. При VPN-з'єднанні потоки даних, що використовують протокол TCP/IP, захищені від дій зловмисника.

За допомогою VPN можна уникнути низки загроз. VPN забезпечує цілісність та конфіденційність даних шляхом шифрування а також їх аутентифікацію за допомогою використання спеціальних протоколів і схем аутентифікації.

Також засоби VPN за рахунок приховування інформації, що стосується транспорту IP пакетів, захищені від ряду мережевих атак, таких як IP-spoofing, також вони захищені від атак типу man-in-the-middle.

Основні вимоги, які повинні виконувати рішення VPN, наступні:

1 Аутентифікація користувача. Засіб має аутентифікувати віддаленого VPN-клієнта і надавати доступ тільки авторизованим користувачам. Він також має

забезпечувати політику аудиту для перегляду активності користувачів: хто, коли і на який час підключався.

2 Управління IP адресами. Засіб VPN має видавати адреси з підмережі і давати гарантію що ці адреси не розкриються.

3 Шифрування даних. Дані що передаються по публічних мереж повинні бути зашифрованими.

4 Управління ключовою інформацією. VPN-засіб повинен генерувати ключі для шифрування і оновлювати їх з певною періодичністю.

Можна виділити наступні варіанти побудови мережі VPN, які використовуються при створенні VPN мереж провайдера:

1 Варіант «Intranet VPN» (рисунок 2.4), який дозволяє об'єднати в єдину захищену мережу декілька користувачів, що взаємодіють по відкритих каналах зв'язку. Саме цей варіант отримав широке поширення у всьому світі, і саме його в першу чергу реалізують провайдери. Цей варіант є топологію мережа-мережа. У цій конфігурації кожен шлюз розташований на кінці мережі та забезпечує безпеку каналу зв'язку між двома (або більше) мережами. Конфігурація цього типу краще всього підходить для з'єднання територіально розділених локальних мереж. Основна перевага даної конфігурації полягає в тому, що віддалені локальні мережі в VPN прозорі для кінцевого користувача. Фактично шлюзи VPN є для користувачів умовними маршрутизаторами. Структури мережа-мережа VPN можуть бути використані для зв'язку внутрішніх мереж, як якщо б вони мали суміжні канали. Передача даних між мережами Інтранет, зберігають конфіденційність під час передачі.

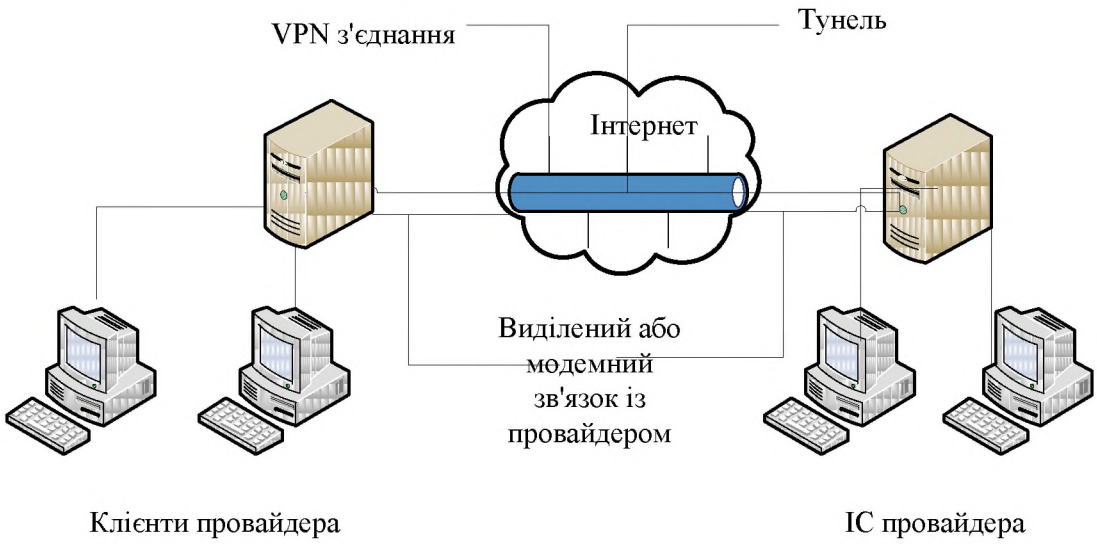

Рисунок 2.4 - Схема подключения мережа-мережа

2 Варіант «Client / Server VPN» (рисунок 2.5), який забезпечує захист переданих даних між двома вузлами мережі провайдера. Особливість даного варіанта в тому, що VPN будується між вузлами, що знаходяться, як правило, в одному сегменті мережі, наприклад між робочою станцією і сервером. Така необхідність дуже часто виникає в тих випадках, коли необхідно створити в одній фізичній, кілька логічних мереж. Цей варіант схожий на технологію VLAN, яка діє на рівні вище канального.

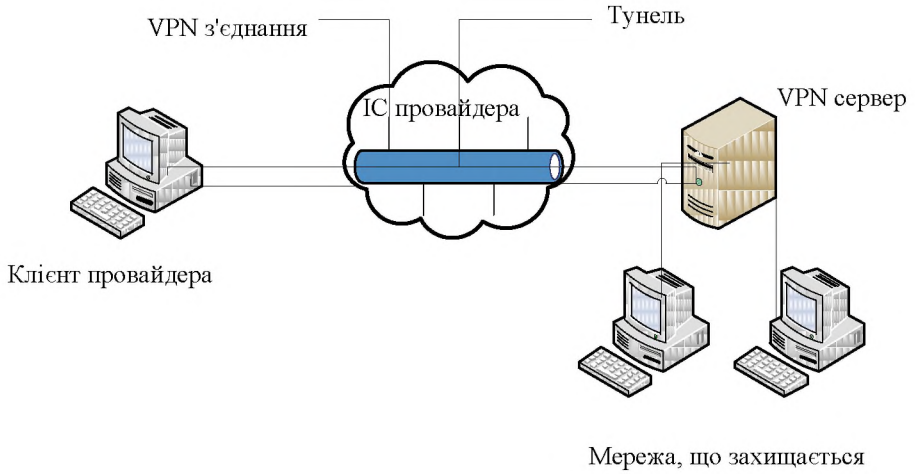

Рисунок 2.5 - Підключення до мережі VPN двох стаціонарних комп'ютерів

3 Варіант «Remote Access VPN» (рисунок 2.6), що дозволяє реалізувати захищену взаємодію між сегментом мережі провайдера і одиночним

