МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп’ютерної інженерії

САВЧУК Володимир Андрійович

Модуль системи захисту інформації для інтернет-провайдера / Information security system module for Internet provider

спеціальність: 123 – Комп’ютерна інженерія
освітньо-професійна програма – Комп’ютерна інженерія

Кваліфікаційна робота

Виконав: студент групи КІ-41
САВЧУК Володимир Андрійович

Науковий керівник
к.т.н. Н.Я. Савка

ТЕРНОПІЛЬ - 2026

АНОТАЦІЯ

Савчук В.А. Модуль системи захисту інформації для інтернет-провайдера. – Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» за спеціальністю 123 «Комп'ютерна інженерія», освітньо-професійна програма. Західноукраїнський національний університет, Тернопіль, 2026.

Робота написана обсягом 63 сторінки і містить 16 рисунків, 6 таблиць, 2 додатки та 39 джерел за переліком посилань. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою кваліфікаційної роботи є розробка комплексної системи інфозахисту для інтернет-провайдера, що уможливить мінімізацію ризиків витоку інформації й підвищити рівень захисту даних. Методи дослідження включають методи аналізу та синтезу, порівняльного аналізу, проектування системи захисту, оцінювання ефективності.

У дослідженні розглянуто задачу проєктування модуля системи захисту інформації інтернет-провайдера. Проаналізовано нормативну базу на якій ґрунтуються системи захисту інформації., особливості діяльності інтернет-провайдерів. Досліджено основні загрози безпеки даних інтернет-провайдерів. Розроблено технічне завдання на розробку модуля системи захисту. Побудовано модель загроз та політики безпеки для інтернет-провайдера. Удосконалено систему захисту інформації інтернет-провайдера, результатами оцінки ефективності підтверджено її перспективність.

Практичне значення полягає удосконаленні системи захисту інформації інтернет-провайдера.

Ключові слова: ІНТЕРНЕТ-ПРОВАЙДЕР, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МЕТОДИ ШИФРУВАННЯ, МОДЕЛЬ ЗАГРОЗ, ПОЛІТИКИ БЕЗПЕКИ.

ANNOTATION

Savchuk V.A. Information security system module for Internet provider. – Manuscript.

Qualification work for the Bachelor degree in specialty 123 “Computer Engineering”, educational and professional program. Western Ukrainian National University, Ternopil, 2026.

The work is written in 63 pages and contains 16 figures, 6 tables, 2 appendices and 39 references. The volume of graphic material is 2 sheets of A3 format.

The purpose of the qualification work is to develop comprehensive information security system for Internet provider that will enable minimizing the risks of information leakage and increasing the level of data protection. The research methods include methods of analysis and synthesis, comparative analysis, security system design and efficiency assessment.

The study addresses the problem of designing information security system module for Internet provider. The regulatory framework on which information security systems are based and the specifics of Internet providers’ activities were analyzed. The main threats to data security for Internet providers were investigated. Technical specifications for development of the security system module were created. A threat model and security policies for Internet provider were developed. The information security system of Internet provider was improved, and the results of the efficiency assessment confirmed its feasibility and prospects for implementation.

The practical significance lies in improving the information security system of Internet provider.

Keywords: INTERNET PROVIDER, INFORMATION SECURITY SYSTEM, ENCRYPTION METHODS, THREAT MODEL, SECURITY POLICIES.

ЗМІСТ

ВСТУП

Забезпечення інформаційної безпеки (ІБ) в мережах інтернет-провайдерів є важливою задачею сучасних телекомунікаційних систем. Постійне зростання обсягів мережевого трафіку, розширення спектра цифрових послуг і збільшення кількості підключених пристроїв зумовлюють підвищення вимог до надійності та захисту мережевої інфраструктури. Водночас ускладнюється характер загроз, які можуть призводити до несанкціонованого доступу до даних, їх модифікації або порушення доступності інфоресурсів.

Таким чином, ефективний інфозахист в мережах провайдерів передбачає застосування комплексного підходу, що поєднує засоби моніторингу, аналізу та реагування на потенційні загрози. Традиційні методи захисту не завжди забезпечують достатню гнучкість у змінних умовах функціонування мереж, що обумовлює необхідність розробки нових засобів, здатних адаптуватися до динаміки мережевого середовища.

Існуючі захистсистеми включають мережеві екрани, системи виявлення вторгнень та засоби шифрування, що забезпечує базовий рівень безпеки. Проте такі інструменти часто характеризуються обмеженою адаптивністю до динамічних змін мережевого середовища та нових типів загроз. Це зумовлює необхідність їх удосконалення шляхом інтеграції додаткових компонентів, здатних підвищити ефективність аналізу трафіку та прийняття рішень.

Одним із підходів до підвищення рівня надійності та безпеки існуючих захистсистем є впровадження спеціалізованого програмного модуля, який здійснює аналіз стану мережі та адаптивне керування процесами виявлення й нейтралізації загроз. Такий модуль не змінює наявні засоби безпеки, а доповнює їх, забезпечуючи більш гнучке реагування на зміну параметрів мережевого трафіку та поведінки користувачів.

Зважаючи на зазначене вище, метою роботи є розробка комплексної системи інфозахисту для провайдера, що уможливить мінімізацію ризиків витоку

інформації й підвищити рівень захисту даних. Досягнення мети вимагає виконання таких задач:

– аналіз нормативно-правової бази для розробки захистсистеми;

– дослідження особливостей функціонування інфоресурсів інтернет-провайдера;

– проаналізувати загрози безпеки передачі даних;

– проаналізувати методи захисту інфоресурсів у мережах інтернет-провайдера;

– розробка моделі загроз;

– розробка моделі політики безпеки;

– проектування захистсистеми;

– оцінка ефективності запропонованої системи.

Об’єктом дослідження є процес захисту інфоресурсів інтернет-провайдера.

Предметом дослідження є методи та технології ІБ при розробці захистсистем.

Практична значущість роботи полягає у можливості застосування удосконаленої захистсистеми на підприємствах провайдерів для підвищення рівня захисту інфоресурсів, зменшення кількості інцидентів, що уможливить знизити загальні витрати.

Кваліфікаційну роботу підготовлено на основі вимог, що викладені у [27, 28].

Основні результати, отримані при виконанні кваліфікаційної роботи опубліковано на XXVI Всеукраїнській науково-технічній конференції молодих вчених, аспірантів та студентів «Стан, досягнення і перспективи інформаційних систем і технологій» [18].З копіями публікації можна ознайомитися у додатку А.

1 ОСНОВИ ІНФОЗАХИСТУ В МЕРЕЖАХ ІНТЕРНЕТ-ПРОВАЙДЕРА

1.1 Особливості функціонування мереж інтернет-провайдерів

Функціонування мереж провайдерів характеризується складною багаторівневою організацією, що забезпечує передавання, маршрутизацію та обробку великих обсягів даних у режимі реального часу (див. рисунок 1.1). Такі мережі поєднують різнорідні технології доступу, транспортні сегменти та магістральні канали зв'язку, об'єднуючи їх в єдину інфраструктуру, орієнтовану на надання послуг широкому колу абонентів [5, 6, 12].

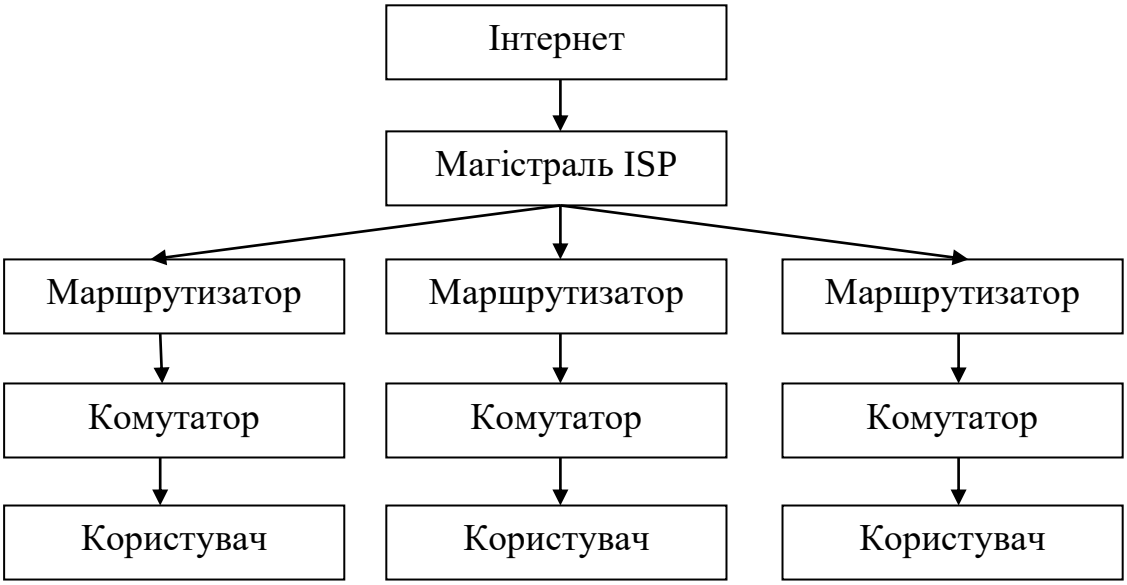

Рисунок 1.1 – Узагальнена структура мережі інтернет-провайдера

Узагальнена структура мережі провайдера являє багаторівневу телекомунікаційну інфраструктуру, що забезпечує підключення абонентів до глобальної мережі Інтернет, передачу даних між вузлами та керування мережевими ресурсами. Така мережа складається з кількох основних функціональних рівнів:

– рівень абонентського доступу (Access Network) забезпечує безпосереднє підключення користувачів до мережі провайдера. До нього належать абонентські маршрутизатори та модеми, точки доступу Wi-Fi або GPON/FTTH-термінали,

комутатори доступу (Access Switches), базові станції (у випадку бездротового доступу);

– рівень агрегації (Aggregation Layer) – об’єднання трафіку від великої кількості абонентів і його попередня обробка. Основні елементи цього рівня включають агрегуючі комутатори, маршрутизатори агрегації, механізми балансування навантаження;

– рівень ядра мережі (Core Network) відповідає за швидкісну та надійну передачу великих обсягів даних між сегментами мережі та зовнішніми каналами. Сюди входять високопродуктивні маршрутизатори, магістральні канали зв’язку (backbone), оптоволоконні лінії передачі даних;

– рівень виходу в глобальну мережу (Internet Gateway) забезпечує взаємодію з іншими мережами через точки обміну трафіком (IXP), зовнішні провайдери (upstream providers), міжнародні канали зв’язку;

– службовий та керуючий рівень, що виконує функції адміністрування та контролю – сервери DHCP, DNS, AAA (Authentication, Authorization, Accounting), системи моніторингу та управління мережею (NMS), засоби кіберзахисту (firewall, IDS/IPS).