користувачем, який підключається до ресурсів провайдера з дому (домашній користувач) або через notebook (мобільний користувач). Даний варіант відрізняється тим, що віддалений користувач, як правило, не має «статичної» адреси і підключається до ресурсу, щор захищається не через виділений пристрій VPN, а безпосередньо з власного комп'ютера, де і встановлюється програмне забезпечення, що реалізує функції VPN. Простий спосіб забезпечити мобільним користувачам можливість з'єднання з мережею провайдера дає віртуальна захищена мережа, або структура, хост-мережа VPN. У конфігурації такого роду кожен хост незалежно зв'язується з локальною мережею через шлюз VPN. Кожен хост автентифікований, і для нього організовується VPN-тунель. Мобільний хост може бути приєднаний будь-яким способом, будь то комутована лінія (dial-up), з'єднання з локальною мережею або бездротове з'єднання. Структура хост-мережа виправдана в разі віддаленого доступу.

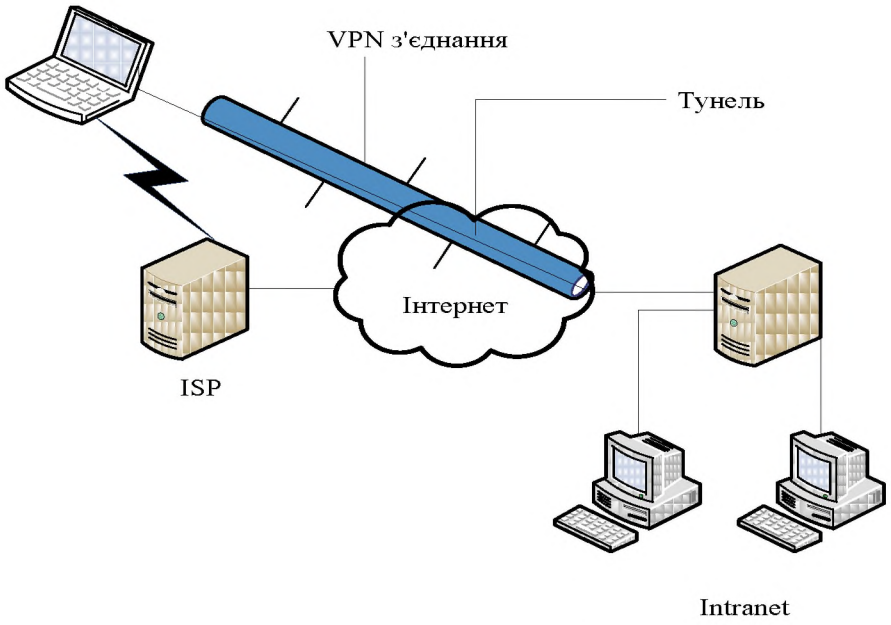

Рисунок 2.6 - Підключення до мережі VPN віддаленого користувача

Всі продукти для створення VPN можна умовно розділити на дві категорії: програмні і апаратні. Програмне рішення для VPN - це, як правило, готовий додаток, який встановлюється на підключеному до мережі окремому комп'ютері. Ряд виробників, такі як компанії Axent Technologies, Check Point Software Technologies і NetGuard, поставляють VPN-пакети, які легко інтегруються з

програмними мережевими екранами і працюють на різних операційних системах, включаючи Windows NT/2000, Sun Solaris і Linux. Оскільки для побудови VPN на базі спеціалізованого програмного забезпечення потрібне створення окремої комп'ютерної системи, такі рішення зазвичай складніше для розгортання, ніж апаратні. Створення подібної системи передбачає конфігурування сервера для розпізнавання даного комп'ютера і його операційної системи, VPN-пакетів, мережевих плат для кожного з'єднання і спеціальних плат для прискорення операцій шифрування. Така робота в ряді випадків може виявитися складною навіть для досвідчених фахівців. З іншого боку, програмні рішення для VPN коштують відносно недорого. На відміну від них апаратні VPN-рішення включають в себе все, що необхідно для з'єднання, - комп'ютер, приватну (як правило) операційну систему і спеціальне програмне забезпечення. Ряд компаній, у тому числі Cisco Systems, NetScreen і Sonic, пропонують цілий спектр рішень, які можуть масштабуватися в залежності від кількості одночасних VPN-з'єднань, з якими передбачається працювати, і очікуваного обсягу трафіку. Ще однією перевагою апаратних VPN-рішень є більш висока продуктивність. До мінусів апаратних VPN-рішень можна віднести їх високу вартість. Ще один недолік таких рішень полягає в тому, що управління ними здійснюється окремо від інших рішень з безпеки, що ускладнює завдання адміністрування інфраструктури безпеки.

Існують також інтегровані рішення, в яких функції побудови VPN реалізуються поряд з функцією фільтрації мережевого трафіку, забезпечення якості обслуговування або розподілу смуги пропускання. Основна перевага такого рішення - централізоване управління всіма компонентами з єдиної консолі. Друга перевага - більш низька вартість у розрахунку на кожний компонент у порівнянні з ситуацією, коли такі компоненти купуються окремо.

Процес шифрування даних вимагає істотних обчислювальних ресурсів і може перевантажити комп'ютер, коли кілька VPN-з'єднань одночасно беруть участь у передачі даних. В цьому випадку, щоб розвантажити центральний процесор, можливо, доведеться встановити спеціальні прискорювальні плати.

За статистикою, до 80% всіх інцидентів, пов'язаних з інформаційною безпекою, відбувається з вини авторизованих користувачів, які мають санкціонований доступ до мережі провайдера, а це означає, що атака або вірус від такого користувача будуть зашифровані та передані нарівні з нешкідливим трафіком. Необхідно згадати ще одну особливість VPN - використання цієї технології знижує продуктивність мережі, що обумовлено затримками встановлення захищеного з'єднання між VPN-пристроями, затримками шифрування даних, затримками контролю їх цілісності і збільшеним трафіком через використання більш довгих заголовків пакетів.

Загалом засоби VPN дозволяють здійснювати безпечну передачу даних через відкриті канали зв'язку, при цьому забезпечуючи надійний криптографічний захист даних від загроз. При цьому рівень захищеності при використанні VPN засобів залежить від правильності їх налаштування, що вимагає певного кваліфікаційного рівня системного адміністратора і знання технології VPN.