Особливістю є необхідність підтримки безперервності сервісу за умов високого навантаження, що досягається при використанні механізмів балансування трафіку, резервування каналів та оптимізації маршрутів передачі даних. Схему взаємозв’язку операторів зв’язку різного рівня наведено у додатку КР.КІ.11492694.00.00.00.000 С1.

Суттєвим аспектом функціонування мереж провайдерів є динамічний характер трафіку, який формується під впливом поведінки користувачів і різних типів сервісів. Передавання потокового відео, голосових даних, інтерактивних сервісів і великих масивів інформації створює неоднорідні вимоги до пропускної здатності, затримок і надійності. У зв’язку з цим мережа повинна забезпечувати ефективне управління ресурсами, включаючи розподіл пропускної здатності та пріоритезацію трафіку, що безпосередньо впливає на якість обслуговування.

Функціонування мереж інтернет-провайдерів також супроводжується постійним впливом зовнішніх і внутрішніх факторів, які можуть погіршувати якість передавання даних. До таких факторів належать перевантаження мережі, затримки в передаванні пакетів, втрати даних, а також різноманітні завади та шуми в каналах зв'язку. Крім того, мережі піддаються загрозам, що можуть призводити до порушення їх стабільності та безпеки. Це зумовлює необхідність впровадження засобів моніторингу та аналізу трафіку, здатних своєчасно виявляти аномалії та реагувати на них.

Ще однією важливою особливістю є масштабованість і розподілений характер мереж провайдерів. Вони охоплюють великі території та включають велику кількість вузлів, що взаємодіють між собою через різні протоколи та інтерфейси. Така структура потребує узгодженого управління та координації роботи всіх компонентів, що досягається за рахунок використання централізованих і децентралізованих систем керування. Водночас зростає складність забезпечення ІБ, оскільки необхідно враховувати і локальні, і глобальні загрози.

Таким чином, мережі інтернет-провайдерів функціонують в умовах високої динамічності, неоднорідності трафіку та постійного впливу зовнішніх факторів, що висуває підвищені вимоги до ефективності управління, якості обслуговування та рівня інфозахисту. Це обумовлює необхідність удосконалення існуючих захистсистем шляхом впровадження інтелектуальних модулів, здатних адаптивно реагувати на зміни в мережевому середовищі.

1.2 Нормативна база для розробки систем інфозахисту

Нормативна база для розробки систем інфозахисту є сукупністю чинних законодавчих актів, державних стандартів, нормативних документів та міжнародних рекомендацій, які визначають вимоги до побудови, впровадження та

експлуатації систем інфозахисту [14, 20-22, 31-33]. Вона встановлює правові, організаційні та технічні засади забезпечення ІБ, регламентує порядок обробки, зберігання та передачі інформації, а також визначає вимоги до захисту інфоресурсів від несанкціонованого доступу, витоку, модифікації або знищення.

До нормативної бази, що використовується при розробці систем інфозахисту, зазвичай, належать закони України у сфері ІБ, нормативні документи Державної служби спеціального зв'язку та інфозахисту України, державні стандарти (зокрема ДСТУ), а також міжнародні стандарти серії ISO/IEC [3, 4, 7, 8], які регламентують підходи до управління інформаційною безпекою (див. таблицю 1.1).

Таблиця 1.1 – Нормативно-правова база

Категорія	Нормативний документ	Характеристика та призначення
Міжнародні стандарти	ISO/IEC 27001:2022	Визначає вимоги до розробки, впровадження та постійного вдосконалення системи управління ІБ
	ISO/IEC 27002:2022	Містить рекомендації щодо реалізації заходів і моніторингу ІБ
	NIST SP 800-53	Описує набір практик і механізмів захисту інформаційних систем
	GDPR (General Data Protection Regulation)	Встановлює правила обробки та захисту персональних даних у межах ЄС
Національне законодавство України	Закон України «Про інфозахист в інформаційно-телекомунікаційних системах»	Визначає правові засади інфозахисту в ІТ-системах

Продовження таблиці 1.1

	Закон України «Про інформацію»	Регламентує процеси обробки, зберігання та поширення інформації
	Закон України «Про електронні довірчі послуги»	Визначає правові аспекти використання електронного підпису та довірчих сервісів
	ДСТУ ISO/IEC 27001:2015	Національна адаптація міжнародного стандарту управління ІБ
	Концепція забезпечення кібербезпеки України	Визначає стратегічні напрями розвитку системи кібербезпеки держави
Галузеві та технічні стандарти	ДСТУ 3396.2-97	Встановлює вимоги до інфозахисту в автоматизованих системах
	ДСТУ 3396.3-97	Описує підходи до побудови систем інфозахисту
	Методики оцінювання ризиків	Передбачає процедури аналізу загроз, вразливостей і рівня ризику
Внутрішні нормативні документи	Політики інформаційної безпеки та конфіденційності	Визначають внутрішні правила інфозахисту на підприємстві
	Регламенти та корпоративні процедури	Забезпечують дотримання вимог безпеки в операційній діяльності

Таблиця 1.1 дає структурований огляд нормативно-правової бази, що слугують основою для розробки систем інфозахисту, із описом змісту кожної групи документів. Використання нормативних актів і стандартів забезпечує відповідність систем захисту вимогам українського законодавства, міжнародним стандартам та сучасним технологічним вимогам у галузі ІБ.

1.3 Загрози безпеки в мережах передачі даних

Загрози безпеці в мережах передачі даних формуються під впливом відкритості телекомунікаційного середовища, великої кількості взаємодіючих вузлів і постійної циркуляції інформації. У таких умовах будь-який етап обробки або передавання даних може стати точкою шкідливого впливу, що зумовлює необхідність комплексного розгляду природи загроз і механізмів їх реалізації. Безпека мереж визначається здатністю системи забезпечувати конфіденційність, цілісність і доступність інформації, проте кожна з цих властивостей може бути порушена різними типами атак, що відрізняються за способом реалізації та наслідками.

Однією з найбільш поширених загроз є перехоплення інформації в процесі її передавання каналами зв’язку. Через те, що значна частина мережевого трафіку проходить через спільні або недостатньо захищені середовища, виникає можливість несанкціонованого доступу до даних шляхом пасивного аналізу трафіку. Такий підхід дозволяє отримувати відомості без безпосереднього втручання в роботу системи, що ускладнює виявлення загрози. У випадку відсутності або недостатнього рівня криптографічного захисту це може призводити до витоку конфіденційної інформації, включаючи персональні дані, службові повідомлення або облікові дані користувачів [37, 38].

Порушення цілісності інформації реалізується через активний вплив на дані, коли зловмисник змінює їх зміст під час передачі або на етапі обробки. Такі дії можуть мати як цілеспрямований характер, так і бути наслідком впровадження шкідливого програмного забезпечення, яке змінює або замінює інформацію. Внаслідок цього користувач або система отримує некоректні дані, що може призводити до помилкових рішень, збоїв у роботі сервісів або компрометації інформаційних ресурсів.

Окрему групу становлять загрози, спрямовані на порушення доступності мережевих ресурсів. Такі атаки, зазвичай, реалізуються шляхом створення

надмірного навантаження на мережеву інфраструктуру або окремі її елементи, що унеможливлює обслуговування легітимних користувачів. Найбільш характерним прикладом є DDoS attack, у межах якого велика кількість скомпрометованих пристроїв одночасно генерує запити до цільового ресурсу. У результаті відбувається вичерпання обчислювальних або мережевих ресурсів, що призводить до часткової або повної відмови в обслуговуванні [35, 36].

Суттєвою загрозою є також несанкціонований доступ до мережевих ресурсів, який може бути наслідком використання слабких механізмів автентифікації, помилок конфігурації або вразливостей програмного забезпечення. У разі успішної реалізації такої атаки зловмисник отримує можливість взаємодіяти з системою від імені легітимного користувача або адміністратора, що відкриває шлях до подальших дій, включаючи зміну конфігурацій, встановлення шкідливих компонентів або організацію нових атак [15].

У сучасних досить поширеними є загрози, пов’язані з підміною мережевих вузлів і спотворенням маршрутів передавання даних. Такі атаки дозволяють зловмиснику інтегруватися в процес обміну інформацією, перехоплювати або змінювати дані, а також перенаправляти трафік через контрольовані вузли. У результаті виникає ризик повної компрометації каналу зв’язку навіть без явного порушення його працездатності.

Не менш важливою є проблема поширення шкідливого програмного забезпечення, яке може проникати в мережу через уразливі вузли або користувацькі пристрої. Після проникнення такі програми здатні самостійно поширюватися мережею, використовуючи її ресурси для виконання шкідливих дій, зокрема збору інформації, організації атак або порушення роботи систем. Це створює додаткове навантаження на мережу та ускладнює процес її захисту [38].

Варто враховувати, що загрози можуть мати як зовнішнє, так і внутрішнє походження. Внутрішні загрози часто пов’язані з помилками адміністрування, недостатнім контролем доступу або неналежною політикою безпеки. Вони можуть проявлятися у вигляді витоку інформації, несанкціонованого використання ресурсів або порушення роботи системи. Особливість таких загроз полягає в тому,

що вони виникають у межах довіреного середовища, що суттєво ускладнює їх виявлення та нейтралізацію.

1.4 Аналіз методів інфозахисту в телекомунікаційних системах

Аналіз методів інфозахисту в телекомунікаційних системах доцільно розглядати як комплекс взаємопов’язаних підходів, спрямованих на забезпечення основних властивостей ІБ, зокрема конфіденційності, цілісності, доступності та автентичності даних. У сучасних телекомунікаційних мережах, де передача інформації здійснюється через відкриті та потенційно вразливі канали зв’язку, жоден окремий метод не є достатнім, тому використовується багаторівнева система захисту [34, 37, 38].

Одним із основних напрямів є застосування криптографічних методів, які базуються на математичних перетвореннях інформації з метою її приховування від несанкціонованих осіб [5]. Симетричне шифрування характеризується високою швидкістю обробки даних і ефективністю при великих обсягах трафіку, однак потребує безпечного каналу для обміну ключами. Асиметричне шифрування дозволяє вирішити проблему розповсюдження ключів, але вимагає складних обчислювальних процедур. Додатково застосовуються механізми хешування та цифрового підпису, які гарантують цілісність даних та підтвердження авторства. Основною перевагою криптографічних методів є високий рівень теоретичної стійкості до атак, однак їх недоліком залишається суттєве навантаження на обчислювальні ресурси, а також складність управління інфраструктурою, особливо в масштабних мережах (див. рисунок 1.2).