2.2.3.5 Сервер оновлень ПЗ

В ІС провайдера чисельність робочих станцій вже давно перевищила цифру в 100 одиниць. При всьому цьому перелік прикладного ПЗ, яке використовується користувачами в ІС, також може бути досить великим. Адміністратори стикаються з проблемою відновлення ОС і додатків в локальній мережі. Щоб забезпечувати належний рівень безпеки ПЗ не повинно містити в собі потенційно небезпечних вразливостей. Суть проблеми полягає в тому, щоб встановити ці оновлення на робочі станції ІС. ПЗ може мати в собі вбудовані засоби оновлення, а виробники даного ПЗ, як правило, регулярно оновлюють свої веб-сайти новими версіями ПЗ. Але якщо в мережі нараховується велика кількість комп'ютерів, то оновлення кожного з них займе певний відсоток часу адміністратора, а також спричинить велику витрату Інтернет трафіку.

Для автоматизації процесу оновлення, а також економії ресурсів провайдера використовується спеціалізоване ПЗ для централізованого оновлення. Сервер

оновлень викачує всі необхідні програми з певною періодичністю на свій локальний диск, а робочі станції для поновлення підключаються вже безпосередньо до нього. Найчастіше ці засоби оновлення розраховані на конкретну операційну систему або антивірусний продукт. Вигоди такого рішення очевидні: економія часу адміністратора, актуальна версія ПЗ, що містить останні програмні поліпшення, оновлена база вірусів забезпечує захист від усіх відомих вірусів.

До того ж централізована система оновлень зменшує ймовірність завантаження підроблених пакетів оновлень, змінених зловмисником з метою порушення безпеки провайдера. Багато програм оновлення підтримують перевірку ЦП виробника для завантаження пакетів і забезпечують захищений режим взаємодії, виключаючи можливість підміни зловмисником сервера оновлень і самих пакетів оновлень.

Таким чином, централізована система оновлення ПЗ в ІС провайдера сприяє підвищенню рівня захищеності всієї системи в цілому, економить час адміністраторів і ресурси провайдера. У той же час такі системи перекривають загрози, такі як переповнення буфера, відмова в обслуговуванні і т. ін. Для забезпечення належного рівня захищеності ІС провайдера в ній обов'язково має бути присутня система централізованого оновлення ПЗ.

Окрім перерахованих засобів захисту існують також і організаційні заходи із захисту інформації провайдера. Серед них можна виділити робробку та введення в дію політики захисту паролів та ідентифікаторів користувачів мережі Інтернет, а також плану забезпечення безперервної роботи та відновлення працездатності системи.

2.2.3.6 Політика захисту паролів та ідентифікаторів користувачів мережі Інтернет

Мета

Для здійснення доступу до мережі Інтернет співробітник або клієнт провайдера отримує від обслуговуючого персоналу логін (ідентифікатор

користувача) та пароль. Ці дані є унікальними для кожного користувача мережі, тому їх потрібно захищати від несанкціонованого використання.

Ця політика визначає правила використання паролів та ідентифікаторів користувачів, і є обов'язковою для виконання для всіх співробітників та клієнтів провайдера.

Права та обов'язки клієнтів та співробітників провайдера Співробітнику та клієнту забороняється:

1) повідомляти свій логін та пароль кому-небудь;

2) зберігати логіни та паролі, записані на папері, в легко доступному місці.

Співробітник та клієнт зобов'язаний:

1) у разі підозри на те, що пароль став комусь відомий, поміняти пароль і повідомити про факт компрометації обслуговуючий персонал;

2) негайно повідомити обслуговуючий персонал в разі отримання від когось прохання повідомити логін та пароль;

3) співробітник провайдера повинен після закінчення роботи з документами, які містять відомості про логіни та паролі, зберігати їх в закритій шухляді.

Обслуговуючий персонал зобов'язаний при отриманні заяви про факт компрометації паролю або отримання прохання про надання логіну та паролю негайно повідомити системного адміністратора.

Права та обов'язки системного адміністратора

Системний адміністратор зобов'язаний:

1) змінювати пароль при отриманні заяви щодо його компрометації;

2) створювати пароль, який відповідає таким вимогам: мінімальна довжина

пароля повинна бути 8 символів;

3) пароль повинен містити символи в різних регістрах, а також цифри і спеціальні символи (! @ # $% ^ & * ()-_ + = ~ [] {} | \:; '"<>,.? /).

Права провайдера:

Провайдер залишає за собою право:

1) здійснювати періодичну перевірку стійкості паролів користувачів, що використовуються співробітниками та клієнтами для доступу до мережі Інтернет;

2) вживати заходів дисциплінарного характеру до співробітників та клієнтів, що порушують положення цієї політики.

Розробка даної політики є необхідною для провайдера, оскільки вона передбачає зменшення ризику компрометації логіну та пароля, що є атрибутами користувача мережі Інтернет. Якщо зловмисник буде несанкціоновано використовувати декілька паролів клієнтів провайдера, то даний провайдер буде отримувати збитки за рахунок зменшення кількості клієнтів.

2.2.3.7 План забезпечення безперервної роботи та відновлення працездатності інформаційної системи провайдера

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Цей документ визначає основні заходи, методи та засоби збереження (підтримання) працездатності ІС при виникненні різних кризових ситуацій, а також способи і засоби відновлення інформації і процесів її обробки в разі порушення працездатності ІС і її основних компонентів. Крім того, він описує дії різних категорій персоналу інформаційної системи провайдера в кризових ситуаціях по ліквідації наслідків реалізації загроз та мінімізації збитків провайдера.

Класифікація кризових ситуацій. Ситуація, що виникає в результаті небажаного впливу на ІС, що не запобігається засобами захисту, називається кризовою. Кризова ситуація може виникнути в результаті злого умислу або випадково (в результаті ненавмисних дій, аварій, стихійних лих і т.д.).

За ступенем серйозності і розмірам завданої шкоди кризові ситуації поділяються на такі категорії:

1) загрозлива - приводить до повного виходу ІС з ладу і її нездатності виконувати далі свої функції, а також до знищення, блокування, неправомірною модифікації або компрометації найбільш важливої інформації;

2) серйозна - приводить до виходу з ладу окремих компонентів системи (часткової втрати працездатності), втрати продуктивності, а також до порушення цілісності та конфіденційності програм і даних в результаті несанкціонованого доступу.

Джерела інформації про виникнення кризової ситуації:

1) користувачі, що виявили підозрілі зміни в роботі або конфігурації інформаційної системи чи засобів її захисту;

2) засоби захисту, що виявили кризову ситуацію;

3) системні журнали, в яких є записи, що свідчать про виникнення або можливість виникнення кризової ситуації.

ЗАХОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ

Безперервність процесу функціонування ІС і своєчасність відновлення її працездатності досягається:

1) проведенням спеціальних організаційних заходів та розробкою організаційно-розпорядчих документів з питань забезпечення БРВ обчислювального процесу;

2) регламентацією процесу обробки інформації із застосуванням ПК і дій персоналу системи, у тому числі в кризових ситуаціях;

3) призначенням і підготовкою посадових осіб, відповідальних за організацію і здійснення практичних заходів щодо забезпечення БРВ інформації та обчислювального процесу;

4) чітким знанням і дотриманням усіма посадовими особами, які використовують засоби обчислювальної техніки ІС, вимог керівних документів щодо забезпечення БРВ;

5) застосуванням різних способів резервування апаратних ресурсів, еталонного копіювання програмних і страхового копіювання інформаційних ресурсів системи;

6) ефективним контролем за дотриманням вимог щодо забезпечення БРВ посадовими особами і відповідальним;

7) постійним підтриманням необхідного рівня захищеності компонентів системи, безперервним керуванням та адміністративною підтримкою коректного застосування засобів захисту;

8) проведенням постійного аналізу ефективності вжитих заходів і застосовуваних способів і засобів забезпечення БРВ, розробкою і реалізацією пропозицій щодо їх удосконалення.

ЗАГАЛЬНІ ВИМОГИ

Всі користувачі мережі Інтернет, які можуть не отримати доступ до мрежі в результаті виникнення загрозливої чи серйозної кризової ситуації, повинні негайно бути проінформованими. Подальші дії щодо усунення причин порушення працездатності ІС, відновлення обробки та відновлення пошкоджених (втрачених) ресурсів визначаються функціональними обов'язками співробітників провайдера.

Кожна кризова ситуація повинна аналізуватися адміністратором та за результатами цього аналізу повинні вироблятися пропозиції щодо зміни повноважень користувачів, атрибутів доступу до мережі, створення додаткових резервів, зміни конфігурації системи чи параметрів настройки засобів захисту тощо.

Серйозна і загрозлива кризова ситуація можуть вимагати оперативної заміни та ремонту обладнання, що вийшло з ладу, а також відновлення пошкоджених програм і наборів даних за допомогою резервних копій.

Оперативне відновлення програм і даних в разі їх знищення або псування забезпечується резервним копіюванням і довготривалим зберіганням копій.

Резервному копіюванню підлягають всі програми і дані, що забезпечують працездатність інформаційної системи та виконання нею своїх завдань (системне та прикладне програмне забезпечення, бази даних та інші набори даних), а також архіви, системні журнали і т.д.

Всі програмні засоби, що використовуються в системі повинні мати еталонні копії. Їх місцезнаходження та відомості про відповідальних за їх створення, зберігання і використання повинні бути зазначені у формулярах на кожну ПЕОМ (робочу станцію). Там же повинні бути зазначені переліки наборів

даних, що підлягають резервному копіюванню, періодичність копіювання, місце зберігання і відповідальні за створення, зберігання і використання резервних копій даних.

Необхідні дії співробітників провайдера щодо створення, зберігання і використання резервних копій програм і даних повинні бути відображені у функціональних обов'язках відповідних категорій персоналу.

Кожен носій, що містить резервну копію, повинен мати позначку, яка містить дані про клас, цінності, призначенні збереженої інформації, відповідального за створення, зберігання і використання, дату останнього копіювання, місце зберігання тощо.

Дублюючі апаратні ресурси призначені для забезпечення працездатності інформаційної системи в разі виходу з ладу всіх або окремих апаратних компонентів в результаті кризової ситуації. Кількість і характеристики дублюючих ресурсів повинні забезпечувати виконання основних завдань системою в будь-який з передбаченої планом ЗБРВ кризової ситуації.

У разі виникнення будь-якої кризової ситуації має здійснюватися розслідування причин її виникнення, оцінка заподіяної шкоди, визначення винних та прийняття відповідних заходів.

Розслідування кризової ситуації проводиться групою, яка призначається керівництвом установи. Очолює групу системний адміністратор. Про результати своєї роботи група доповідає безпосередньо керівництву.

Якщо причиною загрозливої чи серйозної кризової ситуації з'явилися недостатньо жорсткі заходи захисту та контролю, а збиток перевищив встановлений рівень, то така ситуація є підставою для повного перегляду Плану забезпечення безперервної роботи та відновлення.

ПОРЯДОК ПЕРЕГЛЯДУ ПЛАНУ

План ЗБРВ підлягає повному перегляду в наступних випадках:

1) при зміні переліку вирішуваних завдань, конфігурації технічних і програмних засобів ІС, що призводять до зміни технології обробки інформації;

2) при зміні пріоритетів у значущості загроз безпеки ІС.

План ЗБРВ підлягає частковому перегляду в наступних випадках:

1) при зміні конфігурації, додавання або видалення програмних і технічних засобів в ІС, не змінюють технологію обробки інформації;

2) при зміні конфігурації використовуваних програмних і технічних засобів;

3) при зміні складу, обов'язків і повноважень користувачів системи. Профілактичний перегляд Плану ЗБРВ проводиться не рідше 1 разу на рік і має на меті перевірку достатності визначених цим планом заходів реальним умовам застосування ІС та існуючим вимогам.

У разі часткового перегляду можуть бути додані, видалені або змінені різні додатки до плану з обов'язковим зазначенням даних про те, хто санкціонував, хто, коли і з якою метою вніс зміни.

Внесені в план зміни не повинні суперечити іншим положенням Плану ЗБРВ і повинні бути перевірені на коректність, повноту і можливість реального здійснення.

Перегляд Плану ЗБРВ повинен здійснюватися спеціальною комісією, склад якої затверджується керівництвом провайдера.

ВІДПОВІДАЛЬНІ ЗА РЕАЛІЗАЦІЮ ПЛАНУ

Відповідальним за реалізацію даного документа призначається системний адміністратор.

Розробка даного плану є необхідною для провайдера, оскільки зменшення часу на відновлення працездатності ІС дає змогу зменшити збитки внаслідок простою системи.