Рисунок 1.2 – Алгоритми шифрування даних

Важливу роль відіграють мережеві методи захисту, які реалізуються на рівні маршрутизації та фільтрації трафіку (див. рисунок 1.3). Мережеві екрани дозволяють контролювати вхідні та вихідні потоки даних відповідно до заданих політик безпеки, що суттєво знижує ризик несанкціонованого доступу.

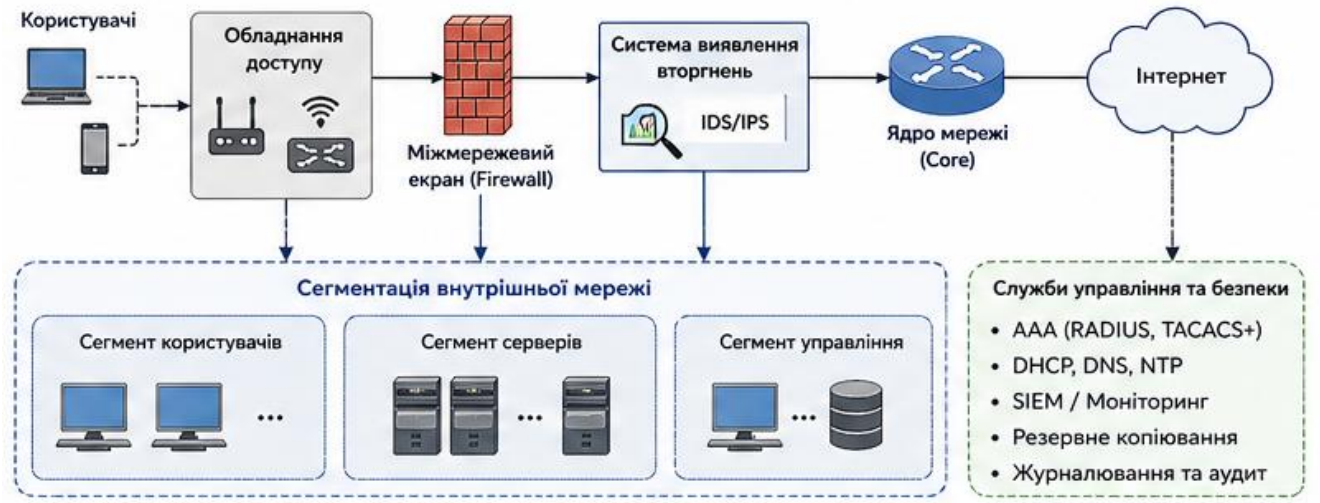

Рисунок 1.3 – Структура системи виявлення та запобігання вторгненням

Системи виявлення та запобігання вторгненням забезпечують моніторинг аномальної активності, що дозволяє оперативно реагувати на потенційні загрози [36]. Однак ефективність таких засобів знижується при використанні шифрованого трафіку, а також у випадках складних атак, що імітують легітимну

поведінку користувачів. Крім того, суттєвим обмеженням є необхідність постійного оновлення сигнатур і правил, що потребує адміністративних ресурсів.

Окрему категорію становлять програмно-апаратні методи захисту, які включають системи автентифікації, авторизації та контролю доступу. Вони забезпечують ідентифікацію користувачів та обмеження їхніх прав відповідно до встановлених політик безпеки (див. рисунок 1.4). Використання багатофакторної автентифікації суттєво підвищує рівень захисту, оскільки поєднує декілька незалежних механізмів підтвердження особи. Разом із тим, такі методи можуть знижувати зручність користування системою та вимагати додаткових витрат на впровадження і підтримку інфраструктури. До апаратних засобів також належать засоби захисту кінцевих пристроїв, які дозволяють ізолювати потенційно небезпечні процеси та обмежувати вплив шкідливого програмного забезпечення.

Рисунок 1.4 – Програмно-апаратні методи захисту

Організаційні методи інфозахисту формують нормативно-процедурну основу функціонування всієї системи безпеки. Вони включають розробку політик інформаційної безпеки, регламентів доступу до ресурсів, а також процедур реагування на інциденти [37]. Їхня ефективність полягає у зниженні ризиків, пов’язаних із людським фактором, який у багатьох випадках є найслабшою ланкою захистсистеми. Водночас ці методи не можуть самостійно забезпечити технічний рівень безпеки, оскільки їх реалізація залежить від дисципліни персоналу, рівня підготовки користувачів та контролю з боку адміністрації.

Слід також враховувати методи сегментації мережі та побудови захищених віртуальних середовищ, які дозволяють обмежувати розповсюдження потенційних атак усередині інфраструктури (див. рисунок 1.5). Поділ мережі на логічні сегменти з різними рівнями довіри зменшує площу атаки та підвищує керованість безпекових політик. Однак ускладнення архітектури мережі може призводити до зростання витрат на адміністрування та діагностику несправностей.

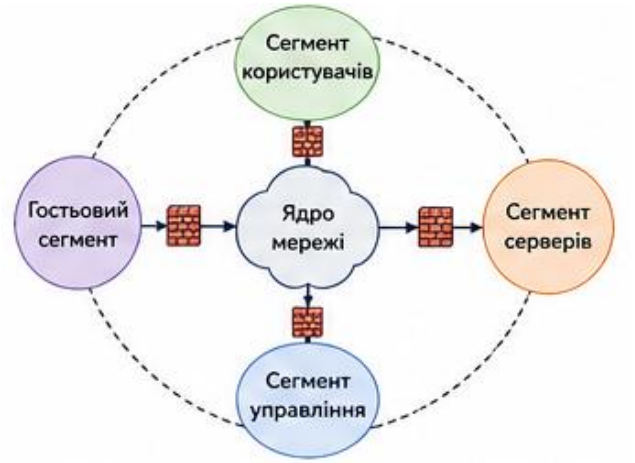

Рисунок 1.5 – Сегментація мережі

Таким чином, вищепроведений аналіз показує, що кожен із методів інфозахисту має свої переваги та недоліки. Криптографічні засоби забезпечують високий рівень конфіденційності, але потребують значних ресурсів. Мережеві механізми ефективні для контролю трафіку, але вразливі до складних атак. Програмно-апаратні методи підвищують рівень контролю доступу, але залежать від правильності конфігурації системи. Організаційні методи знижують ризики людського фактору, проте не забезпечують технічного захисту. Зважаючи на зазначене, оптимальним підходом до розробки система інфозахисту у телекомунікаційних системах є комплексне поєднання існуючих підходів в єдину багаторівневу захистсистему.

1.5 Постановка задачі кваліфікаційної роботи

Функціонування мереж інтернет-провайдерів супроводжується обробкою значних обсягів різнорідного мережевого трафіку в умовах постійної зміни навантаження та впливу кіберзагроз. Існуючі системи інфозахисту забезпечують базові механізми фільтрації та контролю доступу, однак їх ефективність є обмеженою в умовах динамічного середовища та складних комбінованих атак. Це призводить до зниження якості виявлення загроз, збільшення кількості помилкових спрацювань і перевантаження мережевих ресурсів.

Забезпечення безпеки даних є однією із ключових задач сучасних підприємств у галузі телекомунікацій, зокрема, інтернет-провайдерів, діяльність яких пов’язана з обробкою великої кількості даних користувачів, що містять конфіденційну, комерційну та персональну інформацію. Ключовою проблемою виступає недостатня узгодженість підходів до забезпечення ІБ, які часто не враховують технічні та організаційні аспекти захисту. Ситуація ускладнюється також стрімким розвитком інформаційних технологій, який зумовлює появу нових вразливостей і, відповідно, підвищує рівень ризиків для безпеки даних.

Таким чином, виникає необхідність у розробці модуля системи інфозахисту для інтернет-провайдера, який враховуватиме специфіку функціонування підприємства та сучасні загрози безпеки. Основні задачі, як необхідно вирішити:

- розробка моделі загроз;
- розробка моделі політики безпеки інформації;
- проектування компонентів захистсистеми;
- оцінка ефективності запропонованої системи.

2 МОДЕЛЬ ЗАГРОЗ БЕЗПЕКИ ДАНИХ В МЕРЕЖАХ ІНТЕРНЕТ-ПРОВАЙДЕРА

2.1 Ситуаційний план об’єкта

Об’єктом дослідження виступає підприємство інтернет-провайдер, що надає послуги доступу до мережі Інтернет як фізичним, так і юридичним особам. До основних напрямів діяльності компанії належить забезпечення стабільного та якісного доступу до мережі, а також надання супутніх сервісів, серед яких хостинг, реєстрація доменних імен, IP-телефонія, налаштування корпоративних мереж [39].

Підприємство є приватною телекомунікаційною структурою регіонального рівня, що обслуговує значну кількість клієнтів, що сягає кілька тисяч. Його інфраструктура охоплює центральний офіс, у межах якого функціонують адміністративні та технічні підрозділи, серверні приміщення та дата-центр. До складу мережевої інфраструктури входять маршрутизатори, комутатори, точки бездротового доступу та програмно-апаратні платформи, призначені для управління послугами. Передавання даних із високою швидкістю забезпечується завдяки використанню оптоволоконних каналів зв’язку.

До основних інформаційних ресурсів підприємства належать:

– клієнтські бази даних, що містять контактні відомості, інформацію про укладені договори та платіжні дані;

– технічна документація, яка включає мережеві схеми та плани обслуговування;

– облікові записи доступу до інформаційних систем як адміністративного, так і користувацького рівня.

Інформаційна система підприємства включає апаратні засоби, зокрема сервери, мережеві пристрої та системи резервного копіювання. Програмне забезпечення представлене системами управління взаємовідносинами з клієнтами, засобами моніторингу мережі та білінговими платформами. Канали зв’язку

забезпечують як внутрішню взаємодію між компонентами системи, так і обмін даними із зовнішніми мережами.

Серед основних загроз ІБ підприємства виокремлюються несанкціонований доступ до клієнтських даних, атаки типу DDoS attack, спрямовані на серверну та мережеву інфраструктуру, використання шкідливого програмного забезпечення для компрометації інформаційних систем, фізичне пошкодження або знищення обладнання внаслідок аварій чи навмисних дій, а також порушення функціонування внутрішньої мережі через людський фактор або недостатній рівень підготовки персоналу.

З урахуванням критичності опрацьовуваних даних та наявних ризиків, підприємство потребує удосконалення системи інфозахисту, що поєднує технічні, організаційні та програмні заходи, спрямовані на забезпечення конфіденційності, цілісності та доступності даних. Реалізація такого підходу дозволить підвищити рівень безпеки інфоресурсів, зміцнити довіру клієнтів, мінімізувати можливі фінансові втрати.

Ситуаційний план підприємства є важливим для розробки системи інфозахисту. Він включає візуалізацію фізичного розташування офісних приміщень, серверних кімнат, мережевого обладнання та інших елементів, що потребують захисту. Опишемо основні елементи плану в таблиці 2.1.