Звичайно, крім перерахованих рішень може існувати і маса інших, відмінних своїми характеристиками, реалізацією або набором засобів. Вибір оптимального набору засобів є одним з питань, що вирішуються в даній дипломній роботі.

2.2.4 Оцінка ефективності СЗІ

Розрахунок збитку від реалізації загроз приведений в розділі 3. Враховані час простою системи, час відновлення інформації та заробітна плата обслуговуючого персоналу, що займається усуненням наслідків реалізації загроз.

Для оцінки ймовірності нейтралізації загроз кожним із засобів захисту використовувався метод експертної оцінки. Результати оцінки ймовірностей нейтралізації загроз ІБ СЗІ наведено в таблиці 2.1

Рівень ефективності СЗІ буде розраховуватись за формулою (2.3). При цьому буде використовуватись перший спосіб оптимістично-песимістичного підходу. При використанні цього способу припускається, що що інтенсивності загроз рівні $\forall\ \lambda_i = \alpha$, і рівні константі $\alpha = const$. Таким чином, підставляючи значення ймовірностей p_i і суму втрат C_i в формулу (2.3) отримуємо загальний рівень ефективності СЗІ, який дорівнює:

$D = 0{,}95 * 100\% = 95\%$.

Таким чином була отримана оцінка ефективності набору засобів захисту. На практиці частіше виникають ситуації, коли необхідно вибрати з набору засобів тільки ті, які більшою мірою відповідають потребам компанії, в даному випадку забезпечують найбільший рівень захисту, при цьому система повинна мати мінімальну вартість і здійснювати мінімальний вплив на продуктивність всієї системи в цілому.

Таблиця 2.1 – Ймовірність нейтралізації загроз безпеці СЗІ

Вид загрози	Ймовірність нейтралізації загроз з урахуванням засобів захисту, рі						Загальна ймовірність рі
	Мережевий екран	VPN шлюз	IDS	Антивірус	Політика захисту паролів	Аварійний план	
Віруси	0,00	0,00	0,00	0,90	0,00	0,00	0,90
Dos	0,80	0,99	0,99	0,00	0,00	0,50	1,00
IP Spoofing	0,70	0,99	0,93	0,00	0,70	0,00	1,00
Захват мережевих підключень	0,50	0,99	0,90	0,00	0,50	0,70	1,00
Різні види	0,60	0,00	0,90	0,00	0,50	0,00	0,98

сканування мережі							
Недоступність даних	0,00	0,00	0,85	0,00	0,00	0,80	0,97
Порушення конфіденційності даних	0,00	0,95	0,00	0,00	0,70	0,00	0,99
Підбір паролів	0,75	0,00	0,90	0,00	0,90	0,00	1,00
Неавторизоване використання ІС	0,60	0,70	0,80	0,66	0,70	0,70	1,00
Зловживання правами користувачів та адміністраторів	0,10	0,10	0,00	0,00	0,50	0,30	0,72
Ймовірність нейтралізації всіх загроз системою захисту інформації							0,95
Загальна сума збитку без використання СЗІ, грн.							95936,00
Загальна сума збитку при використанні СЗІ, грн.							4335,18
Рівень ефективності СЗІ							0,95

Застосуємо запропоновану методику для вибору оптимальної системи захисту. При цьому введемо обмеження на вартість такої системи захисту. Припустимо, що система захисту повинна становити від 10 до 20 % від загальної вартості ІС. Саме такий підхід пропонують багато сучасних експертів під час оцінки вартості СЗІ. Припустимо, що загальна вартість аналізуємої ІС згідно даних її власника становить 100 000 грн. У цьому випадку доцільно на систему захисту витратити 20000 грн. В загальному випадку обмеження на вартість СЗІ обмежуються зверху вартістю інформації.

Оцінимо рівень захищеності при використанні набору таких засобів захисту як МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи: політика захисту паролів та аварійний план. Результати оцінка наведені в таблиці 2.2.

У цьому випадку рівень захищеності буде дорівнювати D = 0,92* *100% = 92%. Вартість такого рішення складе близько 10 000 грн.

В якості альтернативного набору засобів будемо використовувати ME, VPN-шлюз, систему IDS, і організаційні заходи: політика захисту паролів та аварійний план. (таблиця 2.3). Для такої системи рівень захисту дорівнюватиме D = 0,86* 100% = 86%. Вартість другого рішення буде складати 25000-35000 грн, оскільки системи виявлення вторгнень IDS є досить дорогими.

Варто зазначити що зниження продуктивності ІС провайдера за рахунок використання СЗІ знаходиться в межах допустимих 10 відсотків. В випадку провайдера доступу рівень продуктивності системи задається каналом доступу в мережу Інтернет. Для підключення до мережі Інтернет 2000 клієнтів цілком достатньою для нашої моделі ІС є швидкість 500 Мбіт / с. При чому швидкість до 100 Мбіт/с забезпечується кожному клієнту.

Всі засоби, що використовуються для захисту є програмними, тому їх швидкість роботи залежить від потужності обчислювальних засобів, і, таким чином, здійснюють мінімальний вплив на продуктивність системи.

Таблиця 2.2 – Ймовірність нейтралізації загроз СЗІ, яка складається із елементів: МЕ, VPN-шлюзу, та сервера антивірусного захисту

Вид загрози	Ймовірність нейтралізації загроз з урахуванням засобів захисту, pi					Загальна ймовірність pi
	Мережевий екран	VPN шлюз	Антивірус	Політика захисту паролів	Аварійний план	
Віруси	0,00	0,00	0,90	0,00	0,00	0,90
Dos	0,80	0,99	0,00	0,00	0,50	1,00
IP Spoofing	0,70	0,99	0,00	0,70	0,00	1,00
Захват мережевих підключень	0,50	0,99	0,00	0,50	0,70	1,00
Різні види сканування мережі	0,60	0,00	0,00	0,50	0,00	0,80
Недоступність даних	0,00	0,00	0,00	0,00	0,80	0,80
Порушення конфіденційності даних	0,00	0,95	0,00	0,70	0,00	0,99
Підбір паролів	0,75	0,00	0,00	0,90	0,00	0,98
Неавторизоване використання ІС	0,60	0,70	0,66	0,70	0,70	1,00
Зловживання правами користувачів та адміністраторів	0,10	0,10	0,00	0,50	0,30	0,72
Ймовірність нейтралізації всіх загроз системою захисту інформації						0,92
Загальна сума збитку без використання СЗІ, грн.						95936,00
Загальна сума збитку при використанні СЗІ, грн.						7960,98
Рівень ефективності СЗІ						0,92

Таблиця 2.3 – Ймовірність нейтралізації загроз СЗІ, що складається із елементів: ME, VPN-шлюзу, системи IDS та організаційних заходів

Вид загрози	Ймовірність нейтралізації загроз з урахуванням засобів захисту, pi					Загальна ймовірність pi
	Мережевий екран	VPN шлюз	IDS	Політика захисту паролів	Аварійний план	
Віруси	0,00	0,00	0,00	0,00	0,00	0,00
Dos	0,80	0,99	0,99	0,00	0,50	1,00
IP Spoofing	0,70	0,99	0,93	0,70	0,00	1,00
Захват мережевих підключень	0,50	0,99	0,90	0,50	0,70	1,00
Різні види сканування мережі	0,60	0,00	0,90	0,50	0,00	0,98
Недоступність даних	0,00	0,00	0,85	0,00	0,80	0,97
Порушення конфіденційності даних	0,00	0,95	0,00	0,70	0,00	0,99
Підбір паролів	0,75	0,00	0,90	0,90	0,00	1,00
Неавторизоване використання ІС	0,60	0,70	0,80	0,70	0,70	1,00
Зловживання правами користувачів та адміністраторів	0,10	0,10	0,00	0,50	0,30	0,72
Ймовірність нейтралізації всіх загроз системою захисту інформації						0,86
Загальна сума збитку без використання СЗІ, грн.						95936,00
Загальна сума збитку при використанні СЗІ, грн.						12983,10
Рівень ефективності СЗІ						0,86

За допомогою запропонованої методики методики визначено, що для прикладу ІС провайдера оптимальним рішенням щодо захисту буде набір засобів, що складається з: МЕ, VPN-шлюзу, антивірусного сервера і організаційних заходів: політики захисту паролів та ідентифікаторів користувачів мережі Інтернет, плану забезпечення безперервної роботи та відновленняипрацездатності інформаційної системи провайдера (аварійного плану). Цей набір характеризується високим рівнем ефективності, незначним впливом на продуктивність інформаційної системи провайдера доступу до мережі Інтернет, незначними витратами на створення та впровадження. Якщо при аналізі буде використовуватися значно більша кількість варіантів СЗІ, для вибору найбільш ефективного може використовуватися метод послідовних поступок, який був описаний в розділі 2.3.

2.3 Висновок

В даному розділі виконана розробка методики оцінки ефективності СЗІ. Результатом методики є кількісна оцінка рівня захищеності, що дозволяє більш точно порівнювати декілька варіантів захисту і, таким чином, вибирати найбільш ефективний. В якості вихідних даних методики подаються ймовірності реалізації загроз і вразливостей щодо ІС, вартість ресурсів (оцінка втрат у разі виходу з ладу інформаційного ресурсу) і частота загроз кожного виду в загальному потоці загроз. Вводяться обмеження на вартість СЗІ і зниження рівня продуктивності системи, який чиниться СЗІ. На виході методики отримуємо кількісну оцінку захищеності для всієї СЗІ в цілому.

До переваг методики слід віднести простоту її реалізації, поширений математичний апарат, доступність для розуміння.

Таким чином, розроблена методика може використовуватися для визначення забезпечуваного рівня захисту СЗІ провайдера доступу до мережі Інтернет як на початкових етапах проектування СЗІ, так і на стадії оцінки рівня захисту існуючої системи з метою їх модифікації. Розроблена методика характеризує інформаційну систему з боку ризиків і відповідно може бути конкретизована під відповідну організацію.

Рівень точності одержуваної на виході оцінки залежить в першу чергу від повноти списку загроз і вразливостей, як основних складових ризику, точності оцінки інформаційних ресурсів, а також точності оцінки імовірносних характеристик реалізації загроз. Для оцінки цих характеристик може знадобитися залучення, як технічних фахівців, так і представників управління самої компанії, що дозволяє надалі результативніше фінансувати і контролювати процес впровадження СЗІ.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є аналіз економічної доцільності розробки засобів підвищення ефективності системи захисту інформації провайдера доступу до мережі Інтернет. У вище наведених розділах здійснено розробку методики оцінки ефективності СЗІ, яка передбачає кількісну оцінку рівня захищеності, що дозволяє більш точно порівнювати декілька варіантів захисту і, таким чином, обирати найбільш ефективний. Для обґрунтування економічної доцільності застосування розробленої методики здійснюватиметься порівняння варіантів систем захисту інформації провайдера доступу до мережі Інтернет для кількості клієнтів, яка налічує 2000 чоловік.

3.1 Розрахунок (фіксованих) капітальних витрат

Відповідно до методики сукупної вартості володіння (ТСО), розробленої компанією Gartner Group, витрати класифікуються на капітальні (фіксовані) та поточні.

Капітальні (фіксовані) витрати є величиною коштів, призначених для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

Інформаційна система провайдера, є мережею невеликої організації з декількома відділами, співробітниками та клієнтами, що можуть віддалено підключатись до мережі провайдера.

Система складається з наступних елементів:

1) точка доступу VPN для віддаленого підключення до мережі провайдера клієнтів;

2) мережевий екран з підтримкою proxy та NAT;

3) IDS-система виявлення вторгнень;

4) сервер оновлень ПЗ, клієнтських ОС;

5) сервер антивірусного захисту;

6) сервер баз даних;

7) внутрішня локальна мережа з робочими станціями співробітників провайдера;

8) файл-сервер, на якому зберігаються документи відділів та інформація загального користування;

9) веб-сервер, який приймає HTTP-запити від клієнтів, зазвичай веб-браузерів, і видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом або іншими даними.

На комп'ютерах співробітників встановлена операційна система MS Windows 2012 з останнім набором оновлень і стандартним ПЗ від Microsoft, що входять в комплект поставки ОС. На серверах встановлена ОС Linux.

3.1.1. Визначення витрат на розробку методики оцінки ефективності СЗІ, яка передбачає кількісну оцінку рівня захищеності інформаційної безпеки

3.1.1.1 Визначення трудомісткості розробки методики оцінки ефективності СЗІ, яка передбачає кількісну оцінку рівня захищеності інформаційної безпеки

Трудомісткість розробки визначається тривалістю кожної робочої операції:

$$t = t_{тз} + t_в + t_а + t_р + t_д, \quad \text{годин},$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку методики оцінки ефективності СЗІ, $t_{тз}=6$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в=32$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а=28$;

$t_р$ – тривалість розробки методики оцінки ефективності СЗІ, $t_м=34$;

$t_д$ – тривалість підготовки технічної документації, $t_д=6$.