Таблиця 2.1 – Компоненти ситуаційного плану

Елемент	Розташування
Центральний офіс	Центральна частина міста, містить адміністративні приміщення, абонентські кімнати, технічний відділ і серверну кімнату
Серверна кімната	Приміщення з обмеженим доступом, оснащене системами контролю доступу і відеоспостереженням
Дата-центр	Приміщення з посиленою охороною, яке розташоване окремо, слугує місцем зберігання даних та хостингу критичних сервісів

Продовження таблиці 2.1

Мережеве обладнання	По всьому офісу з метою безперебійного доступу до мережі Інтернет, основні вузли розміщені у серверній кімнаті
Канали зв’язку	Оптоволоконна мережа, що забезпечує з’єднання з клієнтами та між філіями компанії, резервні канали забезпечують стійкість системи
Зони загального доступу	Приміщення адміністративного призначення для роботи персоналу, кімнати переговорів та нарад, зони обслуговування клієнтів
Критичні зони	Серверна кімната, приміщення з технічним обладнанням, дата-центр

Опис заходів захисту фізичної інфраструктури включає комплекс організаційних і технічних рішень, спрямованих на обмеження доступу до критичних ресурсів та забезпечення безперервності функціонування обладнання. Контроль фізичного доступу реалізується шляхом впровадження електронних замків і систем ідентифікації персоналу, що дозволяє обмежити доступ до критичних зон лише авторизованим особам. Додатково застосовуються системи відеоспостереження, які забезпечують постійний моніторинг переміщення співробітників і відвідувачів, що підвищує рівень контролю та дозволяє оперативно реагувати на потенційні порушення.

Захист від фізичних загроз передбачає використання спеціалізованих технічних засобів, спрямованих на запобігання пошкодженню обладнання. До них належать протипожежні системи, зокрема датчики диму та автоматизовані засоби пожежогасіння, які забезпечують своєчасне виявлення та ліквідацію загорянь. Окрім цього, застосовуються джерела безперебійного живлення, що дозволяють захистити обладнання від негативного впливу перепадів напруги та забезпечити його стабільну роботу у випадку аварійних ситуацій.

Організація розміщення обладнання також відіграє важливу роль у забезпеченні безпеки інфраструктури. Сервери та мережеві пристрої

розміщуються у спеціалізованих стійках із обмеженим доступом, що надається виключно уповноваженому персоналу. Резервні сервери, у свою чергу, розташовуються в окремих захищених зонах, що дозволяє підвищити стійкість системи до відмов і забезпечити збереження даних у разі виникнення надзвичайних ситуацій.

Для наочного представлення структури фізичної інфраструктури розроблено план-схему, яка показує розташування ключових елементів, зокрема офісних приміщень, серверної кімнати, мережевого обладнання, зон загального доступу та критичних зон (див рисунок 2.1).

Рисунок 2.1 – Ситуаційний план приміщення

Ситуаційний план слугує базою для подальшої ідентифікації ризиків і розроблення заходів захисту, що дозволяють врахувати всі фізичні особливості інфраструктури підприємства. Його використання сприяє більш ефективній

організації захисту інформаційних ресурсів та зменшенню рівня потенційних загроз.

2.2 Модель загроз

Модель загроз для інтернет-провайдера відображає сукупність потенційних джерел небезпеки, вразливостей інфраструктури та можливих наслідків їх реалізації, що можуть впливати на конфіденційність, цілісність і доступність інформації [29, 37, 38]. Її формування ґрунтується на аналізі особливостей функціонування мережі провайдера, характеру оброблюваних даних і типових сценаріїв атак у телекомунікаційному середовищі.

У межах моделі враховується, що джерелами загроз можуть виступати як зовнішні зловмисники, так і внутрішні користувачі або персонал підприємства. Зовнішні загрози пов’язані з відкритістю мережі та можливістю віддаленого доступу до її ресурсів, що створює передумови для реалізації атак, спрямованих на перехоплення даних, порушення роботи сервісів або отримання несанкціонованого доступу. Внутрішні загрози виникають унаслідок помилок персоналу, недотримання політик безпеки або навмисних дій, що можуть призводити до витоку інформації чи порушення функціонування системи.

Об’єктами впливу в моделі загроз виступають інфоресурси підприємства, зокрема бази даних клієнтів, мережеве обладнання, серверна інфраструктура та програмні системи керування послугами. Уразливості цих об’єктів можуть бути пов’язані з недосконалістю програмного забезпечення, помилками конфігурації, недостатнім рівнем захисту каналів зв’язку або фізичною доступністю обладнання.

Сценарії реалізації загроз включають різні форми впливу на систему. До них належить:

– перехоплення трафіку, що дозволяє отримувати конфіденційну інформацію;

– модифікація даних, яка призводить до порушення їх цілісності;

– атаки, спрямовані на зниження доступності ресурсів, зокрема DDoS attack.

Окрім цього, можливими є атаки, пов’язані з використанням шкідливого програмного забезпечення, яке здатне проникати в систему та поширюватися мережею, порушуючи її нормальне функціонування.

Реалізація зазначених загроз може мати різні наслідки, серед яких витік конфіденційної інформації, фінансові втрати, зниження довіри клієнтів і порушення стабільності роботи мережі. Це обумовлює необхідність врахування ризиків на всіх рівнях функціонування системи, починаючи від фізичної інфраструктури і закінчуючи програмними засобами обробки даних.

Таким чином, модель загроз для провайдера є основою для побудови системи інфозахисту, оскільки дозволяє систематизувати потенційні ризики, визначити критичні елементи інфраструктури та обґрунтувати вибір відповідних заходів безпеки. В таблиці 2.2 наведено основні типи загроз.

Таблиця 2.3 – Класифікація загроз

Тип загроз	Приклади
Технічні загрози	Відмова обладнання, збої у мережевих з’єднаннях, некоректне функціонування серверів, відсутнє або неналежно організоване резервне копіювання даних
Програмні загрози	Шкідливе програмне забезпечення, зокрема віруси і троянські програми, експлуатація вразливостей у програмних компонентах системи, що може призводити до компрометації інформаційних ресурсів
Кіберзагрози	Несанкціонований доступ до баз даних, DDoS-атаки, фішингові впливи, перехоплення даних під час передачі по каналах

Продовження таблиці 2.3

Фізичні загрози	Викрадення обладнання, пошкодження серверних приміщень унаслідок надзвичайних ситуацій, несанкціонований доступ до критично важливих зон інфраструктури
Організаційні загрози	Недотримання вимог інформаційної безпеки персоналом, недостатнім рівнем його підготовки та відсутністю чітко визначених політик безпеки на підприємстві

Ймовірні сценарії реалізації загроз для інтернет-провайдера включають отримання зловмисниками доступу до мережевих ресурсів через наявні вразливості захищених з'єднань, поширення шкідливого програмного забезпечення через електронну пошту співробітників, несанкціоноване проникнення до серверної з метою фізичного впливу на обладнання, а також проведення масштабних атак типу DDoS attack, які можуть призвести до порушення надання послуг.

Реалізація таких загроз здатна спричинити втрату або компрометацію конфіденційної інформації клієнтів, виникнення перебоїв у роботі сервісів, що, у свою чергу, призводить до зниження рівня задоволеності користувачів. Крім того, можливими наслідками є фінансові втрати, пов'язані з відновленням працездатності інформаційних систем, а також суттєве погіршення ділової репутації компанії. Основні моделі загроз опишемо в таблиці 2.3.

Таблиця 2.3 – Моделі загроз

Клас загроз	Джерела виникнення	Потенційний вплив	Рівень імовірності	Ступінь впливу
Технічні	Відмови апаратного забезпечення, несправність серверів, відсутність резервування та відновлення	Порушення доступу інформаційних ресурсів, простої сервісів, втрата доступу до даних	Високий	Високий

Продовження таблиці 2.3

Програмні	Експлуатація вразливостей програмного забезпечення, помилки конфігурації, впровадження шкідливого програмного коду	Порушення цілісності та конфіденційності даних, компрометація систем	Середній	Високий
Мережеві	Несанкціонований доступ до мережі, DDoS-атаки, перехоплення або модифікація трафіку	Деградація або недоступність сервісів, втрата чи підміна даних	Високий	Високий
Фізичні	Несанкціонований фізичний доступ, аварії електроживлення, пожежі, затоплення	Пошкодження або знищення обладнання, втрата інформації	Низький	Середній
Організаційні	Недостатній рівень підготовки персоналу, порушення регламентів безпеки, людський фактор	Зниження ефективності захистсистеми, витік конфіденційної інформації	Середній	Високий

Розроблена модель загроз уможливлює сформувати чітке розуміння найбільш критичних ризиків для інфоресурсів провайдера. Це забезпечує ефективний розподіл ресурсів для мінімізації ризиків, оптимізацію заходів захисту та забезпечення відповідності стандартам. Типову систему виявлення та запобігання вторгненням наведено на КР.КІ.11492694.00.00.00.000 С2.

2.3 Технічне завдання на розробку системи інфозахисту

Метою проєкту є удосконалення системи інфозахисту для телекомунікаційної мережі провайдера з метою забезпечення конфіденційності, цілісності та доступності даних відповідно до вимог сучасної кібербезпеки [29, 30, 37].

1. Система безпеки повинна забезпечувати захист від внутрішніх і зовнішніх загроз, включаючи несанкціонований доступ, мережеві атаки, шкідливе програмне забезпечення та витоки інформації.

2. Підстава для розробки. Підставою для створення системи є:

- зростання кількості кіберзагроз у корпоративних мережах;
- необхідність захисту конфіденційних даних;
- вимоги до забезпечення безперервності бізнес-процесів;
- відповідність міжнародним стандартам ІБ.

3. Призначення системи. Система призначена для:

- виявлення та блокування мережевих атак;
- контролю доступу до інформресурсів;
- захисту каналів передачі даних;
- моніторингу подій безпеки в реальному часі;
- запобігання витоку або модифікації даних.

4. Вимоги до захистсистеми.

4.1 Функціональні вимоги – система повинна забезпечувати автентифікацію та авторизацію користувачів, шифрування даних із використанням сучасних алгоритмів, захист мережевого трафіку, виявлення атак типу DDoS attack, журналювання подій безпеки, інтеграцію з системами Intrusion Detection System (IDS) та Intrusion Prevention System (IPS).

4.2 Вимоги до надійності – безперервна робота системи 24/7, стійкість до відмов апаратного та програмного забезпечення, автоматичне відновлення після збоїв, резервування критичних компонентів.

4.3 Вимоги до безпеки – захист від несанкціонованого доступу, багаторівнева автентифікація користувачів, мінімізація поверхні атаки, захист від внутрішніх загроз, відповідність політикам безпеки підприємства.

4.4 Вимоги до продуктивності – мінімальна затримка обробки мережевого трафіку, можливість масштабування системи, підтримка великої кількості одночасних з’єднань.

5. Склад і структура системи. Система повинна включати:

- модуль мережевого моніторингу;
- модуль аналізу загроз;
- підсистему шифрування даних;
- міжмережевий екран (Firewall);
- систему IDS/IPS;
- модуль журналювання та звітності.

6. Вимоги до програмного та апаратного забезпечення – підтримка сучасних операційних систем, використання віртуалізації за необхідності, сумісність із мережевим обладнанням стандарту Ethernet/Wi-Fi, підтримка криптографічних бібліотек.

7. Етапи розробки проєкту.

1) Аналіз вимог та загроз безпеки.
2) Проєктування архітектури системи.
3) Розробка програмних модулів.
4) Інтеграція компонентів системи.
5) Тестування (функціональне, навантажувальне, безпекове).
6) Впровадження та налаштування.
7) Підготовка документації.

8. Порядок контролю та приймання – перевірка відповідності функціональним вимогам, тестування стійкості до атак, оцінка продуктивності системи, аналіз журналів безпеки, затвердження результатів замовником.

9. Очікувані результати. У результаті впровадження системи очікується:

- зниження ризику інцидентів;

– підвищення рівня захищеності мережі;

– контроль і моніторинг подій безпеки в реальному часі;

– забезпечення стабільної роботи інформаційної інфраструктури.

Зважаючи на вищезазначене, технічне завдання визначає загальні положення, на яких повинно ґрунтуватися розробка, мету розробки, аналіз вимог, етапи виконання та реалізації проєкту, технічні характеристики системи інфозахисту. Технічне завдання забезпечує чітку структуру розробки, враховуючи всі етапи, вимоги до функціональності та обладнання.

Обґрунтування переваг впровадження та удосконалення системи інфозахисту для інтернет-провайдера відображено у таблиці 2.4.

Таблиця 2.4 – Обґрунтування переваг впровадження захистсистеми

Загроза	Заходи протидії	Досягнутий ефект
Порушення доступу до інформаційних ресурсів	Реалізація механізмів багатофакторної перевірки користувачів та застосування криптографічного захисту даних	Гарантування обмеженого доступу та збереження конфіденційності інформації
Атаки на відмову в обслуговуванні та інші мережеві впливи	Впровадження систем аналізу мережевого трафіку та засобів виявлення / блокування атак	Забезпечення безперервного функціонування сервісів і стабільності мережі
Помилки персоналу та людський фактор	Формування політик інформаційної безпеки та проведення регулярного навчання співробітників	Зменшення кількості інцидентів, пов’язаних із неправильними діями користувачів
Наявність вразливостей у програмному забезпеченні	Своєчасне оновлення програмних продуктів і застосування засобів антивірусного захисту	Зниження ймовірності використання вразливостей та зараження систем

Продовження таблиці 2.4

Загрози фізичного характеру	Організація контролю доступу до приміщень і використання систем захисту інфраструктури	Запобігання пошкодженню обладнання та збереження працездатності систем

Варто зазначити, що доцільність розробки захистсистеми та її вдосконалення визначається комплексом показників, що охоплюють технічну стійкість, швидкість реагування, рівень захищеності, продуктивність і здатність до розвитку [30, 37]. Саме поєднання цих критеріїв дозволяє об'єктивно оцінити рівень безпеки інформаційної інфраструктури провайдера:

$$E = \sum_{i=1}^{n} w_i \cdot K_i, \tag{2.1}$$

де E – інтегральна оцінка системи інфозахисту,

K_i – значення *i*-го показника ефективності,

w_i – коефіцієнт значущості *i*-го критерію,

n – кількість показників.

Для інтернет-провайдера формула (2.1) набуває вигляду:

$$E = w_1 K_{\text{det}} + w_2 K_{pre} + w_3 K_{res} + w_4 K_{perf} + w_5 K_{avail}, \tag{2.2}$$

де K_{det} – коефіцієнт виявлення загроз;

K_{pre} – ефективність запобігання атак;

K_{res} – стійкість до навантаження / відмов;

K_{perf} – продуктивність системи;

K_{avail} – доступність сервісу;

w_i – вагові коефіцієнти кожного критерію, причому:

$$\sum_{i=1}^{5} w_i = 1,\ w_i \geq 0.$$

Для інтернет-провайдера, зазвичай, більшу вагу отримують:

w_1, w_2 – безпека (виявлення та блокування атак);

w_4, w_5 – стабільність і якість сервісу,

а менше:

w_3 – безпека (виявлення та блокування атак).

Підсумовуючи, розробка захистсистеми інфоресурсів є необхідною для забезпечення належного рівня безпеки даних провайдера, мінімізації ризиків загроз. Удосконалення такої системи на основі сучасних технологій уможливить підвищити якість надання послуг та рівень діяльності провайдера.

3 УДОСКОНАЛЕНА СИСТЕМА ІНФОЗАХИСТУ ІНТЕРНЕТ-ПРОВАЙДЕРА

3.1 Модель політики безпеки

Модель політики безпеки для провайдера описує не лише технічні засоби захисту, а й правила управління доступом, обробки даних та реагування на інциденти [16, 17, 24]. У межах сучасних вимог до безпеки така модель, зазвичай, будується за принципом багаторівневого захисту (defense in depth) і поєднує організаційні, технічні та процедурні механізми (див. рисунок 3.1).

Рисунок 3.1 – Рівнева структура політики безпеки

На концептуальному рівні політика визначає основну мету – забезпечення конфіденційності, цілісності та доступності інформації, а також безперервності надання телекомунікаційних послуг. Для інтернет-провайдера це особливо важливо, оскільки порушення роботи мережі безпосередньо впливає на велику кількість користувачів.

Основою моделі є контроль доступу до ресурсів мережі. Для цього застосовуються механізми автентифікації та авторизації, які можуть реалізовуватися за допомогою централізованих серверів доступу та обліку. При цьому доцільно використовувати підходи рольового або атрибутного контролю доступу, що дозволяє гнучко керувати правами користувачів і персоналу.

Наступним елементом є захист мережевої інфраструктури. Він передбачає сегментацію мережі, фільтрацію трафіку, використання міжмережевих екранів і систем виявлення вторгнень. Це дозволяє виявляти аномальну активність і запобігати атакам ще на ранніх етапах.

Важливу роль відіграє криптографічний захист даних. Передача інформації повинна здійснюватися через захищені протоколи, а конфіденційні дані мають зберігатися у зашифрованому вигляді Це мінімізує ризики перехоплення або підміни інформації.

Окремий компонент політики – моніторинг і аудит подій безпеки. Він включає централізоване журналювання, аналіз логів та виявлення інцидентів у реальному часі. Для провайдера це дає змогу оперативно реагувати на загрози, які можуть порушити роботу всієї мережі.

Не менш важливою є політика реагування на інциденти. Вона повинна визначати процедури виявлення, локалізації, усунення наслідків і відновлення роботи систем. Також необхідно передбачити резервне копіювання та аварійне відновлення інфраструктури.

Організаційна складова моделі включає навчання персоналу, регламентування доступу до обладнання та визначення відповідальності за порушення політики безпеки. Людський фактор залишається одним із найслабших елементів, тому його контроль є надзвичайно важливим.

Таким чином, узагальнену модель політики безпеки провайдера можна представити як сукупність таких рівнів (див рисунок 3.1):

– нормативний (правила, стандарти, політики);

– технічний (засоби захисту мережі та даних);

– операційний (моніторинг, реагування, аудит);

– організаційний (регламенти, інструкції, навчальні тренінги для персоналу).

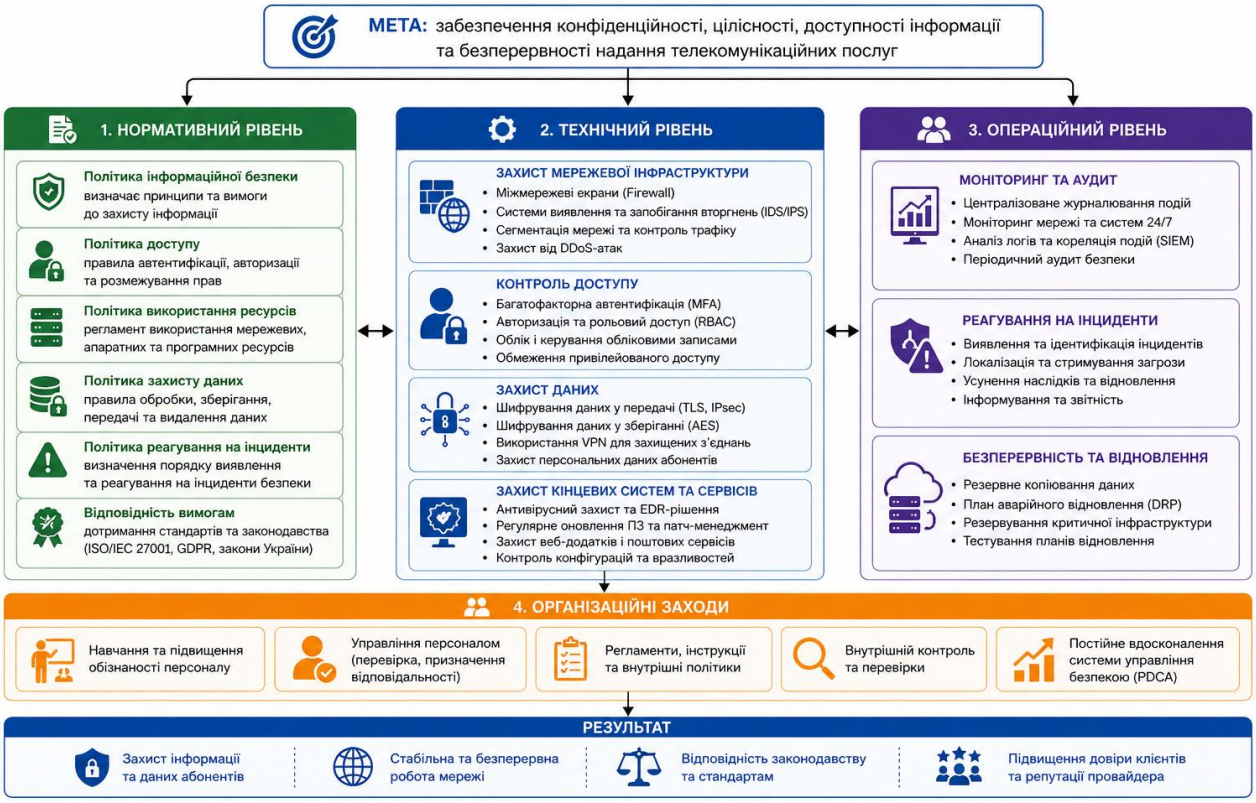

Рисунок 3.1 – Модель політики безпеки інтернет-провайдера

Така модель забезпечує комплексний підхід до захисту мережі провайдера інтернет-послуг і дозволяє ефективно протидіяти як зовнішнім, так і внутрішнім загрозам.

3.2 Проєкт системи інфозахисту інтернет-провайдера

Проєктування системи інфозахисту передбачає формування загальної архітектури, обґрунтування вибору програмно-апаратних засобів, а також визначення підходів до їх інтеграції в існуючу інфраструктуру. Основною метою цього процесу є досягнення належного рівня захисту інформаційних ресурсів підприємства з урахуванням актуальних загроз і сучасних вимог до безпеки [16, 17].

Процес проєктування охоплює декілька взаємопов'язаних етапів. На початковому етапі формується архітектура системи, яка включає логічну, фізичну

та функціональну складові. Паралельно розробляється модель загроз і механізмів захисту, що базується на аналізі активів, потенційних вразливостей і можливих сценаріїв атак. Наступним кроком є підбір необхідного програмного та апаратного забезпечення, а також визначення меж і зон безпеки. Завершальним етапом виступає планування інтеграції захистсистем в існуюче інформаційне середовище організації.

Логічна структура орієнтована на забезпечення захисту мережевої інфраструктури та інфоресурсів. На рівні периметра застосовуються міжмережеві екрани, які виконують функції контролю та фільтрації мережевого трафіку. Захист серверів, баз даних і робочих станцій реалізується шляхом впровадження спеціалізованих засобів безпеки. Управління доступом здійснюється на основі рольової моделі, що забезпечує розмежування прав користувачів. Додатково впроваджуються системи виявлення та запобігання вторгненням, які дозволяють оперативно реагувати на підозрілу активність.

Фізична структура системи передбачає організацію захищених приміщень для розміщення критичного обладнання. Серверні кімнати обладнуються засобами контролю доступу, системами відеоспостереження та датчиками стану навколишнього середовища. Центри обробки даних додатково оснащуються джерелами безперебійного живлення та системами пожежогасіння. При цьому зони з відкритим доступом обмежуються у можливостях взаємодії з інформаційними ресурсами, що знижує ризик несанкціонованого доступу.

До складу програмних засобів входять системи управління ІБ, що забезпечують централізований моніторинг подій та аналіз загроз, криптографічні механізми для захисту даних під час передавання і зберігання, антивірусні програми, а також технології захищеного віддаленого доступу, зокрема VPN.

Апаратна складова включає мережеве обладнання безпеки, зокрема міжмережеві екрани (див рисунок 3.3), які реалізують контроль доступу на рівні мережевого периметра, а також інші спеціалізовані пристрої, що забезпечують фільтрацію трафіку та протидію мережевим атакам (див. рисунки 3.4-3.6).

Рисунок 3.3 – Фаєрвол

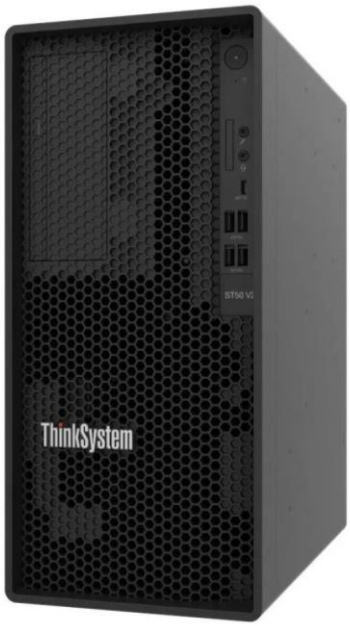

Рисунок 3.4 – Сервер з високою продуктивністю

Рисунок 3.5 – Мережевий комутатор для сегментації мережі

Рисунок 3.6 – Система резервного копіювання

Архітектура системи інфозахисту провайдера відображає типову структуру мережі з урахуванням сучасних вимог до безпеки. На периметрі мережі розташовані засоби протидії DDoS-атакам і крайові маршрутизатори, що забезпечують взаємодію з глобальною мережею Інтернет за допомогою протоколів маршрутизації.

Ядро мережі реалізоване на базі високопродуктивних маршрутизаторів, які підтримують MPLS та забезпечують швидкісну передачу даних між сегментами. Рівень агрегації об’єднує трафік від абонентських вузлів і передає його до BRAS/BNG, де відбувається автентифікація користувачів і керування сесіями доступу.

Доступ абонентів організовано через технологію GPON із використанням OLT та ONU/ONT, що дозволяє масштабувати мережу. Для розмежування трафіку застосовується сегментація на основі VLAN (інтернет, IPTV, VoIP, службовий трафік).

Сегмент дата-центру включає сервери та публічні сервіси, розміщені в DMZ, які захищені міжмережевими екранами. Для підвищення рівня безпеки використовуються системи моніторингу, такі як SIEM, а також IDSi IPS, що забезпечують виявлення та запобігання атакам [1, 2, 6, 10]. На рисунку 3.7 зображено типову архітектуру мережі інтернет провайдера.

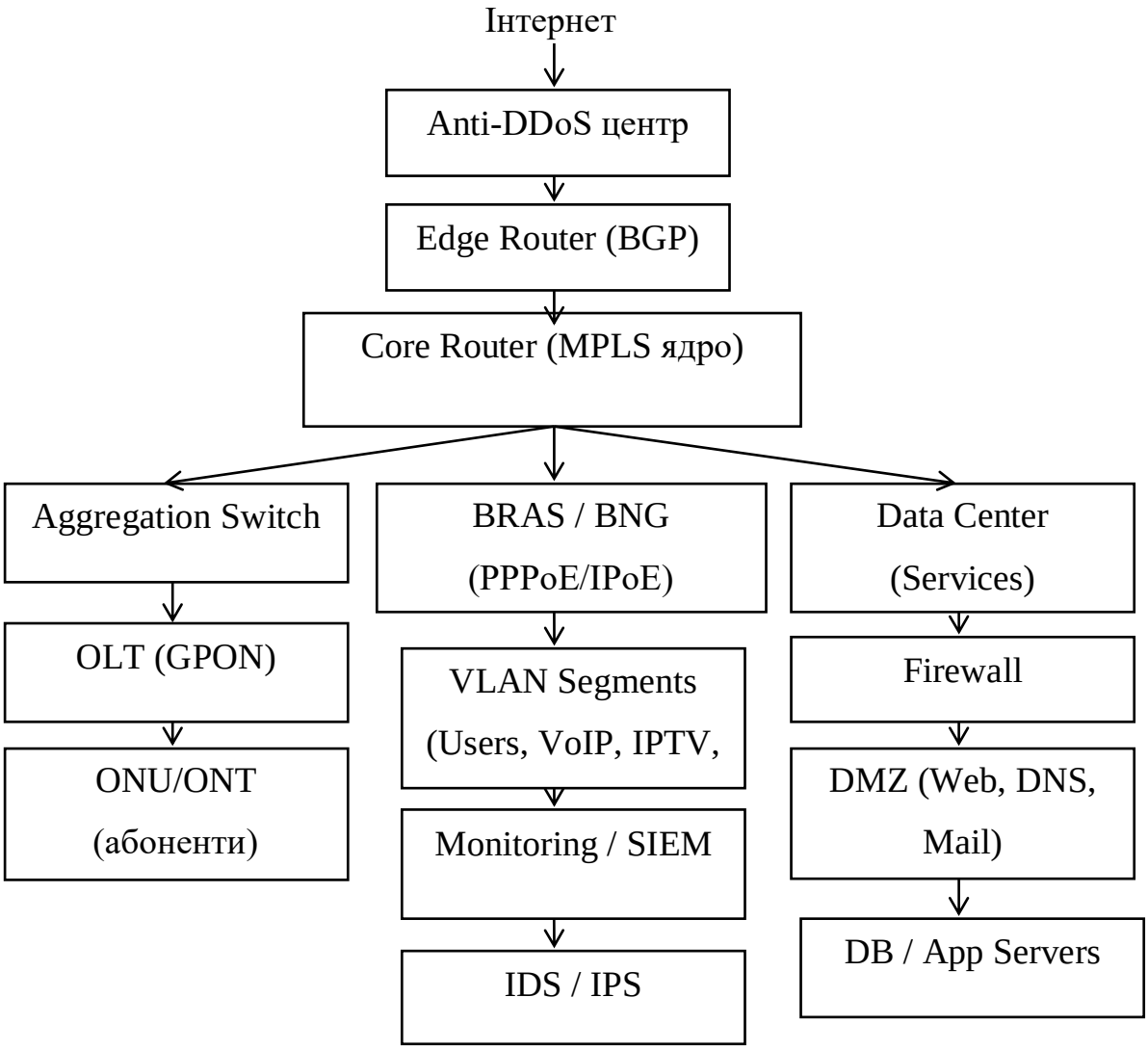

Рисунок 3.7 –Архітектура мережі інтернет-провайдера

У такій архітектурі вже закладено базові механізми захисту, але сучасні виклики вимагають удосконалення. Ключова ідея полягає у переході від «наявності засобів» до керованої, автоматизованої та сегментованої безпеки.

Перш за все варто підсилити периметр. Навіть за наявності Anti-DDoS і Firewall доцільно додати інтелектуальні системи фільтрації трафіку з поведінковим аналізом і репутаційними базами. Це дозволить ефективніше протидіяти складним атакам, включаючи варіації DDoS attack, які маскуються під легітимний трафік. Також бажано впровадити Web Application Firewall (WAF) для захисту сервісів у DMZ.

Другий напрям стосується сегментації та ізоляції. Хоч використовується VLAN, сучасні підходи вимагають додати інтелектуальні системи фільтрації

трафіку з поведінковим аналізом і репутаційними базами. [5]. Це означає, що навіть всередині сегментів доступ має надаватися за принципом «мінімальних привілеїв». Такий підхід суттєво обмежує горизонтальне переміщення зловмисника у випадку компрометації.

Доцільно також розширити механізми автентифікації, додавши багатофакторну перевірку для адміністративного доступу, а також централізовані системи керування ідентифікацією (IAM). Це знижує ризики внутрішніх загроз і компрометації облікових записів.

Суттєве удосконалення можливе в частині моніторингу. Якщо вже використовується SIEM, його варто доповнити системами поведінкової аналітики (UEBA) та автоматизованого реагування (SOAR). У поєднанні з IDS iIPS це дозволить не лише виявляти інциденти, а й оперативно їх локалізувати без участі людини.

Варто посилити захист абонентського доступу. На рівні BRAS/BNG доцільно реалізувати антиспуфінг, контроль DHCP, захист від MAC-flooding і фільтрацію аномального трафіку. Для GPON-сегмента бажано додати контроль ONU та виявлення несанкціонованих підключень.

Окрім використання TLS і AES, варто впровадити повноцінне управління ключами (KMS) і шифрування між внутрішніми сервісами (east-west traffic), що часто залишається незахищеним [9].

Необхідно передбачити георезервування (DR-site), дублювання критичних вузлів (BRAS, Core, Firewall) і регулярне тестування планів відновлення. Це важливо для провайдера, де навіть короткочасна недоступність сервісу має серйозні наслідки.

Часто організаційний рівень є найслабшим місцем системи безпеки. Тому регулярні аудити безпеки, тестування на проникнення (pentest), оновлення політик і навчання персоналу дають не менший ефект, ніж технічні засоби. На рисунку 3.8 зображено удосконалену архітектуру мережі інтернет-провайдера із модулем системи інфозахисту на основі сучасних технологій та викликів до систем безпеки підприємств у галузі телекомунікацій. Штрих-пунктирною лінією на рисунку

позначено блоки, які удосконалено з метою підвищення рівня захисту даних, що передаються по каналах зв’язку.

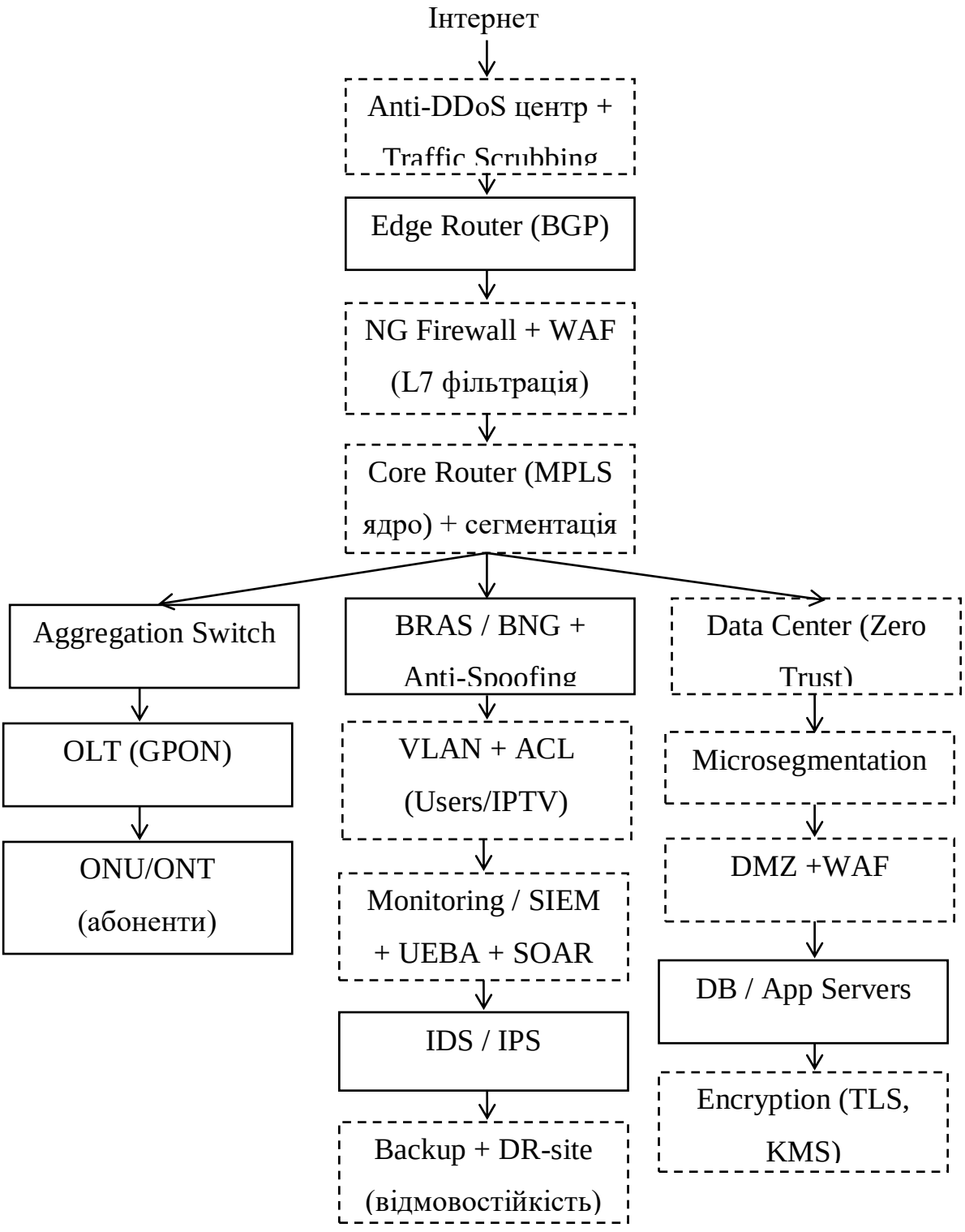

Рисунок 3.8 – Удосконалена архітектура мережі інтернет-провайдера із модулем безпеки

Інтеграція системи інфозахисту в архітектуру мережі інтернет-провайдера реалізується як розподілена багаторівнева система, що охоплює всі рівні Такий підхід забезпечує комплексний захист, мінімізує ризики компрометації та дозволяє своєчасно реагувати на сучасні загрози.

3.3 Оцінка ефективності захистсистеми

Для оцінки ефективності впровадження модуля захистсистеми інтернет-провайдера, використаємо модель (2.2). Для обчислення інтегрального показника показника ефективності, спочатку підберемо коефіцієнти, які занесемо у таблицю 3.1

Таблиця 3.1 – Критерії оцінки ефективності модуля захистсистеми інтернет-провайдера

№	Критерій оцінки	Опис критерію	Ваговий коефіцієнт
1	Ефективність виявлення загроз	Імовірність своєчасного виявлення атак, вторгнень і аномальної активності	0.3
2	Ефективність запобігання атакам	Здатність системи блокувати DDoS, сканування портів, шкідливий трафік	0.25
3	Відмовостійкість системи	Стійкість модуля захисту до перевантажень та відмов обладнання	0.15
4	Продуктивність мережі	Вплив засобів захисту на затримку, пропускну здатність і швидкість обробки пакетів	0.2
5	Доступність сервісів	Рівень безперервності надання послуг	0.1

Вагові коефіцієнти обрано експертним методом із врахуванням пріоритетності для системи захистту інтернет-провайдера. Найбільші ваги отримали критерії виявлення та блокування загроз (0,3; 0,25), середні – продуктивність і відмовостійкість (0,2; 0,15), найменшу вагу – доступність сервісів (0,1), оскільки вона залежить не лише від захистсистеми, а й від усієї мережевої інфраструктури.

Таким чином, модель для оцінювання інтегрального показника ефективності захистсистеми матиме вигляд:

$$E = 0{,}3 \cdot K_{\text{det}} + 0{,}25 \cdot K_{pre} + 0{,}15 \cdot K_{res} + 0{,}2 \cdot K_{perf} + 0{,}1 \cdot K_{avail}. \quad (3.1)$$

У результаті імітаційного моделювання віртуальної мережевої інфраструктури (див. рисунок 3.9) в умовах різного рівня навантаження та впливу типових загроз отримуємо значення основних критеріїв. На їх основі обчислюємо інтегральний показник ефективності:

$$E=0.3\cdot0.92+0.25\cdot0.88+0.15\cdot0.81+0.2\cdot0.85+0.1\cdot0.95 = 0.882.$$

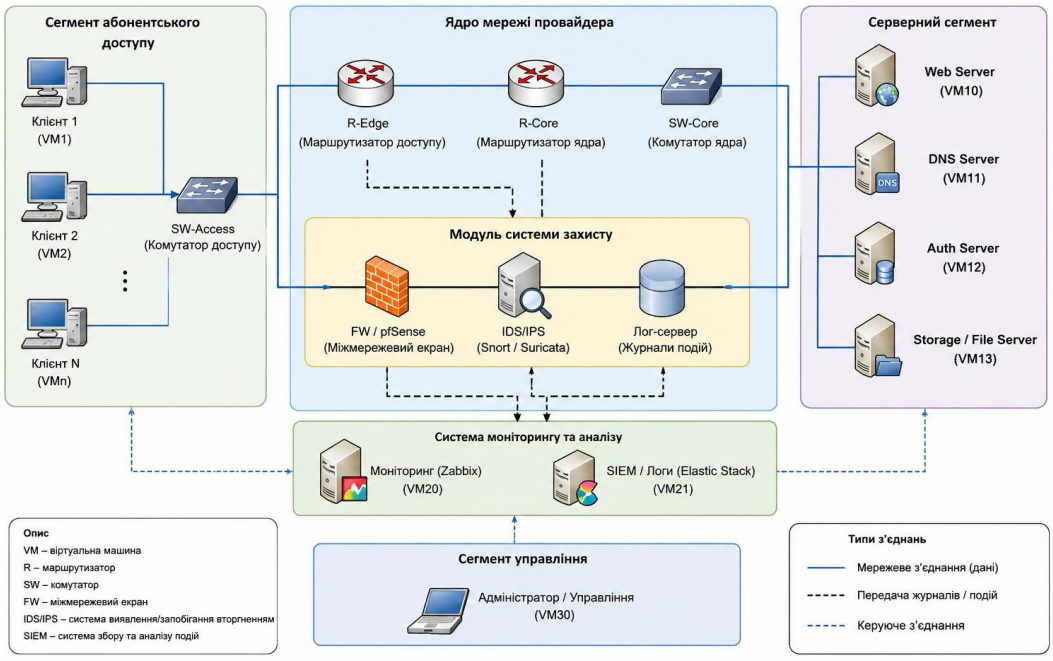

Рисунок 3.9 – Топологія віртуальної мережі провайдера

Отриманий показник свідчить про досить високий рівень ефективності – значення близьке до 1, тобто близько 90 %, функціонування захистсистеми інтернет-провайдера на основі впровадження розробленого модуля, що ґрунтується на сучасних технологіях безпеки даних, достатню стійкість до загроз та здатність підтримувати стабільну роботу мережевої інфраструктури навіть за умов підвищеного навантаження.

Тепер продемонструємо, як рівень навантаження мережі впливає на інтегральний показник ефективності захистсистеми провайдера. Для цього побудуємо графік залежності, що демонструє рисунок 3.10.

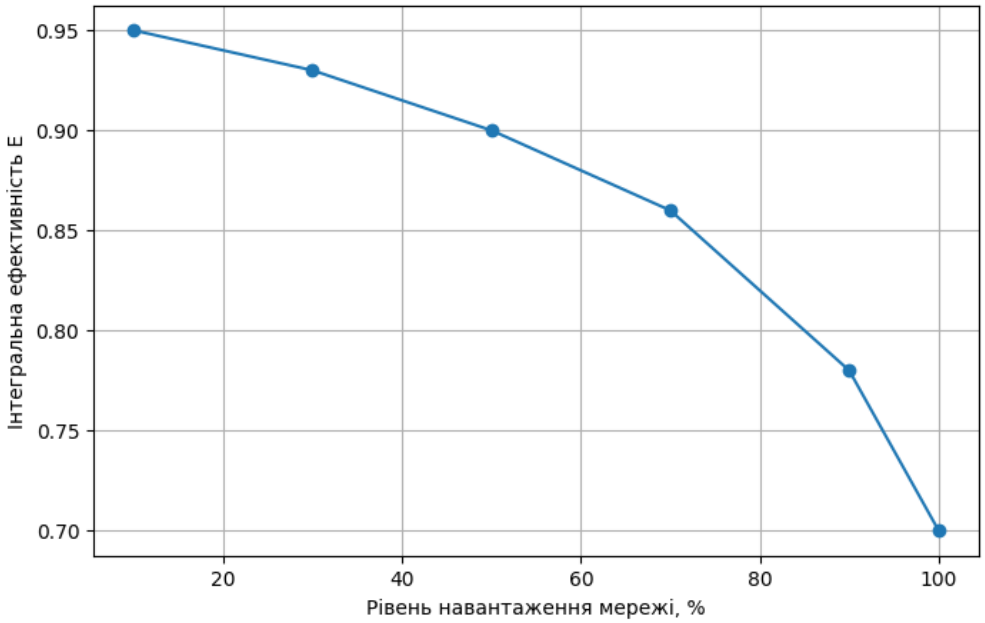

Рисунок 3.10 – Залежність ефективності захистсистеми від навантаження мережі

Як видно із графіка, зі збільшенням навантаження спостерігається поступове зниження ефективності функціонування модуля захисту через зростання затримок обробки пакетів, підвищення навантаження на IDS/IPS-механізми та збільшення ймовірності пропуску шкідливого трафіку. При цьому навіть за високого рівня навантаження (100 %) система забезпечує допустимий рівень захищеності та доступності сервісів провайдера й не викодить з ладу, проте її продуктивність дещо знижується.Техніко-економічне обґрунтування розробки захистсистеми мережі інтернет-провайдера наведено у додатку Б.

ВИСНОВКИ

У результаті виконання дослідження розв’язано практичну задачу розробка модуля інфозахисту для провайдера й при цьому отримано результати, можна сформулювати у вигляді висновків.

1. Проаналізовано нормативно-правову базу для розробки системи інфозахисту, що дозволило визначити основні вимоги до побудови захищених інформаційних систем і забезпечити відповідність розробки чинним нормативам.

2. Досліджено особливості функціонування інформаційних ресурсів інтернет-провайдера з урахуванням специфіки мережевої інфраструктури, структури трафіку та принципів надання послуг, що уможливило врахувати реальні умови експлуатації системи та адаптувати механізми захисту до середовища провайдера.

3. Проаналізовано сучасні загрози безпеки передачі даних, включаючи можливі атаки на мережеву інфраструктуру, перехоплення інформації та впливи на доступність сервісів, що дозволило визначити критичні вразливості та сформувати вимоги до системи інфозахисту.

4. Проаналізовано методи захисту інформаційних ресурсів у мережах провайдерів, зокрема криптографічні алгоритми, системи виявлення та запобігання вторгненням, що забезпечило обґрунтований вибір технологій для удосконалення системи безпеки провайдера.

5. Розроблено модель загроз, яка базується на аналізі потенційних атак, вразливостей і активів системи, що дозволило структуровано описати ризики та визначити пріоритети їх мінімізації.

6. Розроблено модель політики безпеки інформації, що визначає правила доступу, обробки та захисту даних, що забезпечило організаційне підґрунтя для функціонування системи інфозахисту.

7. Спроєктовано модуль системи інфозахисту, включаючи мережеві, програмні та організаційні засоби й інтегровано його в архітектуру мережі провайдера.

СПИСОК ВИКОНАНИХ ДЖЕРЕЛ

1. Anderson R. Security engineering: a guide to building dependable distributed systems. 2nd ed. Indianapolis: Wiley Publishing, 2008. 1040 p.
2. Dierks T., Rescorla E. The transport layer security (TLS) protocol version 1.2. RFC 5246. IETF, 2008. URL: https://datatracker.ietf.org/doc/html/rfc5246 (дата звернення: 12.01.2026).
3. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva: ISO, 2022. URL: https://www.iso.org/standard/27001 (дата звернення: 10.04.2026).
4. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection. Code of practice for information security controls. Geneva: ISO, 2022. URL: https://www.iso.org/standard/27002 (дата звернення: 11.03.2026).
5. Juniper Networks. Securing the network infrastructure. Juniper Networks, 2018. URL: https://www.juniper.net/documentation (дата звернення: 02.05.2026).
6. Kurose J. F., Ross K. W. Computer networking: a top-down approach. 7th ed. Boston: Pearson, 2016. 864 p.
7. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: National Institute of Standards and Technology, 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (дата звернення: 12.03.2026).
8. NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide. Gaithersburg: NIST, 2012. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (дата звернення: 11.04.2026).
9. Rescorla E. The transport layer security (TLS) protocol version 1.3. RFC 8446. IETF, 2018. URL: https://datatracker.ietf.org/doc/html/rfc8446 (дата звернення: 18.03.2026).

10. Scarfone K., Mell P. Guide to intrusion detection and prevention systems (IDPS). Gaithersburg: NIST, 2007. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (дата звернення: 02.04.2026).

11. Stallings W. Network security essentials: applications and standards. 6th ed. Harlow: Pearson Education Limited, 2017. 488 p.

12. Tanenbaum A. S., Wetherall D. J. Computer networks. 5th ed. Boston: Pearson, 2011. 960 p.

13. Tjoa S., Gafić M., Kieseberg P. Standards and Best Practices. In Cyber Resilience Fundamentals. Cham: Springer International Publishing. 2016. P. 23-35.

14. Бліхар М. М. Адміністративно-правове забезпечення інформаційної безпеки в мережі Інтернет. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. № 68. С. 134-138.

15. Василенко М. В., Слатвінська В. М., Рачук В. В. Аналіз несанкціонованого доступу до комп'ютерних мереж. Інформаційні технології та суспільство. 2024. № 1. С. 23-29.

16. Гвоздьов Р. Ю., Заболотний В. І., Бойко, А. О. Методика формального проектування КСЗІ в ІТС, С. 39-40.

17. Гребенніков В. Комплексні системи інфозахисту. Проектування, впровадження, супровід. Litres. 2018. 354 с.

18. Гуменяк М.О., Галяс А.В., Савчук В.А. Методи оптимізації сховища даних в інофрмаційній системі // Матеріали XXVI Всеукраїнської науково – технічної конференції молодих вчених, аспірантів та студентів «Стан, досягнення і перспективи інформаційних систем і технологій». Одеса: ОНТУ, 2026. С. 86-88.

19. Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: теоретичні аспекти. Інформація і право. 2018. № 3. С. 5-12.

20. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Основні положення. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=50868 (дата звернення: 11.03.2026).

21. ДСТУ 3396.3-97 Захист інформації. Технічний захист інформації. Порядок проведення робіт. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=50869 (дата звернення: 12.03.2026).

22. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=64013 (дата звернення: 11.03.2026).

23. Константинова Л. В., Сосна О. С. Огляд засобів комплексних систем інфозахисту. Тези доповідей. 2018. 7 с.

24. Коробейнікова Т. Метод аналізу даних від систем IDS/IPS на основі комбінування сигнатур і політик. Вісник Хмельницького національного університету. Технічні науки. 2025. № 2. С. 112-118.

25. Лукова-Чуйко Н. В., Толюпа С. В., Пархоменко І. І. Методи виявлення вторгнень у сучасних системах IDS. Безпека інформаційних систем і технологій. 2021. № 3. С. 67–73.

26. Ляпін К. Е. Виклики та можливості сучасності: комплексна система інфозахисту. Аналітично-порівняльне правознавство. 2023. Вип. 4. С. 262-265.

27. Методичні вказівки до виконання практичних робіт з дисципліни «Економіка проєктів в комп'ютерній інженерії"/ Н.Я. Савка / Під ред. Л.О. Дубчак. Тернопіль: ЗУНУ, 2025. 33 с.

28. Методичні рекомендації до виконання кваліфікаційної роботи з освітнього ступеня "Бакалавр" спеціальності 123 «Комп'ютерна інженерія» галузі знань 12 Інформаційні технології / О.М. Березький, Л.О.Дубчак, Г.М. Мельник, Ю.М. Батько, О.Й. Піцун / Під ред. Л.О.Дубчак. Тернопіль: ЗУНУ, 2026. 54 с.

29. Необхідність створення комплексної системи інфозахисту (КСЗІ). ТЗІ – інформаційна безпека та інфозахист. URL: https://tzi.com.ua/neobxdnst-stvorennya-kompleksno-sistemi-zaxistu-nformacz-ksz.html (дата звернення: 24.031.2026).

30. Павлов І. М., Бірюков В. О. Формалізація проектних показників якості інфозахисту комплексної системи інфозахисту. Ukrainian Information Security Research Journal. 2023. Вип. 13(2 (51)). С. 5-11.

31. Про електронні довірчі послуги: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 08.04.2026).

32. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 02.04.2026).

33. Про інформацію: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 10.04.2026).

34. Савлюк М. О. Значення інформаційної безпеки в сучасному цифровому середовищі. Вісник Прикарпатського університету. Серія: Політологія. 2024. № 2. С. 77-82.

35. Селіхов Д. А. Кібербезпека як складова інформаційної безпеки: теоретичні та прикладні аспекти. Аналітично-порівняльне правознавство. 2026. № 1. С. 45-50.

36. Терейковський І. А., Корченко О. О., Паращук Т. І., Педченко Є. М. Аналіз відкритих систем виявлення вторгнень. Український науковий журнал з інформаційної безпеки. 2018. № 1. С. 23-30.

37. Толюпа С. В., Самохвалов Ю. Я., Цьопа Н. В. Комплексні системи інфозахисту спеціальних об’єктів та методика їх оцінки. Сучасний інфозахист. 2014. Вип. (1). С. 81-88.

38. Чередневченко О. Ю., Фесоха В. В., Процюк Ю. О., Бондаренко Т. В. Аналіз підходів до протидії кібернетичним загрозам в інформаційно-телекомунікаційних мережах. Сучасні інформаційні технології у сфері безпеки та оборони. 2018. № 2. С. 98-104.

39. Що таке провайдер? Які його функції?. URL: https://dovidka.biz.ua/shho-take-provayder-yaki-yogo-funktsiyi/ (дата звернення: 18.01.2026).