Отже,

$$t = 6+32+28+34+6 = 106 \text{ годин.}$$

3.1.1.2. Розрахунок витрат на розробку методики оцінки ефективності СЗІ

Витрати на розробку заходів безпеки Кпз складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки *Ззп* і вартості витрат машинного часу *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 16112 + 1781{,}86 = 17893{,}86 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 106*152 = 16112 \text{ грн.}$$

де t – загальна тривалість операцій, годин;

Зпр – средньогодинна заробітна плата спеціаліста с інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{Мч} = t \cdot С_{Мч} = 106 \cdot 16{,}81 = 1781{,}76 \text{ грн.}$$

де t – трудомісткість операцій із побудови ефективної системи доступу персоналу, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{Мч} = 0{,}9 \cdot 10 \cdot 1{,}55 + \frac{6800 \cdot 0{,}4}{1920} + \frac{4600 \cdot 0{,}6}{1920} = 16{,}81 \text{ грн.}$$

Варіанти систем захисту інформації провайдера доступу до мережі Інтернет складається із таких елементів, як: МЕ, VPN-шлюзу, сервери антивірусного захисту та системи IDS, які вже є частково наявними в інформаційній системі провайдера, тому додаткові витрати не виникають.

Для варіанту СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи, додатково необхідно здійснити витрати на розробку політики захисту паролів та аварійний план, які складатимуть 1500 грн.

Планується здійснення витрат на налагодження системи інформаційної безпеки в розмірі 500 грн. ($К_н$=500 грн.)

Для варіанту СЗІ, яка включає МЕ, VPN-шлюз, системи IDS організаційні заходи, додатково необхідно здійснити витрати на закупівлю системи виявлення вторгнень IDS, які складатимуть 16206,14 грн.

Заплановані організаційні заходи передбачають розробку політики захисту паролів та ідентифікаторів користувачів мережі Інтернет, плану забезпечення безперервної роботи та відновлення працездатності

інформаційної системи провайдера (аварійного плану), що потребує додаткових витрат величиною 4000 грн.

В цьому варіанті також планується здійснення витрат на налагодження системи інформаційної безпеки в розмірі 500 грн. ($К_н$=500 грн.)

Отже, капітальні (фіксовані) витрати на розробку засобів підвищення ефективності системи захисту інформації провайдера доступу до мережі Інтернет складуть за варіантами СЗІ за варіантами:

1) СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи:

$$К_1 = 17893,86 + 1500 + 500 = 19893,86 \text{ грн.}$$

2) СЗІ, яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи:

$$К_2 = 17893,86 + 12206,14 + 4000 + 500 = 34600 \text{ грн.}$$

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad \text{грн.}$$

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки).

При розробці методики оцінки ефективності системи захисту інформації провайдера доступу до мережі Інтернет значною мірою планується до використання наявне програмне та апаратне забезпечення, що

не потребує додаткових витрат на відновлення та модернізації системи. При цьому оновлення системи виявлення вторгнень IDS складає 128 грн./ місяць, тобто:

$$С_в = 128*12 = 1536 \text{ грн.}$$

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів становлять за варіантами:

1) СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи (політики захисту паролів та аварійний плану):

$$К_{н1} = 1200 \text{ грн.}$$

2) СЗІ, яка включає яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи (політика захисту паролів та ідентифікаторів користувачів мережі Інтернет, план забезпечення безперервної роботи та відновлення працездатності інформаційної системи провайдера (аварійний план)):

$$К_{н2} = 3600 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

На обслуговування додаткових функцій системи захисту інформації провайдера доступу до мережі Інтернет буде виділятися додатково 1200 грн./місяць на оплату праці спеціаліста з інформаційної безпеки. Отже,

$$С_з = 1200*12 = 14400 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 14400*0,22 = 3168 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,8 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,55 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0,8*1920*1,55 = 2380,8 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% за варіантами:

$$С_{тос}^{1} = 19893,86*0,01=198,94 \text{ грн.}$$

$$С_{тос}^{2} = 34600*0,01=346 \text{ грн.}$$

Таким чином, витрати на керування системою інформаційної безпеки ($С_к$) становлять за варіантами:

1) СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи:

$$С_{к1} = 1200 + 14400 + 3168 +2380,8 + 198,94 = 21347,74 \text{ грн.}$$

2) СЗІ, яка включає яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи:

$$С_{к1} = 3600 + 14400 + 3168 +2380,8 + 346 = 23894,8 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) за обома варіантами не виникають, оскільки зниження продуктивності ІС провайдера за рахунок використання СЗІ знаходиться в межах допустимих 10 відсотків. Рівень продуктивності системи задається каналом доступу в мережу Інтернет. У випадку підключення до мережі Інтернет аналізованою кількості клієнтів, яка налічує 2000 осіб, достатньою є швидкість 500 Мбіт/с., що дозволить провайдеру надавати клієнтам послуги зі швидкістю до 100 Мбіт/с. Всі засоби, що використовуються для захисту є програмними, тому їх швидкість роботи залежить від потужності обчислювальних засобів, і, таким чином, здійснюють мінімальний вплив на продуктивність системи.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають за варіантами:

1) СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи:

$$C_1 = 21347,74 \text{ грн.}$$

2) СЗІ, яка включає яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи:

$$C_2 = 1536 + 23894,8 = 25430,8 \text{ грн.}$$

3.2 Оцінка можливого збитку

3.2.1 Оцінка величини збитку

Відповідно до проведеного аналізу загроз та ймовірності їх реалізації з урахуванням засобів захисту інформаційного системи, який наведений у розділі 2 (див. табл. 2.2 та 2.3.) визначено загальна сума збитку без використання СЗІ, яка за обома варіантами складає 95936 грн.

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки за варіантами становитиме наступні значення:

1) СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи:

$$E_1 = 95936 - 21347{,}74 = 74588{,}26 \text{ грн.}$$

2) СЗІ, яка включає яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи:

$$E_2 = 95936 - 25430{,}8 = 70505{,}2 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

За методикою сукупної вартості володіння (ТСО) визначають такі показники економічної ефективності системи інформаційної безпеки як Коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де Е – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI за варіантами:

1) СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи:

$$ROSI = \frac{74588,26}{19893,86} = 3,75, \quad \text{частки одиниці,}$$

2) СЗІ, яка включає яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи:

$$ROSI = \frac{70505,2}{34600} = 2,04, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (5,5 %);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$3,75/2,04 > (5,5 - 5)/100 = 3,75/2,04 > 0,005.$$

Отже, обидва варіанти є економічно доцільним щодо інвестування. Але за загальною сумою збитку варіант СЗІ, який включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи, передбачає отримання збитку величиною 7960,98 грн. з ймовірністю нейтралізації всіх загроз системою захисту інформації, яка дорівнює 0,92, що демонструє ефективність СЗІ з рівнем 0,92. А варіант СЗІ, яка включає яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи, отримання збитку величиною 12983,10 грн. з ймовірністю нейтралізації всіх загроз системою

захисту інформації, яка дорівнює 0,86, що демонструє ефективність СЗІ з рівнем 0,86.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки. Відповідно термін окупності розробки засобів підвищення ефективності системи захисту інформації провайдера доступу до мережі Інтернет за варіантами складе:

1) СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{3,75} = 0,27, \quad \text{років (3,2 місяці),}$$

2) СЗІ, яка включає яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{2,04} = 0,49, \quad \text{років (5,9 місяців).}$$

3.4 Висновок

Згідно з наведеними розрахунками можна зробити висновок, що розробка засобів підвищення ефективності системи захисту інформації провайдера доступу до мережі Інтернет шляхом розробки та впровадження методики оцінки ефективності СЗІ, яка передбачає кількісну оцінку рівня захищеності інформаційної безпеки, є економічною доцільною. Обидва проаналізовані варіанти систем інформаційної безпеки (СЗІ, яка включає МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи; СЗІ, яка включає яка включає МЕ, VPN-шлюз, система IDS та організаційні заходи) за показниками економічного ефекту, коефіцієнту повернення інвестицій, терміну окупності є економічно доцільними. Але варіант СЗІ, яка включає

МЕ, VPN-шлюз, сервер антивірусного захисту та організаційні заходи, передбачає більший економічний ефект (Е=74588,26 грн.), коефіцієнту повернення інвестицій (ROSI=3,75) та коротший термін окупності, 0,27 року (3,2 місяці) при нижчих як капітальних витратах, які складають 19893,86 грн., так і експлуатаційних витратах (21347,74 грн.). При цьому цей варіант також має більш високу ймовірність нейтралізації всіх загроз системою захисту інформації, яка дорівнює 0,92, та біль високий рівень ефективності СЗІ, який дорівнює 0,92.

ВИСНОВКИ

При дослідженні діяльності провайдерів доступу до мережі Інтернет було визначено, що для даної організації характерна велика кількість загроз та велика кількість клієнтів, яким надається доступ до мережі. Внаслідок успішної реалізації загроз клієнти можуть не отримати доступу до мережі, що вплине на репутацію провайдера. При цьому провайдер зазнає значних збитків, пов'язаних із витратами на відновлення роботи інформаційної системи. Для підвищення рівня захищеності інформаційної системи провайдера необхідно оцінювати ефективність системи захисту інформації, реалізованої у даній організації.

В роботі була запропонована методика оцінки ефективності СЗІ, яка враховує специфіку провайдера, зокрема кількість його клієнтів, при визначенні збитків, яких зазнає дана організація внаслідок успішної реалізації атак. Розроблена методика передбачає визначення коефіцієнту ефективності СЗІ, враховуючи обмеження по витратам на її створення та по зниженню продуктивності ІС. За даними показниками обирається найбільш оптимальні засоби та заходи захисту інформації, які мають найвищий рівень ефективності, здійснюють мінімальний вплив на продуктивність інформаційної системи та мають невелику вартість.

При використанні даної методики на підприємстві зменшується час, що відводиться на вибір ефективного набору засобів та заходів захисту інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1 Рішення НКРЗ №512 від 11.11.2010 «Умови здійснення діяльності у сфері телекомунікацій з надання послуг доступу до Інтернет (Електрон. ресурс) / Спосіб доступу: URL: http://www.nkrz.gov.ua/uk/activities/ruling2/ 1289571519/print - Загол. з екрана

2 Закон України № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» (Електрон. ресурс) / Спосіб доступу: URL: zakon.rada.gov.ua/go/80/94-вр

3 Закон України № 1280-IV «Про телекомунікації» (Електрон. ресурс) / Спосіб доступу: URL: zakon.rada.gov.ua/go/1280-15

4 Шаньгин В.Ф., Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. – Изд-во: ДМК, 2011. – 134 с.

5 Маслова Н.А. Построение модели защиты информации с заданными характеристиками качества //Штучний інтелект. – Донецьк: ІШІ, 2011. – № 1. – С. 51-57.

6 Чипига А.Ф., Пелешенко В.С. Оценка эффективности защищенности автоматизированных систем от несанкционированного доступа.

7 Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. –Изд-во «ДиаСофт», 2011. – 693с.

8 Розробка ефективних систем захисту інформації в автоматизованих системах (Електрон. ресурс) / Спосіб доступу: URL: http://ua-referat.com/

9 Способы задания исходных параметров для оценки защищенности (Електрон. ресурс) / Спосіб доступу: URL: http://supermegayo.ru/nesdost/16.html Загол. з екрану.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	1	
5	А4	1 Розділ	44	
6	А4	2 Розділ	47	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу бакалавра на тему:
Розробка засобів підвищення ефективності системи захисту
інформації провайдера доступу до мережі Інтернет
Сінсевича Тараса Миколайовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатка.

Об'єкт дослідження: методи оцінки ефективності системи захисту інформації провайдера доступу до мережі Інтернет.

Мета роботи: підвищення рівня безпеки ІС провайдера за рахунок застосування результатів оцінки ефективності СЗІ.

У розділі «Стан питання. Постановка задачі» проведено аналіз основних методик оцінки ефективності СЗІ та загроз безпеки інформаційним ресурсам провайдера.

У спеціальній частині був здійснений аналіз механізмів захисту, які можуть використовуватися провайдерами. Розроблена методика оцінки ефективності СЗІ та визначені вихідні дані для розрахунків за даною методикою. Розроблені рекомендації щодо вибору ефективної СЗІ для провайдера доступу до мережі Інтернет.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник