Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Фкультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломного проекту (роботи)

магістр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: **Методи та засоби розробки та впровадження надійної, продуктивної та захищеної мережевої архітектури**

Виконав: студент (ка) 6 курсу, групи СНнм-61
спеціальності (напряму підготовки) 122
комп'ютерні науки
(шифр і назва спеціальності (напряму підготовки))

		Дубчак А.О.
	(підпис)	(прізвище та ініціали)
Керівник		Марценко С.В.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Мацюк О.В.
	(підпис)	(прізвище та ініціали)
Рецензент		Марценюк В.П.
	(підпис)	(прізвище та ініціали)

м. Тернопіль – 2020

АНОТАЦІЯ

Методи та засоби розробки та впровадження надійної, продуктивної та захищеної мережевої архітектури // Дипломна робота // Дубчак Андрій Олегович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно–інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНнм–61 // Тернопіль, 2020 // С. , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: НАДІЙНІСТЬ, ПРОДУКТИВНІСТЬ, БЕЗПЕКА, РИЗИКИ БЕЗПЕКИ, МОДЕЛІ МЕРЕЖ, МЕРЕЖЕВИЙ ДИЗАЙН.

У роботі проведено дослідження вдосконалення методів та засобів розробки та впровадження надійної, продуктивної та захищеної мережевої архітектури, що дасть змогу провести планування та використання покращених мережевих архітектур з підвищеними експлуатаційними характеристиками.

В першому розділі дипломної роботи виконано дослідження вагомих аспектів проектування комп'ютерних інформаційних мереж на прикладі великої організації. При цьому, сформовано основні вимоги до проектування методів та засобів побудови і впровадження надійних, продуктивних та захищених мережевих архітектур. Здійснено огляд трирівневої моделі дизайну та її спрощеної дворівневої версії для компаній з різними вимогами до роботи мереж. На основі проведеного аналізу виявлено та прокласифіковано види та типи мережевих загроз безпеці інформаційних ресурсів. Розглянуто методи протидії інформаційній безпеці, що базуються на системах виявлення та реагування загрозам ресурсів мережі.

В другому розділі дипломної роботи для підвищення надійності функціонування комп’ютерних мереж запропоновано використання методів аналізу та управління трафіком, що базуються на протоколах SNMP та Syslog, що дало змогу в реальному часі проводити моніторинг роботи мережевих компонентів та аналізувати інциденти з фіксацією часу події. Використано при забезпечені організаційно-технічних засобів забезпечення працездатності мережі впровадити AAA сервери для забезпечення аутинтифікації, а також розроблено рекомендації для створення надійних паролів. Проведено аналіз управління ризиками мережевої безпеки. Подано систему управління безпекою. Наведено алгоритми криптування інформації для покращення роботи системи. Запропоновано проект вдосконалених методів та засобі розробки та впровадження надійної, продуктивної та захищеної архітектури.

Метою дослідження є аналіз мережевих архітектур та технологій для розробки та впровадження методів та засобів організації надійних, продуктивних та захищених інформаційно-комунікаційних мереж, що дадуть змогу провести покращеня мережевих архітектур і забезпечити підвищення експлуатаційних характеристик. Для досягнення поставленої мети необхідно виконати наступні завдання: провести аналіз та порівняння існуючих мережевих архітектур, що дасть змогу визначити технічні та організаційні аспекти покращення надійності, продуктивності та захисту; дослідити методи та засоби безпеки комп’ютерних мереж, що дасть змогу визначити шляхи та напрямки їх вдосконалення; на основі проведеного аналізу розробити рекомендації щодо вдосконалення методів та засобів впровадження надійної, продуктивно та захищеної архітектури, що буде задовольняти вимоги до роботи організацій широкого спектру діяльності.

Об’єкт дослідження – процес передавання та захисту даних в мережах.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних.

ANNOTATION

Methods and tools of development and implementation of reliable, efficient and secure network architecture // Diploma thesis Master degree // Dubchak Andrii O. // Ternopil’ Ivan Pul’uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2020 // P. , Tables – , Fig. – , Diagrams – , Annexes. – , References – .

The research has been carried out on the methods and technologies, the development and use of reliable, productive and protected network architectures, which allow to propose the planning and improvement of advanced network architectures using the most important characteristics.

The first section of the thesis explored important aspects of designing computer information networks on the example of a large organization. At the same time, the basic requirements to the design of methods and means of construction and implementation reliable, productive and secure network architectures are generalized. The design of three-tier model and simplified two-tier version that can work in companies of different size was reviewed. Based on the analysis, the types of network threats to the security of information resources have been identified and classified. Methods of counteracting information security based on systems for detecting and responding to network resources threats are considered..

In the second section of the thesis to increase the reliability of computer networks, the use of methods of analysis and traffic management based on SNMP and Syslog protocols was proposed, which allowed real-time monitoring of network components and analyze incidents with time recording. Used to provide organizational and technical means to ensure the network's ability to implement AAA servers to ensure authentication, as well as developed recommendations for creating strong passwords. The analysis of network security risk management is carried out. A security management system is provided. Algorithms for encrypting

information to improve system performance are presented. The project of improved methods and means of development and implementation of reliable, productive and protected architecture is offered.

The aim of the study is to analyze network architectures and technologies for the development and implementation of methods and tools for organizing reliable, productive and secure information and communication networks that will improve network architectures and performance. To achieve this goal, the following tasks must be performed: to analyze and compare existing network architectures, which will identify technical and organizational aspects of improving reliability, performance and protection; to study methods and means of security of computer networks, which will allow to determine the ways and directions of their improvement; on the basis of the conducted analysis to develop recommendations on improvement of methods and means of introduction of reliable, productive and protected architecture that will satisfy requirements to work of the organizations of a wide range of activity.Project overview - process transfer and data transfer in moderation.

The object of research is the process of data transmission and protection in networks.

The subject of research - the theory of telecommunication networks design, the theory of data transmission.

Key words: RELIABILITY, PRODUCTIVITY, SECURITY, SECURITY RISKS, NETWORK MODELS, NETWORK DESIGN.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IP – Internet Protocol

DHCP – Dynamic Host Configuration Protocol

OSI – Open System Interconnection

IDS – Intrusion Detection Sysytem

IPS – Intrusion Prevention Sysytem

AMP – Advanced Malware Protection

WSA – Web Security Appliance

NTP – Network Time Protocol

ICMP – Internet Control Message Protocol

AAA – Authentication, Authorization, Accounting

TACACS – Terminal Access Controller Access Control System

ЗМІСТ

ВСТУП

Головною вимогою, що пред’являється до мереж, є виконання мережею її основної функції – забезпечення користувачам потенційної можливості доступу до ресурсів всіх комп'ютерів об’єднаних в мережу. Всі інші вимоги продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість пов’язані з якістю виконання цієї основної задачі.

Розвиток комп’ютерних мереж донедавна відбувався екстенсивним шляхом: дедалі більше пристроїв об’єднувалося в локальні і глобальні мережі, удосконалювалося мережеве обладнання, зростала пропускна здатність каналів передавання даних, підвищувалася швидкодія серверів і мережевих компонентів. Проте принципово нові вирішення не набувають, як правило, широкого впровадження, і поступово існуючі мережі перестають справлятися зі стрімко зростаючою кількістю пристроїв і потоків даних. Мережевий трафік і його структура зазнали зрештою істотних змін, оскільки кожний запит породжує численні звернення до серверів додатків, баз даних, інших систем зберігання та обробки інформації. Складність сучасної мережевої інфраструктури, а також зростання трафіку призводять до все частіших відмов, а отже, і до різкого погіршення швидкісних характеристик передавання даних.

При цьому існуюча мережева архітектура, зорієнтована на групу досить застарілих протоколів для забезпечення взаємодії, ускладнюється мережевими пристроями, що стають на заваді масштабуванню. Додавання нових пристроїв вимагає великих зусиль, передусім щодо перенастроювання комутаторів, маршрутизаторів і мережевих засобів захисту. Натомість мережева структура, залишаючись статичною, потребує значних коштів для її підтримання.

З повною упевненістю можна стверджувати, що сьогодні паперові підписи, архіви та штампи практично припинили своє існування, а на зміну їм прийшов світ електронних технологій, в якому значно полегшується доступ до даних і їх подальший пошук. Крім того, у багато разів збільшується ефективність праці та швидкість взаємодії. Але, з впровадженням у наше життя сучасних іноваційних технологій, інформація кожної організації не стає менш важливою.

Витік інформації може спричинити за собою серйозний фінансовий збиток, а часом навіть стати причиною втрати позицій підприємства на ринку. Сьогодні вже не достатньо поставити якісний замок та закрити кімнату з цінними паперами на ключ, включивши сигналізацію. Оскільки фізично документа в електронному вигляді не існує, стає дуже складно тримати під контролем доступ до файлів або вчасно помітити витік документів.

Актуальність теми. Значне зростання обсягів інформації створює необхідність розробки нових методів та засобів забезпечення надійності та продуктивності її передавання, а висока інтеграція сучасних мереж в глобальні технології вимагає захисту від несанкціонованого доступу. Тому важливою та актуальною є задача організації високопродуктивних мережевих архітектур, що здатні протистояти загрозам сучасного світу і задовольняти потреби теперішнього часу та майбутніх викликів.

Мета і завдання дослідження. Метою дослідження є аналіз мережевих архітектур та технологій для розробки та впровадження методів та засобів організації надійних, продуктивних та захищених інформаційно-комунікаційних мереж, що дадуть змогу провести покращеня мережевих архітектур і забезпечити підвищення експлуатаційних характеристик. Для досягнення поставленої мети необхідно виконати наступні завдання: провести аналіз та порівняння існуючих мережевих архітектур, що дасть змогу визначити технічні та організаційні аспекти покращення надійності,

продуктивності та захисту; дослідити методи та засоби безпеки комп’ютерних мереж, що дасть змогу визначити шляхи та напрямки їх вдосконалення; на основі проведеного аналізу розробити рекомендації щодо вдосконалення методів та засобів впровадження надійної, продуктивно та захищеної архітектури, що буде задовольняти вимоги до роботи організацій широкого спектру діяльності.

Об’єкт дослідження – процес передавання та захисту даних в мережах.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних.

Практичне значення одержаних результатів. Виконано дослідження вагомих аспектів проектування комп’ютерних інформаційних мереж на прикладі великої організації. При цьому, сформовано основні вимоги до проектування методів та засобів побудови і впровадження надійних, продуктивних та захищених мережевих архітектур. Здійснено огляд трирівневої моделі дизайну та її спрощеної дворівневої версії для компаній з різними вимогами до роботи мереж. На основі проведеного аналізу виявлено та прокласифіковано види та типи мережевих загроз безпеці інформаційних ресурсів. Розглянуто методи протидії інформаційній безпеці, що базуються на системах виявлення та реагування загрозам ресурсів мережі. Для підвищення надійності функціонування комп’ютерних мереж запропоновано використання методів аналізу та управління трафіком, що базуються на протоколах SNMP та Syslog, що дало змогу в реальному часі проводити моніторинг роботи мережевих компонентів та аналізувати інциденти з фіксацією часу події. Використано при забезпечені організаційно-технічних засобів забезпечення працездатності мережі впровадити AAA сервери для забезпечення аутинтифікації, а також розроблено рекомендації для створення надійних паролів. Проведено аналіз управління ризиками мережевої безпеки.

Подано систему управління безпекою. Наведено алгоритми криптування інформації для покращення роботи системи.

Наукова новизна розробки: запропоновано проект вдосконалених методів та засобі розробки та впровадження надійної, продуктивної та захищеної архітектури, що дасть змогу врахувати при проектуванні нових інформаційно-комунікаційних систем необхідні аспекти забезпечення основних характеристик.

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Аналіз нідійних мережевих архітектур

За результатами проведеного аналізу літературних джерел [1-30] вдалось визначити ключові, на сьогоднішній день, моделі мережевого дизайну, що можуть бути використані або є доцільними для інтеграції в сучасні мережеві архітектури. В подальшому викладі матеріалу розглянуто основні характеристики, визначено переваги та недоліки вибраних технологій.

Одним з найкращих варіантів аналізу мережевих архітектур є корпоративна мережа. Вона містить набір взаємопов’язаних та спільно працюючих апаратно-прорамних елементів, що надає можливість передавати дані між різними програмними додатками та сервісами. Як наслідок така мережа спроектована для вирішення завдань конкретної організації та призначена для використання тільки працівниками, що є її співробітниками.

При створенні мережі організації застосовують загальні принципи побудови телекомунікаційних мереж. При цьому враховується організаційна структура, що відображає характер діяльності. Відділи та підрозділи мають бути чітко визначеними і обмін даними між ними повинен бути строго регламентований. В залежності від розміру організації можна виділити локальні мережі структурних одиниць або мережі кампусу, що поєднують різні будівлі, які належать даному підприємству. Основним завданням мережі відділу чи підрозділу є надання відповідних локальних ресурсів, що використовуються ними для ведення своєї діяльності. Також така мережа характеризується типовим програмним забезпеченням та операційними системами. В свою чергу мережа кампусу надає більш широкий спектр послуг і є більш неоднорідною. На практиці також використовують можливість під’єднання віддалених офісів або працівників до корпоративної

мережі. В такому випадку доцільно впроваджувати технології глобальних мереж (WAN). Для побудови мережі відділів та підрозділів використовують горизонтальне кабелювання, а для з'єднання між будинками в межах кампусу – вертикальне. В сучасних мережах горизонтальне кабелювання базується на технології Fast Ethernet або Gigabit Ethernet. В той же час вертикальне може використовувати Gigabit Ethernet та вище. При організації каналів зв'язку потрібно враховувати можливість виникнення вузьких місць у випадку неправильно підібраних технологій горизонтального та вертикального з'єднань. Щоб уникнути таких ситуацій потрібно чітко розуміти об'єми потоків даних, що проходять між різними частинами мережі організації.

Особливістю корпоративних мереж є їх гетерогенність структури, що зумовлена використанням різних типів комп'ютерів, операційних систем та сервісів, що використовуються в мережі. Основним завданням таких мереж є забезпечення повноцінного функціонування всіх систем і забезпечення користувачам можливостей їх використання. Великі мережі доцільно розглядати як рівневу модель, в нижніх рівнях якої буде розміщено користувацьке обладнання (комп'ютери, мережеві принтери, IP телефони та ін.). На вищому рівні знаходиться транспортна мережа, яка надає можливість управління та передавання даних між різними складовими нижчого рівня. Над транспортним рівнем працює кореневий рівень, основним завданням якого є швидка маршрутизація даних та забезпечення WAN сервісів. Як варіант організації корпоративної мережі є можливість використання доступних сервісів віртуалізації мережевих ресурсів, що надає гнучкість побудови та експлуатації, впровадження нових сервісів, забезпечення якості передавання даних. У великих корпоративних мережах можливе створення ще одного підрівня у вигляді центру обробки та збереження даних. Це пов'язано з великою кількістю необхідної інформації, котра використовується організацією для її роботи, а також необхідністю захисту та швидкого доступу до неї. В таких серверних фермах можуть

використовуватись спеціальні технології створення мереж збереження даних SAN. Для швидкого доступу до часто використовуваних ресурсів компанії розгортають свої сервери розв’язування доменних імен DNS, динаміного надання IP адрес DHCP і т.д.

Організація технологічної мережі опирається на використання високопродуктивного мережевого обладнання, що здатне виконувати поточні завдання та швидко інтегрувати нові технології. Це суттєво збільшує вартість побудови та експлуатації мережі, а також додає певні вимоги до обслуговуючого персоналу, який буде налаштовувати та підтримувати працездатність її роботи. Частковим виходом є використання сервісів віртуалізації ресурсів, проте, це ще більше додає вимог до людей, які будуть це робити. Узагальнюючи вимоги до створення та експлуатації сучасної корпоративної мережі можна виділити:

– мережа повинна використовувати високопродуктивні засоби для забезпечення високої доступності сервісів, що надаються в ній (HA - High Availability);

– забезпечувати високу масштабованість для збільшення кількості користувачів без втручання в початковий дизайн;

– для зменшення кількості дротів надавати подачу живлення через мережевий кабель (PoE - Power over Ethernet).

Одним з ключових факторів успішного функціонування корпоративної мережі є можливість мережевого моніторингу її ресурсів. При збільшенні кількості маршрутизаторів та комутаторів необхідно впроваджувати автоматизовані засоби моніторингу та управління. Такі засоби дадуть змогу вести логування подій і у випадку нестандартних ситуацій провести дослідження причин їх виникнення. Для забезпечення цих цілей існує низка стандартизованих засобів таких як SNMP. Для коректної роботи моніторингу потрібно забезпечити контроль правильності системного часу. Це можна зробити використовуючи синхронізацію через протокол NTP.

Проводячи аналіз сучасних мережевих дизайнів можна виділити дві основні моделі організації мережевих ресурсів у вигляді дворівневої та трирівневої моделей. Трирівнева модель була придумана першою і є дещо складнішою ніж дворівнева та складається з:

– рівня доступу користувацького обладнання;
– рівня розподілу мережевих ресурсів;
– кореневого рівня мережі.

На першому рівні забезпечується необхідна кількість точок під'єднання користувацького обладнаня та генерується трафік. Конроль дозволу на використання мережі через фізичний рівень повинен бути реалізований саме на цьому рівні. До основних завдань, що вирішує рівень розподілу можна віднести:

– зменшення можливих наслідків від зміни топології;
– управління наявними маршрутами в таблиці маршрутизації;
– об'єднання користувацького трафіку для підготовки до передавання через кореневий рівень.

Організація маршрутизації між під мережами окремих структурних одиниць організації виконується на цьому рівні. Додатково можуть бути введені правила політики безпеки, що відповідають загальній політиці безпеки організації. Контроль якості послуг забезпечує необхідну пріоритизацію трафіку чутливого до затримок або важливого з точки зору діяльності організації. Створення надлишкових каналів зв'язку підвищує надійність передавання даних та відмовостійкість мережі.

При організації кореневого рівня основними факторами, що відіграють ключову роль є швидкість передавання даних та комутація пакетів. На основі цього цей рівень не обтяжують додатковими технологіями та правилами обробки. У великих мережах рівень ядра мережі може містити багато маршрутизаторів і використовувати функції віртуалізації для

підвищення надійності функціонування. На рисунку 1.1 подано візуальне представлення такої моделі мережі для корпоративних застосувань.

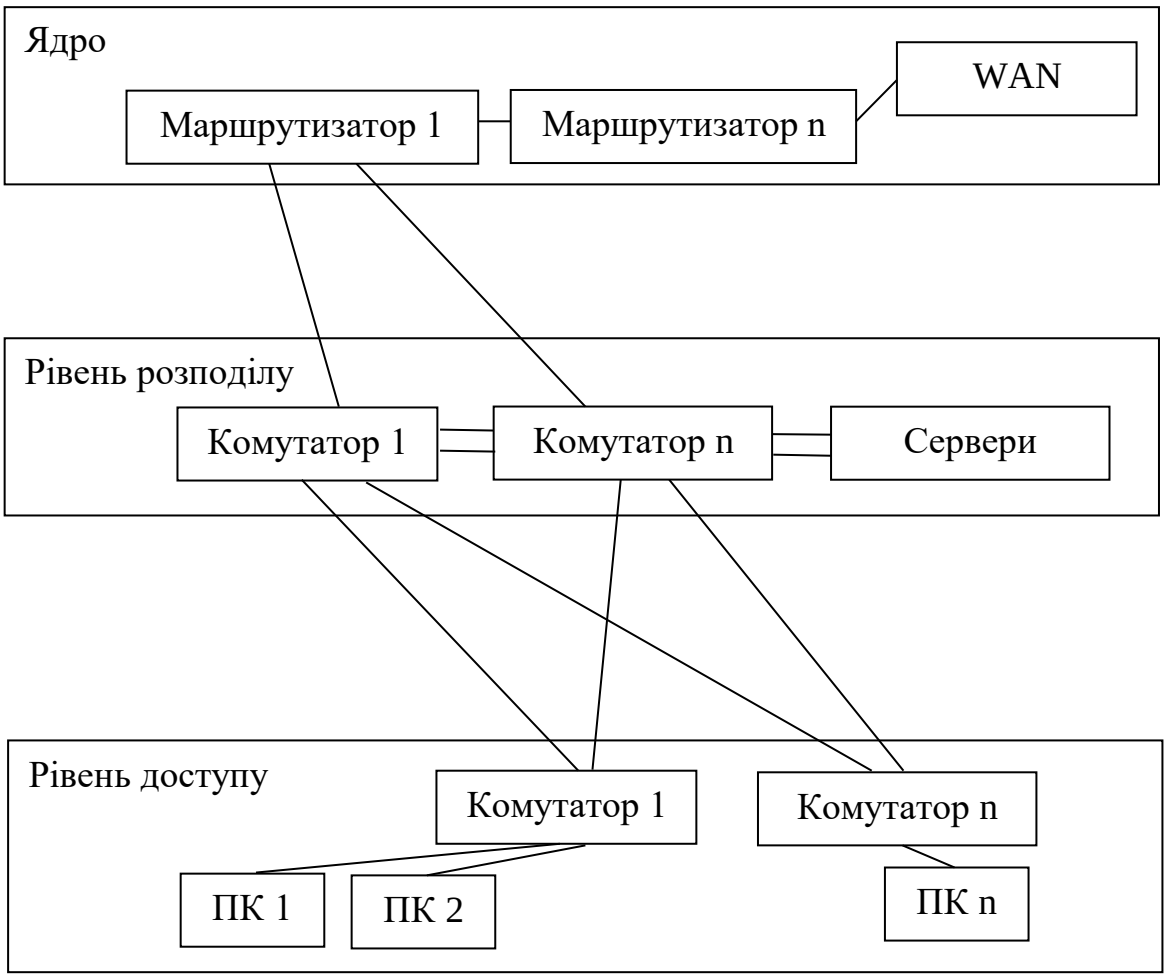

Рисунок 1.1 – Трирівнева модель дизайну мережі

У компаніях невеликого розміру або де об’єми трафіку є не настільки великими можливе спрощення трирівневої моделі до дворівневої. При цьому деякі функції об’єднуються, що приводить до зменшення структурних елементів мережевого дизайну. Наприклад, швидка комутація пакетів та функції маршрутизації можуть бути об’єднані при використанні комутаторів третього рівня, що здешевлює побудову мережі та спрощує її обслуговування. Разом з цим, надійність таких мереж не зменшується через використання дублювання каналів зв’язку та забезпечення надлишкової

надійності мережевого устаткування. При об’єднанні верхніх двох рівнів попередньої моделі отримується спрощена дворівнева модель подана на рисунку 1.2. Такий підхід може бути використаний при організації офісів віток основної компанії де повноцінний трирівневий дизайн непотрібний, а спрощений буде виконувати всі покладені на нього функції.

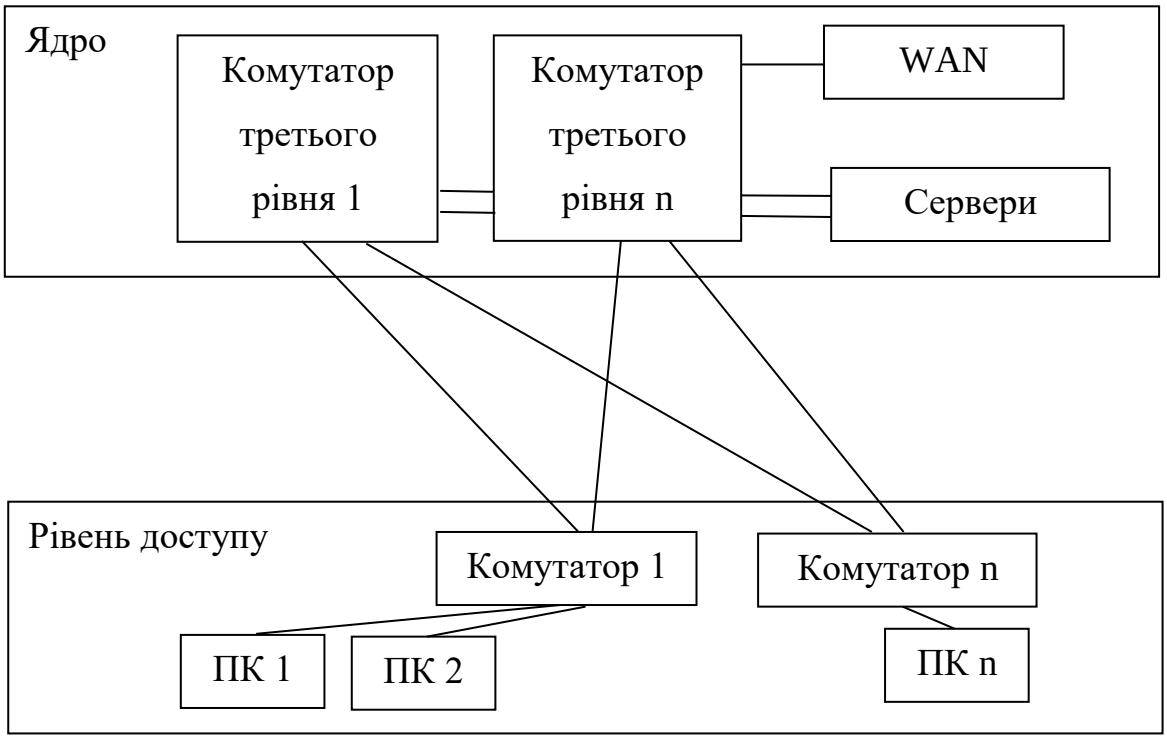

Рисунок 1.2 – Дворівнева модель дизайну мережі

При виборі активного мережевого устаткування слід враховувати технічні характеристики, що відповідають поставленим задачам та вибраному мережевому дизайну. До основних параметрів, що повинні бути враховані на рівні доступу користувачів має бути кількість портів для підключення, можливість надавати живлення через мережевий кабель, наявність функції безпеки підключення до порта. Комутуюче обладнання повинно мати протокол запобігання петель комутації для організації надлишкових каналів. Технологія віртуальних мереж дасть змогу гнучко провести організацію поділу на підрозділи і контроль обміну даними між

ними. При виборі обладнання потрібно враховувати сумісність роботи пристроїв від різних виробників. Об’єм мережевого трафіку, що може опрацювати активне мережеве обладнання визначається пропускною здатністю портів та кількістю пакетів, які опрацьовуються. Суттєве завищення цих показників приводить до зростання вартості і ускладнює побудову мережі. Завжди повинен зберігатись баланс між необхідною продуктивністю та вартістю. При можливості доцільно розглянути технології централізації мережевих ресурсів через створення програмно-конфігурованих мережевих рішень.

Аналіз процесу створення мережі

Сучасні мережі характеризуються великими об’ємами даних і відповідно складністю правил їх обробки. Це суттєво збільшує навантаження на мережевих адміністраторів і вимагає правильного підходу до створення мереж різного розміру. Гетерогенність структури мережі вимагає універсальності мережевого обладнання та стандартизованості підходів та технологій. При цьому слід враховувати процеси, що відбуваються на різних рівнях OSI моделі. Якщо на верхніх рівнях ці процеси є більш закритими і залежать від розробників програмного забезпечення, то починаючи з мережевого рівня повинні бути проаналізовані розробниками мережі.

Основною функцією мережевого рівня є маршрутизація трафіку базуючись на таблицях маршрутизації та правилах безпеки, якщо такі використовуються. Формування цих таблиць та обробка записів в них повинні бути контрольовані і прогнозовані для правильної роботи мережі. Від їх коректності буде залежати швидкість опрацювання пересилання даних. Безкласова маршрутизація реалізовується на цьому рівні. Оскільки маршрутизатори виконують роль шлюзів, протоколи забезпечення надійності доступності цих пристроїв мають бути прийняті до розгляду. Засоби

трансляції мережевих адрес NAT та правила контролю доступу ACL суттєво покращують роботу мережі і реалізовуються на маршрутизаторах.

Рівень комутації даних відноситься до канального рівня моделі мережевої взаємодії. Рішення приймаються на основі MAC адрес, що зберігаються у відповідних таблицях. Особливу увагу потрібно приділити формуванню цих таблиць, оскільки структура кадру не має полів життя TTL які є в IP пакеті. Неправильна інформація в таблицях комутації може привести до попадання кадру в петлю комутації і це може створювати помилки як на програмному рівні, так і на рівні комутації. Бродкаст повідомлення теж будуть перевантажувати мережу з великими таблицями комутації, тому технології віртуальних мереж дадуть змогу розбити широкомовні домени на менші за охопленням. Безпека портів комутаторів дасть змогу унеможливити несанкціоноване підключення до ресурсів мережі.

Правильний дизайн мережі – запорука її нормального функціонування та можливості росту без кардинальних змін. При розробці дизайну мережі потрібно визначити основні цілі які необхідно вирішити. До основних цілей мереженого дизайну можна віднести:

– функціональність – мережа повинна працювати швидко і надійно та дозволяти користувачам виконувати свою роботу;

– масштабованість – мережа повинна рости. Дизайн мережі повинен бути розроблений таким чином, щоб ріст мережі не зачіпав початкового дизайну;

– адаптивність – можливість мережі використовувати новітні технології при їх виникненні. Тобто, в мережі не повинно бути елементів, що будуть обмежувати її вдосконалення і оновлення;

– керованість – мережа повинна забезпечувати моніторинг роботи та керування нею для впевненості в правильному функціонуванні.

Процес створення мережі можна показати у вигляді життєвого циклу мережі рисунок 1.3.

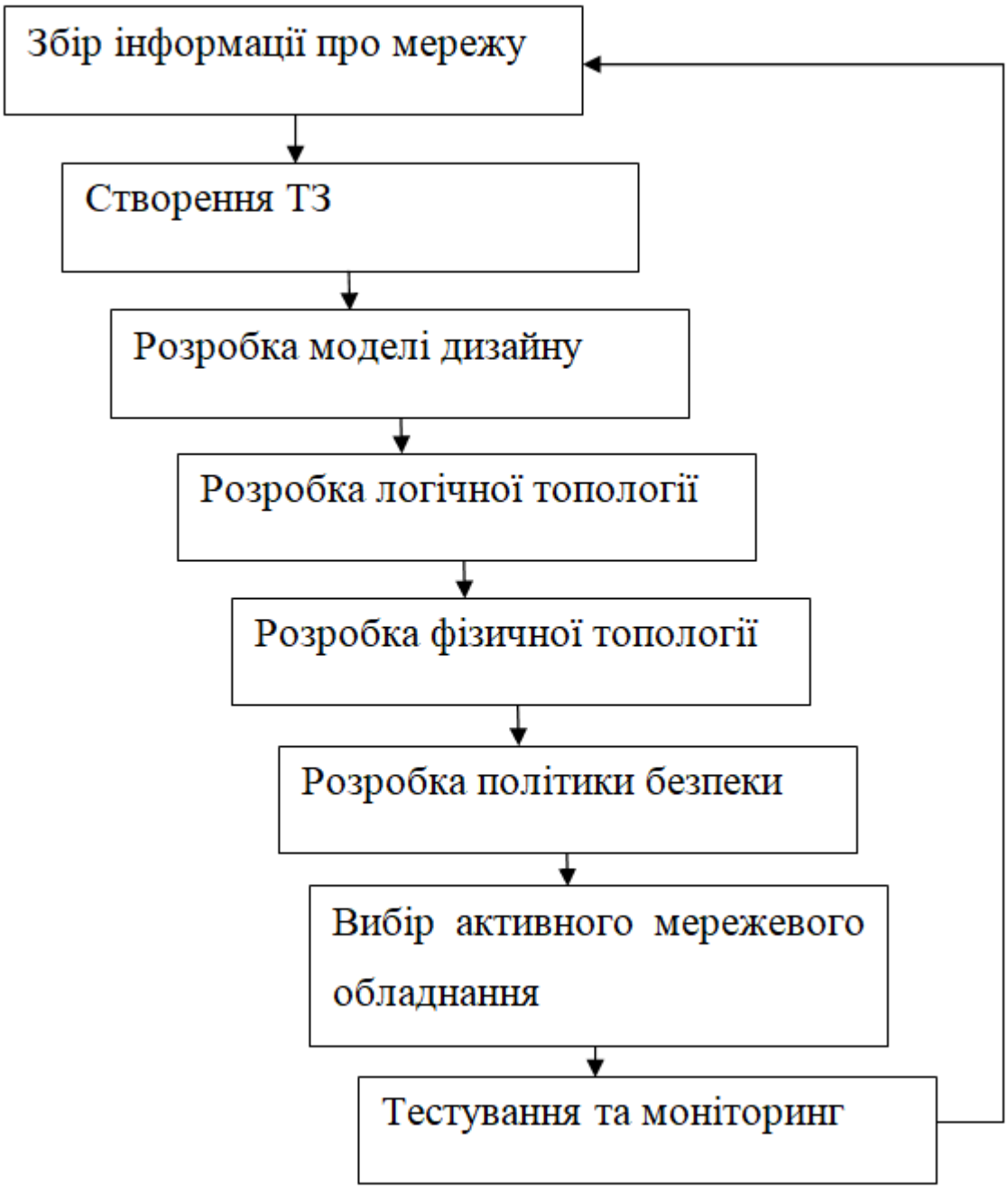

Рисунок 1.3 – Життєвий цикл мережі

Для досягнення цілей описаних вище потрібно провести попередню роботу з дослідження вимог організації, щодо роботи мережі. Такі дослідження проводять методом опитування працівників та керівництва організації. Наприклад, питання для опитування можуть бути:

– хто за фахом люди, що працюють в мережі?;

– який рівень практичних знань в користувачів?;

– яким є відношення людей до комп’ютерів та прикладних програм?;

– яким чином є розробленою та задокументованою політика безпеки фірми?;

– які дані в мережі вважаються критичними?;

– які операції визначаються як критичні?

– які протоколи мають бути дозволені в мережі?

– хто є відповідальним за адресацію, іменування, дизайн топології та конфігурування?

– які людські, апаратні та програмні ресурси має організація?

– як ці ресурси розподіляються і використовуються?

– які фінансові ресурси є в організації для проведення робіт щодо побудови мережі?

Все вищезгадане дасть змогу вибрати правильний підхід до розробки та побудови надійної, продуктивної та захищеної мережевої архітектури.

Аналіз особливостей організації мережевої безпеки

Зростання кількості та важливості інформаційних ресурсів зумовлює необхідність розробки та впровадження відповідних методів та засобів організації їх захисту. Сучасні комп’ютерні мережі містять велику кількість пристроїв, програмних додатків та сервісів. Всі ці елементи потребують детального аудиту для створення компклесної системи захисту інформації [1-30].

Організація безпеки даних – це створення системи захисту мережевих ресурсів від пошкодження та втрати, модифікації, розголошення даних.

Для створення та убезпечення захисту інформаційних систем організації створюють відповідні посади та відділи, розробляють політики

безпеки, які покликані гарантувати безперебійність роботи та цілісність даних. При цьому доцільним є розроблення багаторівневої системи захисту даних, що включає:

– інтегровані в системні та програмні засоби убезпечення, які можуть включати важко дешифровані паролі, розмежування прав доступу та ін.;

– засоби фізичного захисту мережевих ресурсів – виділення окремих серверних кімнат, що замикаються, встановленя системи відео спостереження, сигналізації;

– забезпечення документальної підтримки захисту інформаційних ресурсів – заходи організаційного характеру, створення відповідних наказів, розпоряджень;

– створення та виконання законів покликаних забезпечити захист інформації та ресурсів мережі.

Аналіз рівнів захисту інформаційних ресурсів на основі книги “Критерії оцінки безпеки компютерів” дав змогу визначити сім рівнів убезпечення інформаційних та мережевих систем:

- D – рівень найменшого убезпечення (“Minimal Protection”). Призначений для систем, що неможуть гарантувати потрібного рівня убезпечення за іншими рівнями;
- C1 – рівень селективного убезпечення (“Discretionary Protection”). Уможливлює застосування обмежень до приватної інформації;
- C2 – “рівень керованого доступу (Controlled Access Protection)”. Включає в себе необхідний захист C1 і додає елементи захисту реєстрації в системах, обліку відповідних подій захисту, ізолювання ресурсів певних процесів;
- B1 – категоризований рівень убезпечення (“Labeled Protection”). Розширює вимоги рівня C2 можливістю

файлового захисту, їх вмісту за допомогою спеціальних міток безпеки, що збережені з даними елементами. Для подолання такого захисту потрібна висока підготовка хакера і звичайному користувачеві він не під силу;

— B2 – “рівень структурованого захисту (Structured Protection)”. Ускладнює вимоги рівня B1 повним захистом усіх інформаційних ресурсів, що можуть бути доступні користувачеві. Припускається, що даний варіант захисту неможливо зламати хакерам;

— B3 – “рівень доменів безпеки (Security Domains)”. Розширює рівень B2 явною специфікацією користувачів, що мають заборонений доступ до інформаційних ресурсів, доповнено реєстрування можливо загрозливих подій. Припускають, що програмісти високого рівня невзмозі подолати такі системи;

— A1 – “рівень верифікованої розробки (Verified Design)”. Найповніший з рівнів захисту. Припускають, що в інформаційні системи цього рівня захисту не проникне ніхто.

Існує три основні типи загроз, що класифікуються за метою впливу:

– “загрози порушення конфіденційності інформації”;

– “загрози порушення цілісності інформації”;

– “загрози порушення працездатності системи (відмови в обслуговуванні)”.

Перший тип загроз має на меті розголошення інформації з обмеженим доступом чи секретів. За таких умов витік інформації приводить до ситуації, коли вона стає відомою особам не призначеним для неї. З точки зору мережевої безпеки – це ситуація коли відбувається несанкціонований доступ до конфіденційної інформації, що зберігається в інформаційних ресурсах системи чи під час її передавання.

При загрозах відносно цілісності інформації спостерігається зміна чи знищення змісту інформації, що зберігається чи передається в інформаційних системах. Такий тип загроз може бути спровокований спеціально для здійснення зловмисницьких дій або через вплив факторів зовнішнього середовища. Особливо загрозливим цей тип є для телекомунікаційних мереж.

Одним з найпоширеніших типів загроз є порушення працездатності інформаційних систем внаслідок атак відмови в обслуговуванні. При цьому спостерігається суттєве погіршення показників роботи системи або унеможливлення такої взагалі.

До основних елементів інформаційних систем, що потребують захисту можна віднести:

- апаратні ресурси мережі;
- програмне забезпечення та сервіси;
- убезпечення інформації;
- людські ресурси

Взагальному всі впливи на роботу мережі можна розділити на випадкові та спеціально створені. При розробці та впроваджені методів та засобів організації надійних, продуктивних та захищених мережевих архітектур спостерігається набір випадкових впливів. Основними причинами їх виникнення може бути:

- втрата електричного живлення або природні явища;
- поламка або некоректна робота апаратних засобів;
- недосконалість програмного забезпечення;
- недостатній освітній рівень персоналу та користувачів;
- неправильне проектування мережі.

Загрози навмисного характеру пов’язані з спланованими діями зловмисника, який може працювати в даній організації, відвідувати її чи виконувати завдання на замовлення.

До типових загроз навмисного характеру можна віднести:

– доступ до конфіденційної інформації людей, що не є працівниками даної організації;

– порушення співробітниками правил доступу до інформації і отримання такої з якою вони не повинні працювати;

– недозволене створення копій програмних продуктів та інформації;

– крадіжка вінчестерів чи інших засобів збереження даних з важливою інформацією;

– крадіжка документації;

– пошкодження чи видалення важливої інформації;

– недозволене внесення змін в бази даних чи модифікування інформації;

– підміна інформаційних повідомлень під час передавання в інформаційних мережах;

– крадіжка апаратури.

Загрози інформаційним мережам можуть бути не тільки внутрішніми, а й зовнішніми. Вони реалізуються через вплив на інформаційні системи використовуючи канали зв’язку. При цьому в таких атаках можуть бути задіяні проміжні попередньо скомпроментовані кластери мереж. Протидія таким зловмисним діям потребує ретельної підготовки та розробки планів дій для виявлення та знешкодження зловмисного впливу.

Таблиця 1.1 показує основні напрямки створення загроз мережевій безпеці інформаційних систем і дає змогу узагальнити ситуації, які виникають при порушеннях політики безпеки організації. Чітке розуміння та усвідомлення типових загроз дає змогу створювати відповідні алгоритми протидій та формувати правильну політику безпеки організації. Відсутність документації, яка повідомляє працівників про умови забезпечення інформаційної безпеки можуть привести до неможливості притягнення до відповідальності в законний спосіб.

Таблиця 1.1 – Напрямки створення загроз безпеці

Об'єкти впливу	**Порушення конфіденційності інформації**	**Порушення цілісності інформації**	**Порушення працездатності системи**
Апаратні засоби	Несанкціонований доступ – підключення; використання ресурсів; викрадення носіїв	Несанкціонований доступ – підключення; використання ресурсів; модифікація, зміна режимів	Несанкціонований доступ – зміна режимів; виведення з ладу; пошкодження
Програмне забезпечення	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – впровадження „троянських коней", „вірусів", „черв'яків"	Несанкціонований доступ – спотворення; знищення; підміна
Дані	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – спотворення; модифікація	Несанкціонований доступ – спотворення; знищення; підміна
Персонал	Розголошення; передача відомостей про захист; халатність	"Маскарад"; вербування; підкуп персоналу	Покидання робочого місця; фізичне усунення

Визначення можливих типів мережевих загроз дає змогу розробити програмно-технічні, організаційні заходи убезпечення інформаційних мереж та ресурсів.

Методи захисту мереж

Важливо розуміти різні типи брандмауерів та їх конкретні можливості, щоб правильний брандмауер використовувався для кожної ситуації. Тому аналіз доступних типів брандмауерів дасть змогу визначити доцільність використання того чи іншого варіанту:

– брандмауер пакетної фільтрації (без стану) – зазвичай маршрутизатор з можливістю фільтрувати певний пакетний вміст, наприклад, Layer 3, а іноді і Layer 4 відповідно до набору налаштованих правил;

– брандмауер Стану – Брандмауер перевірки стану, дозволяє або блокує трафік на основі стану, порту та протоколу. Він стежить за всією діяльністю від відкриття з'єднання до її закриття. Рішення про фільтрацію приймаються на основі правил, визначених адміністратором, так і контексту, що стосується використання інформації з попередніх з'єднань та пакетів, що належать до того ж з'єднання;

– брандмауер програмного шлюзу (брандмауер проксі) – фільтрує інформацію на рівнях 3, 4, 5 та 7 еталонної моделі OSI. Більша частина контролю і фільтрації брандмауера виконується програмним забезпеченням. Коли клієнт повинен отримати доступ до віддаленого сервера, він підключається до проксі-сервера. Проксі-сервер підключається до віддаленого сервера від імені клієнта. Тому сервер бачить лише з'єднання з проксі-сервером.

Інші способи впровадження міжмережевих екранів включають:

– брандмауер на базі хоста (серверний та персональний) – комп'ютер або сервер із програмним забезпеченням брандмауера;

– прозорий брандмауер – Фільтрує IP трафік між парою мостових інтерфейсів;

– гібридний брандмауер – комбінація різних типів брандмауера. Наприклад, брандмауер огляду додатків поєднує в собі міжмережевий екран стану з брандмауером програмного шлюзу.

Брандмауери для фільтрування пакетів, як правило, є частиною брандмауера маршрутизатора, що дозволяє або забороняє трафік на основі даних 3 і 4 рівня. Вони – між мережеві екрани без врахування стану, які використовують простий аналіз таблиць політики, що фільтрує трафік за певними критеріями. Наприклад, сервери SMTP за замовчуванням слухають порт 25. Адміністратор може налаштувати брандмауер фільтрування пакетів, щоб заблокувати порт 25 з певної робочої станції, для запобігання передачі вірусу електронною поштою.

Брандмауерами з врахуванням стану є найбільш універсальними та найпоширенішими технологіями брандмауера, що використовуються. Брандмауерами з врахуванням стану забезпечують фільтрування пакетів через стан, використовуючи інформацію про з'єднання, що зберігається в таблиці стану. Фільтрація з врахуванням стану – це архітектура брандмауера, яка класифікується на мережевому рівні. Також аналізується трафік на рівні OSI Layer 4 та Layer 5.

Брандмауери наступного покоління виходять за межі міжмережевих екранів з врахуванням стану, забезпечуючи:

– стандартні можливості брандмауера, такі як перевірка стану;

– комплексний захист від вторгнень;

– ознайомлення з програмою та керування ними, щоб переглядати та блокувати ризикові додатки;

– оновлення шляхів до майбутніх інформаційних каналів;

– методи вирішення проблем майбутніх загроз безпеки.

Зміна парадигми мережевої архітектури вимагає захисту від швидких та еволюційних атак. Це повинно включати в себе економічно ефективні системи виявлення та попередження, такі як системи виявлення вторгнень

(IDS) або більш масштабовані системи запобігання вторгненню (IPS). Архітектура мережі інтегрує ці рішення в точки входу та виходу мережі.

При впровадженні IDS або IPS важливо знати типи доступних систем, підходи на основі хоста та мережі, розміщення цих систем, роль категорій підписів та можливі дії, які може приймати маршрутизатор, коли виявлено атаку.

Технології IDS та IPS мають кілька характеристик, як показано на малюнку. IDS та IPS технології використовуються як датчики. Датчик IDS або IPS може бути у формі декількох різних пристроїв:

– маршрутизатор, налаштований з програмним забезпеченням IPS;

– пристрій, спеціально розроблений для надання виділених служб IDS або IPS;

– мережевий модуль встановлений в адаптивному пристрої безпеки (ASA), комутаторі або маршрутизаторі.

Технології IDS та IPS використовують підписи для виявлення шаблонів у мережевому трафіку. Підпис – це набір правил, які IDS або IPS використовують для виявлення шкідливих дій. Підписи можуть використовуватися для виявлення серйозних порушень безпеки, виявлення загальних мережевих атак та збирання інформації. Технології IDS та IPS можуть виявляти шаблони одинарного підпису (single-packet) або композитні шаблони підписів (multi-packet).

Проведемо аналіз переваг та недоліків IDS та IPS.

Перевагами IDS є:

– ніякого впливу на мережу у вигляді затримки;

– немає впливу на мережу у випадку виходу з ладу датчика;

– немає впливу на мережу у випадку перевантаження сенсорів.

Недоліками IDS є:

– дія у відповідь на подію неможе зупинити потік пакетів;

– правильне налаштування потрібне для реагування на події;

– більш вразливий до методів порушення мережевої безпеки.

Переваги IPS:

– зупиняє потік пакетів у випадку порушення правил;

– може використовувати методи нормалізації потоку даних.

Недоліки IPS:

– проблеми сенсора можуть вплинути на мережевий потік;

– перевантаження сенсора впливає на мережу;

– може створювати певні затримки в мережі.

Основна перевага платформи IDS полягає в тому, що вона розгортається в автономному режимі. Оскільки сенсор IDS не вбудований, він не впливає на продуктивність мережі. Він не створює затримку, джитер та інші проблеми трафіку. Крім того, якщо датчик не працює, це не впливає на функціональність мережі. Це впливає лише на здатність IDS аналізувати дані.

Однак існує багато недоліків розгортання платформи IDS. Датчик IDS в першу чергу зосереджується на виявленні можливих інцидентів, реєстрації інформації про інциденти та повідомленні про інциденти. Датчик IDS не може зупинити тригерний пакет і немає гарантії, що припинить з'єднання. Пакет тригера сповіщає IDS про потенційну загрозу. Датчики IDS також менш корисні для припинення вірусів електронної пошти та автоматичних атак, таких як хробаки.

Користувачі, що розгортають дії реагування на датчики IDS, повинні мати добре продуману політику безпеки та добре розуміти оперативне використання їх IDS розгортання . Користувачі повинні витрачати час на налаштування IDS датчиків для досягнення очікуваних рівнів виявлення вторгнення.

Нарешті, оскільки IDS-датчики не вбудовані, реалізація IDS є більш вразливою до методів ухилення від мережевої безпеки у вигляді різних методів мережевої атаки.

Датчик IPS може бути налаштований для виконання знищення пакетів, щоб зупинити пакет тригер, пакети, пов'язані з підключенням, або пакети з вихідної IP-адреси. Крім того, оскільки сенсори IPS є вбудованими, вони можуть використовувати нормалізацію потоку. Нормалізація потоку - це техніка, яка використовується для відтворення потоку даних, коли атака відбувається в кількох сегментах даних.

Недоліком IPS є те, що (оскільки він вбудований) помилки, збій і перевантаження IPS трафіком можуть спричинити негативний вплив на продуктивність мережі. Датчик IPS може впливати на роботу мережі, вводячи затримку та джиттер. Датчик IPS має бути належним чином розрахований та реалізований таким чином, щоб це не вплинуло на чутливі до часу додатки, такі як VoIP.

Використання однієї з цих технологій не заперечує використання іншого. Справді, технології IDS та IPS можуть доповнювати один одного. Наприклад, IDS може бути реалізований для перевірки роботи IPS, оскільки IDS може бути налаштований для більш глибокого огляду пакетів в автономному режимі. Це дозволяє IPS зосередити увагу на меншій кількості, але більш критичних шаблонах трафіку.

Визначення того, яку реалізацію використовувати, базується на цілях безпеки організації, як зазначено в їх політиці безпеки мережі.

Є два основних типи доступних IPS: на базі хоста та на основі мережі.

Host-based IPS (HIPS) – це програмне забезпечення, встановлене на одному хості для моніторингу та аналізу підозрілих дій. Суттєвою перевагою HIPS є те, що вона може відслідковувати та захищати операційну систему та критичні системні процеси, специфічні для цього хоста. З детальним ознайомленням з операційною системою, HIPS може відстежувати аномальну активність та не дозволяти хосту виконувати команди, які не відповідають типовій поведінці. Ця підозріла або шкідлива поведінка може включати неавторизоване оновлення реєстру, зміни в системному каталозі,

виконання програм інсталяції та дії, що викликають переповнення буфера. Мережевий трафік також можна контролювати, щоб не дозволити хосту брати участь в атаці відмови (служби) (DoS) або бути частиною незаконного сеансу FTP.

HIPS можна розглядати як комбінацію антивірусного програмного забезпечення, програмного забезпечення проти шкідливого програмного забезпечення та брандмауера. Поєднуючи мережевий IPS, HIPS є ефективним інструментом для забезпечення додаткового захисту хоста.

Недоліком HIPS є те, що вона працює лише на місцевому рівні. Вона не має повного перегляду мережі або узгоджених подій, які можуть відбуватися по всій мережі. Щоб бути ефективним у мережі, HIPS необхідно встановити на кожному хості та мати підтримку для кожної операційної системи.

Мережевий IPS може бути реалізований за допомогою спеціального або не спеціального пристрою IPS. Мережеві IPS-реалізації є важливим компонентом запобігання вторгнення. Існують рішення для IDS / IPS на базі хоста, однак вони повинні бути інтегровані в мережеву IPS-версію для забезпечення надійної архітектури безпеки.

Датчики виявляють шкідливу та несанкціоновану діяльність в режимі реального часу і можуть вживати заходів, коли це потрібно. Датчики розгортаються в визначених мережевих точках, які дозволяють менеджерам безпеки стежити за активністю мережі під час її виконання, незалежно від місця розташування цілі нападу.

Advanced Malware Protection (AMP) – це розширений аналіз і захист від шкідливих програм корпоративного рівня. Він забезпечує комплексний захист від шкідливих програм для організацій перед, під час та після нападу:

– перед нападом, AMP зміцнює захист і захищає від відомих та виникаючих загроз;

– під час атаки AMP ідентифікує та блокує типи файлів, які порушують політику, експлуатують спроби, а також шкідливі файли, що проникають через мережу;

– після атаки або після того, як файли спочатку перевірені, AMP виходить за рамки можливостей точкового виявлення в часі і постійно відслідковує та аналізує всі файлові операції та трафік незалежно від розташування, шукаючи будь-які ознаки шкідливої поведінки. Якщо файл з невідомим або той, що раніше вважався “хорошим” розподілом починає вести себе погано, AMP виявляє його та негайно сповіщає команди безпеки з вказівкою на загрозу. Потім він забезпечує видимість того, звідки виникло зловмисне програмне забезпечення, які системи постраждали, і те, що робить шкідливе програмне забезпечення.

AMP отримує доступ до колективної розвідки безпеки та дослідницької групи . Вона виявляє та корелює загрози в режимі реального часу, використовуючи найбільшу мережу виявлення загроз у світі.

Web Security Appliance (WSA) – це захищений веб-шлюз, який поєднує в собі провідні засоби захисту, які допомагають організаціям реагувати на зростаючі виклики щодо забезпечення та контролю веб-трафіку. WSA захищає мережу, автоматично блокуючи ризиковані сайти та тестуючи невідомі сайти, перш ніж дозволити користувачам отримати доступ до них. WSA забезпечує захист від шкідливого програмного забезпечення, видимість програм та контроль, прийнятні правила використання політики, проникливі звіти та безпечну мобільність.

Хоча WSA захищає мережу від вторгнення шкідливих програм, вона не забезпечує захист для користувачів, які хочуть підключитися до Інтернету безпосередньо за межами захищеної мережі, наприклад, у службі загального доступу Wi-Fi. У цьому випадку комп’ютер користувача може бути заражений шкідливим програмним забезпеченням, яке потім може поширюватися на інші мережі та пристрої. Щоб захистити персональні

комп’ютери від таких видів інфікування шкідливих програм, існує Cloud Web Security (CWS).

CWS разом з WSA забезпечує комплексний захист від шкідливих програм і пов’язаних з ними наслідків. Рішення CWS забезпечує надійне з’єднання з Інтернетом та з Інтернету і надає віддаленим працівникам такий же рівень безпеки, як і працівникам на місці, коли використовується ноутбук, виданий роботодавцем. CWS включає дві основні функції, веб-фільтри та веб-безпеку, і обидва вони супроводжуються великою централізованою звітністю.

Email Security Appliance (ESA) / Cloud Email Security допомагають пом’якшити загрози на основі електронної пошти. ESA захищає критично важливі поштові системи. Cisco ESA постійно оновлюється каналами в реальному часі від Talos, які виявляють та корелюють загрози за допомогою глобальної системи моніторингу баз даних. Ось деякі з основних особливостей ESA:

– глобальна розвідка про загрозу – Talos забезпечує цілодобове спостереження глобальної активності трафіку. Він аналізує аномалії, розкриває нові загрози та відстежує тенденції трафіку.

– блокування спаму – багатошаровий захист об’єднує зовнішній шар фільтрації на основі репутації відправника та внутрішній шар фільтрації, який виконує глибокий аналіз повідомлення.

– додатковий захист від зловмисного програмного забезпечення – включає в себе AMP, що використовує розгалужену мережу хмарних служб безпеки Sourcefire. Він забезпечує захист через континуум атаки до, під час та після нападу.

– керування вихідними повідомленнями – керує вихідними повідомленнями, щоб гарантувати, що важливі повідомлення відповідають галузевим стандартам та захищені під час транзиту.

Розробка та впровадження комплексу апаратно-технічних заходів убезпечення мережевих архітектур є важливою складовою частиною організації надійної, продуктивної та захищеної інформаційної мережі.

Висновки до першого розділу

В першому розділі дипломної роботи виконано дослідження вагомих аспектів проектування комп'ютерних інформаційних мереж на прикладі великої організації. При цьому, сформовано основні вимоги до проектування методів та засобів побудови і впровадження надійних, продуктивних та захищених мережевих архітектур. Здійснено огляд трирівневої моделі дизайну та її спрощеної дворівневої версії для компаній з різними вимогами до роботи мереж. На основі проведеного аналізу виявлено та прокласифіковано види та типи мережевих загроз безпеці інформаційних ресурсів. Розглянуто методи протидії інформаційній безпеці, що базуються на системах виявлення та реагування загрозам ресурсів мережі.

РОЗРОБКА ТА ВПРОВАДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ НАДІЙНИХ, ПРОДУКТИВНИХ ТА ЗАХИЩЕНИХ МЕРЕЖ

Підвищення надійності роботи мережі на основі протоколів аналізу та управління трафіком

Простий протокол керування мережею (SNMP) дозволяє адміністраторам управляти кінцевими пристроями, такими як сервери, робочі станції, маршрутизатори, комутатори та пристрої безпеки, в IP-мережі. Це дозволяє мережевим адміністраторам контролювати та управляти продуктивністю мережі, знаходити та вирішувати мережеві проблеми та планувати зростання мережі.

SNMP – це протокол прикладного рівня, який забезпечує формат повідомлення для спілкування між менеджерами та агентами. Система SNMP складається з трьох елементів:

– SNMP-менеджер, який керує програмним забезпеченням SNMP;

– SNMP агенти, які є вузлами, що контролюються та управляються;

– інформаційна база керування (MIB), яка є базою даних агента, що зберігає дані та операційну статистику про пристрій.

NetFlow – це технологія Cisco IOS, яка забезпечує статистику пакетів, що проходять через маршрутизатор Cisco або багаторівневий комутатор. В той час коли SNMP намагається надати дуже широкий спектр функцій та параметрів керування мережею, NetFlow зосереджується на наданні статистики про IP-пакети, що проходять через мережеві пристрої.

NetFlow надає дані для здійснення моніторингу мережі та безпеки, планування мережі, аналізу трафіку, що включає ідентифікацію вузьких місць мережі та облік IP для цілей біллінгу. Наприклад, PC 1 підключається до PC 2 за допомогою програми, такої як HTTPS. NetFlow може відстежувати зв’язок додатків, трекінг байтів та кількість підрахунків пакетів для цього

окремого програмного потоку . Потім він передає статистику на зовнішній сервер, який називається колектором NetFlow.

Технологія NetFlow мала декілька поколінь, що забезпечують більшу вишуканість у визначенні потоків трафіку, але “оригінальні NetFlow” виділяють потоки, використовуючи комбінацію із семи полів. Якщо одне з цих полів відрізняється значенням від іншого пакета, можна сміливо визначити, що пакети належать різним потокам:

– IP-адреса джерела;
– IP-адреса призначення;
– номер вихідного порту;
– номер порту призначення;
– тип протоколу Layer 3;
– Type of Service (ToS) позначка;
– вхідний логічний інтерфейс.

Перші чотири поля NetFlow, що використовуються для ідентифікації потоку, повинні бути знайомі. IP-адреси джерела та призначення, а також порти джерела та призначення, визначають зв’язок між вихідним та призначеним додатками. Тип протоколу Layer 3 визначає тип заголовка, який слідує за заголовком IP (зазвичай TCP або UDP, але інші параметри включають ICMP). Байт ToS у заголовку IPv4 містить інформацію про те, як пристрої повинні застосовувати правила якості обслуговування (QoS) до пакетів у цьому потоці.

Колектори NetFlow, такі як Cisco Stealthwatch, також можуть виконувати розширені функції, зокрема:

– зшивання потоків: групування окремих записів у потоки;

– дедуплікація потоку: фільтрує дублікати вхідних записів з кількох клієнтів NetFlow;

– зшивання NAT: спрощує потоки за допомогою записів NAT.

Cisco StealthWatch має безліч інших функцій, ніж просто NetFlow. Натисніть тут для перегляду короткого відео про Cisco StealthWatch.

Аналізатор пакетів (також відомий як сніффер пакетів або трафік-сніффер), як правило, являє собою програмне забезпечення, яке ловить пакети, що входять і виходять з мережевої інтерфейсної карти (NIC). Не завжди можливо або бажано мати аналізатор пакетів на пристрої, який підлягає моніторингу. Іноді краще на окремій станції, призначеній для захоплення пакетів.

Оскільки мережеві комутатори можуть ізолювати трафік, трафік сніфери або інші мережеві монітори, такі як IDS, не можуть отримати доступ до всього трафіку в сегменті мережі. Дзеркалювання порту - це функція, яка дозволяє комутатору робити дублікати копій трафіку, що проходить через комутатор, а потім відправити його через порт де приєднано мережевий монітор. Оригінальний трафік пересилається звичайним способом. Приклад дзеркалювання порту показано на малюнку.

Коли певні події відбуваються в мережі, мережеві пристрої мають довірчі механізми, щоб сповістити адміністратора про детальні системні повідомлення. Ці повідомлення можуть бути некритичними або значними. Мережеві адміністратори мають різні варіанти зберігання, інтерпретації та відображення цих повідомлень, а також повідомляються про ті повідомлення, які можуть найбільше впливати на мережеву інфраструктуру.

Найпоширенішим способом доступу до системних повідомлень є використання протоколу syslog.

Багато мережевих пристроїв підтримують syslog, включаючи маршрутизатори, комутатори, сервери додатків, міжмережеві екрани та інші мережеві пристрої. Протокол syslog дозволяє мережевим пристроям надсилати системні повідомлення по всій мережі на сервери syslog, як показано на малюнку.

Служба реєстрації syslog забезпечує три основні функції:

– можливість збирати реєстраційну інформацію для моніторингу та усунення несправностей;

– можливість вибирати тип зафіксованої інформації, що є зібрана;

– можливість вказати призначення зібраних syslog повідомлень.

Syslog стандартно використовується для протоколювання повідомлень з мережних та кінцевих пристроїв. Цей стандарт дозволяє використовувати системно нейтральні засоби для передавання, зберігання та аналізу повідомлень. Багато типів пристроїв різних виробників можуть використовувати syslog для надсилання повідомлень системного журналу до центральних серверів на яких запускається демон syslog. Така централізація збору log-журналів допомагає зробити моніторинг безпеки практичним. Сервери, на яких запущено syslog, зазвичай прослуховують 514 UDP порт.

Оскільки системний журнал є дуже важливим для моніторингу безпеки, syslog сервери можуть стати ціллю для зловмисників. Деякі експлойти, наприклад ті, що стосубться екфільтрації даних, можуть тривати довгий термін часу до свого завершення, оскільки спроби викласти таємно дані з мережі відбуваються повільно. Зловмисники можуть спробувати приховати той факт, що відбувається ексфільтрація. Вони атакують syslog сервери, на яких може міститись інформація яка може призвести до виявлення цих експлойтів. Хакери можуть спробувати заблокевати передавання даних від syslog-клієнтів до серверів, втрутитись або знищити дані log-журналу, втрутитись у програмне забезпечення, яке створює та передає log-повідомлення. Нова генерація syslog, реалізація якої відома під назвою syslog-ng, пропонує удосконалення, які можуть допомогти запобігти втручанню деяких експлойтів, які націлені на syslog.

Syslog повідомлення, як правило, позначаються часовими мітками. Це дозволяє одержувати повідомлення від різних джерел з часовими мітками для перегляду комунікаційних процесів. Оскільки повідомлення можуть надходити від багатьох пристроїв, важливо щоб пристрої працювали в

єдиному часовому полі. Один з способів досягнення цього полягає в тому, що пристрої можуть використовувати протокол встановлення мережного часу (Network Time Protocol - NTP). NTP використовує ієрархію авторитетних джерел часу для обміну інформацією про час між пристроями в мережі, як показано на рисунку. Таким чином, повідомлення пристрою, який має інформацію про мережний час, можуть бути передані до syslog-сервера. NTP використовує 123 порт протоколу UDP.

Оскільки події, що пов’язані з експлойтом, можуть залишати сліди на кожному з мережних пристроїв на своєму шляху до системи-жертва, часові мітки є важливими для їх виявлення. Зловмисники можуть намагатися атакувати інфраструктуру NTP, щоб пошкодити інформацію про часові мітки, яка використовується для співставлення задокументованих мережних подій. Це може використовуватись для того, щоб заплутати сліди втручання експлойту. Крім того, часто зловмисники використовують системи NTP для спрямування DDoS атак через уразливості в клієнтському або серверному програмному забезпеченні. Хоча ці напади не обов'язково призводять до пошкоджених даних моніторингу безпеки, вони можуть порушити доступність мережі.

Важливо синхронізувати час на всіх пристроях у мережі, тому що всі аспекти управління, забезпечення, усунення несправностей та планування мереж потребують точного та послідовного відстеження часу. Коли час не буде синхронізовано між пристроями, неможливо визначити порядок подій, що відбулися в різних частинах мережі.

Як правило, налаштування дати та часу в мережевому пристрої можна встановити одним із двох способів:

- ручна настройка дати та часу;
- конфігуруючи Network Time Protocol (NTP).

Коли мережа зростає, стає важко гарантувати, що всі інфраструктурні пристрої працюють з синхронізованим часом. Навіть у менших мережевих

середовищах ручний метод не є ідеальним. Якщо пристрій перезавантажиться, як він отримає точну дату та часовий покажчик?

Кращим рішенням є налаштування NTP у мережі. Цей протокол дозволяє маршрутизаторам мережі синхронізувати свої налаштування часу з NTP-сервером. Група клієнтів NTP, які отримують інформацію про час і дату з одного джерела, мають більш послідовні налаштування часу. Коли NTP реалізовано в мережі, її можна налаштувати для синхронізації з приватним головним годинником або може синхронізуватися з загальнодоступним NTP-сервером в Інтернеті.

NTP-мережі використовують ієрархічну систему джерел часу. Кожен рівень у цій ієрархічній системі називається stratum. Рівень stratum визначається як лічильник кількості вузлів від авторитетного джерела. Синхронізований час розподіляється по мережі за допомогою NTP. На малюнку відображається зразок NTP-мережі.

NTP-сервери розташовані на трьох рівнях:

– Stratum 0 – мережа NTP отримує час від авторитетних джерел часу. Ці авторитетні джерела часу, також називаються пристроями stratum 0, являють собою високоточні прилади хронометражу, які вважаються точними, і з незначною затримкою або взагалі не пов’язані з ними.

– Stratum 1 – пристрої stratum 1 безпосередньо пов'язані з авторитетними джерелами часу. Вони діють як основний стандартний час мережі.

– Stratum 2 та нижче – сервери stratum 2 підключаються до пристроїв stratum 1 через мережеві з’єднання. Пристрої Stratum 2, такі як клієнти NTP, синхронізують свій час, використовуючи пакети NTP з серверів stratum 1. Вони також можуть служити серверами для пристроїв stratum 3.

Числа меншого stratum вказують на те, що сервер знаходиться ближче до авторизованого джерела часу, ніж більші числа stratum. Чим більше число stratum, тим нижче рівень stratum. Максимальна кількість переходів - 15.

Stratum 16, найнижчий stratum рівень, означає, що пристрій не синхронізовано. Сервери часу на тому ж рівні stratum можуть бути налаштовані на взаємодію з іншими серверами часу на тому ж рівні stratum для резервного копіювання або перевірки часу.

ICMP має багато легітимних застосувань, однак функціональність ICMP була використана для розробки багатьох видів експлойтів. ICMP може бути використано для ідентифікації вузлів у мережі, структури мережі та визначення операційних систем, які використовуються у мережі. Цей протокол також може використовуватися як засіб для різного типу DoS-атак.

ICMP також може бути використаний для ексфільтрації даних. Через занепокоєння тим, що ICMP може використовуватися для дослідження або відхилення сервісу з зовнішньої мережі, ICMP трафік всередині мережі іноді ігнорується. Тим не менше, деякі види зловмисного програмного забезпечення використовують створені пакети ICMP для передачі файлів з заражених зловмисниками вузлів, використовуючи метод, який відомий як ICMP - тунелювання.

Організаційно-технічні методи за засоби забезпечення працездатності мережі

AAA – це архітектурна база для налаштування набору трьох незалежних функцій безпеки:

– автентифікація – користувачі та адміністратори повинні довести, що вони є такими, якими вони називаються. Аутентифікацію можна встановити за допомогою комбінацій імені користувача та пароля, запитів на виклики та відповіді, картки токенів та інші методи. Наприклад: "Я є користувачем student", і я знаю пароль, щоб довести це ". Аутентифікація AAA забезпечує централізований спосіб контролю доступу до мережі.

– авторизація – після того, як користувач автентифікується, служби авторизації визначають, які ресурси користувач може отримати та які дії користувачам дозволяється виконувати. Приклад “користувач student” може отримати доступ до хост-сервера XYZ лише за допомогою SSH.

– облік та аудит – облік записів того, що робить користувач, у тому числі до чого був доступ, кількість часу доступу до ресурсу та будь-які внесені зміни. Облік стежить за тим, як використовуються мережеві ресурси. Прикладом може служити “користувач student” отримав доступ до хост-сервер XYZ, використовуючи SSH протягом 15 хвилин.

Terminal Access Controller Access-Control System Plus (TACACS +) та Remote Authentication Dial-In User Service (RADIUS) – це протоколи автентифікації, які використовуються для зв’язку з серверами AAA. Вибір TACACS + або RADIUS залежить від потреб організації.

Хоча обидва протоколи можуть бути використані для зв’язку між маршрутизатором та серверами AAA, TACACS + вважається більш безпечним протоколом. Це є тому, що всі обміни протоколу TACACS + зашифровані, а RADIUS лише шифрує пароль користувача. RADIUS не шифрує імена користувачів, облікові дані або будь-яку іншу інформацію, що міститься в повідомленні RADIUS. Проведемо аналіз відмінностей між цими двома протоколами:

– протокол TACACS + відокремлює AAA відповідно до архітектури AAA, що дає змогу модульності реалізації сервера безпеки;

– використовує протокол двостороннього виклику та відповіді Challenge Handshake Authentication Protocol (CHAP);

– шифрує весь пакет;

– забезпечує авторизацію команд маршрутизатора на основі користувача або групи;

– протокол RADIUS поєднує автинтифікацію та авторизацію, але відокремлює облік, що надає меншу гнучкість реалізації ніж TACACS +;

– використовує одно направлений виклик від сервера до клієнта RADIUS;

– шифрує тільки паролі

– немає можливості авторизувати команди на основі користувача або групи.

Для захисту мережевих пристроїв важливо використовувати надійні паролі. Ось стандартні вказівки, яких слід дотримуватися:

– використовуйте пароль довжиною не менше восьми символів, бажано 10 або більше символів. Більш довгий пароль – це більш безпечний пароль;

– складіть паролі складними. Додайте суміш з великих і малих літер, цифр, символів та пробілів, якщо це дозволено;

– уникайте паролів на основі повторення, загальних словникових слів, послідовностей букв чи цифр, імен користувачів, родичів або імен домашніх тварин, біографічної інформації, таких як дати народження, ідентифікаційні номери, імена предків або інші відомості, які легко ідентифікуються;

– навмисно неправильно введіть пароль. Наприклад, Smith = Smyth = 5mYth або Security = 5ecur1ty;

– часто міняйте паролі. Якщо пароль невідомо порушений, вірогідність можливості учасника загрози використовувати пароль обмежена;

– не записуйте паролі і не залишайте їх у очевидних місцях, таких як на столі чи моніторі.

Сильні паролі корисні лише в тому випадку, якщо вони секретні. Можна зробити кілька кроків, щоб гарантувати, що паролі залишаються таємними на маршрутизаторі та комутаторі, включаючи ці:

– шифрування всіх паролів простого тексту;

– встановлення мінімально прийнятної довжини пароля;

– визначення атак відгадування пароля;

– вимкнення неактивного привілейованого доступу до режиму EXEC через визначений час.

Щоб упевнитись, що всі налаштовані паролі мають мінімальну задану довжину, використовуйте команду паролів захисту мінімальної довжини в режимі глобальної настройки. Будь-який новий налаштований пароль повинен мати мінімальну довжину не менше восьми символів.

Особи, що загрожують, можуть використовувати програмне забезпечення для взлому пароля, щоб здійснити атаку “грубої сили” на мережевий пристрій. Ця атака постійно намагається відгадати дійсні паролі, поки не спрацює. Встановлюйте обмеження на кількість спроб, які можна ввести на протязі часу.

Мережеві адміністратори можуть відволіктись і випадково залишити привілейований сеанс режиму EXEC відкритим на терміналі. Це може дозволити зловмиснику отримати доступ або змінити конфігурацію пристрою.

За замовчуванням маршрутизатори Cisco вийдуть з сеансу EXEC через 10 хвилин бездіяльності. Однак ви можете зменшити цей параметр, скориставшись командою конфігурації.

Управління ризиками мережевої безпеки

Управління ризиками включає в себе вибір і специфікацію управління безпекою для організації. Вона є частиною постійної загальноорганізаційної програми з інформаційної безпеки, яка передбачає управління ризиками для організації або окремих осіб, пов'язаних із функціонуванням системи.

Управління ризиками - це постійний, багатоступеневий, циклічний процес, як це показано на рисунку.

Ризик визначається як співвідношення між загрозою, вразливістю і специфікою організації. В першу чергу це стосується відповіді на наступні питання в рамках оцінки ризику:

– хто такі ці зловмисники, які хочуть нас атакувати?
– які вразливості можуть використовувати організатори загрози?
– як би ми постраждали від атак?
– яка ймовірність того, що різні атаки будуть відбуватися?

Спеціальна публікація NIST 800-30 описує оцінку ризиків як:

“... процес виявлення, оцінки та визначення пріоритетності ризиків інформаційної безпеки. Оцінюючи ризик, потрібно уважно аналізувати інформацію про загрозу та вразливість, щоб визначити, наскільки обставини або події можуть негативно вплинути на організацію та ймовірність того, що такі обставини або події відбудуться.”

Обов’язковою діяльністю з оцінки ризику є виявлення загроз та вразливостей та узгодження загроз з вразливостями у тому, що часто називається парою вразливість-загроза (threat-vulnerabilit - T-V). Пари T-V можуть потім використовуватися в якості бази для позначення ризику, перед здійсненням контролю безпеки. Це базовий рівень і його можна порівняти з поточними оцінками ризику, як засіб оцінки ефективності управління ризиками. Цю частину оцінки ризику визначають, як невід'ємний профіль ризику організації.

Після виявлення ризиків їх можна зазначити або оцінити як спосіб визначення стратегії зменшення ризику. Наприклад, вразливості, які, як було встановлено, відповідають кільком загрозам, можуть отримувати більш високі рейтинги. Крім того, T-V пари, які відображають найбільший інституційний вплив, отримають також більш високі вагові коефіцієнти.

Існує чотири потенційні способи реагування на ризики, які були визначені, виходячи з їх вагових коефіцієнтів або балів:

– уникнення ризику – припинення виконання заходів, які створюють ризик. Цілком можливо, що в результаті оцінки ризику, визначається, що ризик, пов’язаний з діяльністю, переважить вигоди від діяльності для організації. Якщо це виявиться правдою, тоді може бути визнано, що діяльність повинна бути припинена.

– зменшення ризику – зниження ризику шляхом вжиття заходів щодо зменшення вразливості. Це передбачає впровадження управлінських підходів, обговорюваних раніше в цьому розділі. Наприклад, якщо організація використовує серверні операційні системи, які часто стають об'єктом атак, ризик може бути зменшений шляхом забезпечення того, щоб сервера оновлювали виправлення (patched) як тільки вразливості були нейтралізовані.

– розподіл ризиків – перекласти частину ризику на інших осіб. Наприклад, механізмом розподілу ризиків може бути передача деяких аспектів операцій з безпекою стороннім особам. Прикладом є наймання безпеки як сервісу (SECaaS) CSIRT для здійснення моніторингу безпеки. Інший приклад, це придбати страхування, яке допоможе пом’якшити деякі фінансові втрати через інцидент з безпекою.

збереження ризику – прийняти ризик і його наслідки. Ця стратегія прийнятна для ризиків, які мають низький потенційний вплив і відносно високу вартість для пом’якшення наслідків або усунення. Іншими ризиками, які можуть бути збережені, це такі, які є настільки кардинальними, що їх реально не можна уникнути, зменшити або поділитись ними.

Відповідно до NIST, управління вразливостями – це практика безпеки, спрямована на запобігання експлуатації IT-вразливостей, які існують в організації. Очікуваний результат полягає у зменшенні часу та коштів, що витрачаються на усунення вразливостей та експлуатацію цих вразливостей. Випереджаюче управління вразливостями систем дозволить знизити або

усунути потенціал для їх експлуатації, а також дозволить затратити значно менше часу і зусиль, ніж реагування після того, як подія відбулася.

Управління вразливостями вимагає надійних засобів виявлення вразливостей на основі бюлетенів з безпеки вендорів та інших інформаційних систем, таких як CVE. Співробітники служби безпеки повинні бути компетентні в оцінці впливу, якщо такий є, інформації про вразливість яку вони отримали. Рішення повинні бути визначені ефективними засобами реалізації і оцінки непередбачених наслідків реалізованих рішень. І нарешті, рішення повинно бути випробувано, щоб переконатися в тому, що вразливість була усунута.

Нижче описано кроки в життєвому циклі керування вразливостями:

– виявлення – інвентаризація всіх активів у мережі та іднтифікація деталей хоста, включаючи операційні системи та відкриті сервіси, для виявлення вразливостей. Розробити базову лінію поведінки мережі. Виявлення вразливостей в системі безпеки за допомогою регулярного автоматизованого графіку;

– пріоритезуйте активи – класифікація активів у групи або бізнес-одиниці та присвоєння бізнес-цінності групам активів на підставі їх критичності для бізнес-операцій;

– оцінка – визначити базовий профіль ризику для усунення ризиків на основі критичності активів, уразливості, загрози і класифікації активів;

– звіт – виміряйте рівень бізнес-ризиків, пов’язаних із вашими активами відповідно до ваших політик безпеки. Складіть план безпеки, відстежуйте підозрілу активність та опишіть відомі вразливості;

– відновлення – визначте пріоритетність відповідно до бізнес-ризиків і усунення вразливостей в порядку ризику загроз;

– перевірка – переконайтеся в тому, що загрози були усунені за допомогою наступних перевірок.

Управління активами передбачає впровадження систем, які відстежують розташування та конфігурацію мережних пристроїв та програмного забезпечення на підприємстві. У рамках будь-якого плану управління безпекою в організації, повинно бути відомо, яке обладнання має доступ до мережі, де це обладнання знаходиться в межах підприємства та логічно в мережі, а також програмне забезпечення та дані, які ці системи зберігають або можуть отримати доступ. Управління активами не тільки відслідковує корпоративні активи та інші авторизовані пристрої, але також може використовуватися для ідентифікації пристроїв, які не авторизовані в мережі.

NIST визначає в публікації NISTIR 8011 та2 (Volume 2), детальні записи, які слід зберігати для кожного відповідного пристрою. NIST описує можливі методи і інструменти для введення в дію процесу управління активами:

– автоматичне виявлення і інвентаризація фактичного стану пристроїв;

– зазначення бажаного стану для цих пристроїв за допомогою політик, планів і процедур в плані інформаційної безпеки організації;

– виявлення невідповідних вимогам авторизованих активів;

– відновлення або прийняття стану пристрою, можливе повторення визначення бажаного стану;

– повторіть цей процес через регулярні проміжки часу або постійно.

Управління мобільними пристроями (Mobile device management, MDM), особливо у еру BYOD, є особливою проблемою з управління активами. Мобільні пристрої не можуть фізично контролюватися на території організації. Вони можуть бути загублені, вкрадені або підроблені, ставлячи під загрозу дані та доступ до мережі. Частина плану MDM вживання заходів, коли пристрої залишаються під опікою відповідальної сторони. Заходи, які

можуть бути здійснені, включають: відключення втраченого пристрою, шифрування даних на пристрої та вдосконалення доступу до пристроїв за допомогою більш надійних заходів автентифікації.

У зв'язку з різноманітністю мобільних пристроїв, можлива ситуація, що деякі пристрої, які будуть використовуватися в мережі за своїми характеристиками є менш безпечні, ніж інші. Мережні адміністратори повинні припускати, що всі мобільні пристрої є ненадійними, доки вони не будуть належним чином захищені організацією.

Системи MDM, такі як Системний менеджер Cisco Meraki (Cisco Meraki Systems Manager), що показаний на рисунку, дозволяють персоналу з безпеки конфігурувати, контролювати та оновлювати дуже різноманітний набір мобільних клієнтів із хмари (cloud).

Управління конфігурацією стосується обліку та контролю апаратних та програмних конфігурацій систем. Захищені конфігурації пристроїв зменшують ризик для безпеки. Наприклад, організація надає своїм працівникам багато комп’ютерів та ноутбуків. Це збільшує поверхню атаки для організації, оскільки кожна з систем може бути вразлива для експлойтів. Щоб впоратися з цим, організація може створювати базові образи програмного забезпечення та апаратних конфігурацій для кожного типу пристроїв. Ці образи можуть включати в себе базовий пакет необхідного програмного забезпечення, програмне забезпечення для безпеки кінцевих точок, а також налаштовувати політики безпеки, які керують доступом користувачів до певних аспектів конфігурації системи, які можуть стати вразливими. У конфігурації обладнання можуть бути визначені дозволені типи мережних інтерфейсів і дозволені тип зовнішніх сховищ.

Конфігурація обладнання може містити допустимі типи мережних інтерфейсів та дозволені типи зовнішнього сховища. Відповідно до визначення NIST, управління конфігурацією:

“Містить набір заходів, спрямованих на встановлення та підтримку цілісності продуктів і систем шляхом контролю процесів ініціалізації, зміни та контролю за конфігураціями цих продуктів і систем.”

Для пристроїв міжмережної взаємодії, доступні програмні засоби, які будуть резервувати конфігурації, виявляти зміни в файлах конфігурації та дозволяти зміни конфігурацій на кількох пристроях одночасно.

З появою хмарних центрів обробки даних (cloud data centers) і віртуалізації, управління великою кількістю серверів створює особливі проблеми. Інструменти управління конфігурацією, такі як Puppet, Chef, Ansible та SaltStack, були розроблені, щоб забезпечити ефективне управління серверами, що базуються на хмарних комп’ютерних технологіях.

Керування виправленнями (patch) пов’язане з управлінням вразливостями. Вразливості часто з’являються на критичних клієнта, серверах і операційних системах мережних пристроїв і мікрограмах (firmware). Прикладне програмне забезпечення, особливо інтернет-застосунки та фреймворки, такі як Acrobat, Flash і Java, також часто виявляються вразливими. Керування виправленнями (патчами) включає в себе всі аспекти патча програмного забезпечення, включно з виявленням необхідних патчів, отримання, розповсюдження, встановлення та перевірку того, що патч встановлено на всі необхідні системи. Встановлення патчів часто є найбільш ефективним способом зниження вразливості програмного забезпечення. Іноді вони є єдиним способом це зробити.

Керування патчем вимагає певних правил дотримання безпеки, таких як SOX та HIPAA. Несистематичне та несвоєчасне впровадження патчів може призвести до невдалої аудит-перевірки та покарання за недотримання безпеки. Керування патчами залежить від керування активами та даними для ідентифікації систем, на яких запущено програмне забезпечення, яке вимагає виправлення. На рисунку показано копію екрана (screen shot) інструменту SolarWinds Patch Manager.

На рівні підприємства, управління виправленням (патчем) найбільш ефективно запускається з системи управління патчем. Більшість систем управління патчем включають централізовану клієнт-серверну архітектуру, як і інші системи безпеки, пов’язані з кінцевими точками. Існують три технології управління патчем.

– На основі агента (Agent-based) – для цього потрібен програмний агент, який буде працювати на кожному хості, на якому будуть застосовуватись патчі. Агент повідомить, чи встановлено вразливе програмне забезпечення на хості. Агент спілкується з сервером керування патчами, визначає, чи є існуючі патчі, які потребують встановлення, та встановлює їх. Агент працює з достатніми привілеями, щоб він міг встановити патчі. Підходи, що базуються на агентах, є переважним засобом для виправлення (patching) мобільних пристроїв.

– Безагентне сканування (Agentless scanning) – сервери керування патчем сканують мережу для пристроїв, що вимагають внесення виправлення. Сервер визначає, які патчі потрібно, і встановлює ці патчі на клієнтах. Цим способом можна вносити виправлення лише у пристрої, що знаходяться на відсканованих сегментах мережі. Це може бути проблемним для мобільних пристроїв.

– Пасивний моніторинг мережі – пристрої, що вимагають внесення виправлень, ідентифікуються шляхом моніторингу трафіку в мережі. Такий підхід ефективний тільки для програмного забезпечення, яке включає в себе інформацію про версії в свій мережний трафік.

Системи управління безпекою

Система управління інформаційною безпекою (Information Security Management System-ISMS) складається з системи управління, за допомогою якої організація ідентифікує, аналізує та нейтралізує ризики інформаційної

безпеки. ISMS не базуються на серверах або на пристроях безпеки. Натомість ISMS складається з набору практик, які систематично застосовуються організацією для забезпечення постійного вдосконалення інформаційної безпеки. ISMS надає концептуальні моделі, якими керуються організації у плануванні, впровадженні, управлінні та оцінці програм захисту інформації.

ISMS є природним продовженням використання популярних бізнес-моделей, таких як Загальне управління якістю (Total Quality Management - TQM) та Цілі контролю за інформацією та суміжними технологіями (Control Objectives for Information and Related Technologies - COBIT), у сфері кібербезпеки.

ISMS – це системний, багаторівневий підхід до кібербезпеки. Підхід включає взаємодію людей, процесів, технологій та традицій у процесі управління ризиками.

ISMS часто включає в себе структуру "план-що зробити-перевірка-дія" (plan-do-check-act), що відома як цикл Демінга, з TQM. Це розглядається як деталізація процесу компонента моделі Люди-Процеси-Технології-Традиції (People-Process-Technology-Culture) для організації потенціалу, як показано на рисунку.

ISO є Міжнародною організацією з стандартизації (Organization for Standardization). Добровільна стандартизація ISO є прийнятою на міжнародному рівні та полегшує ведення бізнесу між країнами.

ISO співпрацює з Міжнародною електротехнічною комісією (International Electrotechnical Commission - IEC), щоб розробити сімейство специфікацій ISO/IEC 27000 для ISMS.

Сертифікація ISO 27001 – це глобальна, галузева специфікація для ISMS. На рисунку 2 ілюструється взаємозв'язок дій, передбачених стандартом, з циклом план-що робити-перевірка-дія (plan-do-check-act). Сертифікація означає, що політика і процедури безпеки організації були незалежно перевірені, щоб забезпечити систематичний і проактивний підхід

для ефективного управління ризиками безпеки щодо конфіденційної інформації про клієнтів.

NIST є дуже ефективним в області кібербезпеки, як ми вже бачили вище. NIST розробила фреймворк кібербезпеки, який, як і ISO/IEC 27000, є набором стандартів, що призначені для інтеграції існуючих стандартів, керівних принципів та практик щоб допомогти краще керувати та зменшити ризик в кібербезпеці. Цей фреймворк був вперше виданий у лютому 2014 року і продовжує проходити розробку.

Фреймворк складається з комплексу заходів, запропонованих для досягнення конкретних результатів кібербезпеки та посилання на приклади рекомендацій для досягнення цих результатів. Основні функції, що визначені на рисунку 1, поділяються на основні категорії та підкатегорії. Основні категорії забезпечують розуміння типів діяльності, що пов'язана з кожною з функцій.

Організації різних типів використовують фреймворк в різних напрямках. Багато хто вважає це корисним у підвищенні рівня інформованості та взаємодії із зацікавленими сторонами в рамках своєї організації, в тому числі для виконавчого керівництва. Фреймворк також покращує зв’язок між організаціями, дозволяючи розповсюджувати очікування від кібербезпеки між діловими партнерами, постачальниками та секторами. Шляхом порівняльного аналізу цього фреймворку до поточних підходів управління кібербезпекою, організації навчаються та демонструють, як вони відповідають стандартам, керівним принципам та передовому досвіду. Деякі учасники використовують фреймворк, щоб узгоджувати внутрішню політику з законодавством, регулюванням та існуючою практикою в галузі. Цей фреймворк також використовується як інструмент для стратегічного планування оцінки ризиків та існуючої практики.

Використання світового досвіду та локальних стандартів є необхідними для успішної побудови та експлуатації мережевої безпеки.

Алгоритми криптування інформації

Цифрові підписи – це математичний метод, що використовується для забезпеченню трьох основних послуг безпеки. Цифрові підписи володіють особливими характеристиками, які забезпечують автентичність об'єкта і цілісність даних.

Зазвичай, цифрові підписи використовуються у таких двох випадках:

– підписання коду – використовується з метою підтримки цілісності даних і аутентифікації. Підписання коду використовується для перевірки цілісності виконуваних файлів, завантажених із веб-сайту виробника. При цьому також використовуються підписані цифрові сертифікати для автентифікації і перевірки ідентичності сайту.

– цифрові сертифікати – подібні до віртуальної ID-карти, використовуються для підтвердження ідентичності системи веб-сайту виробника і встановлення зашифрованого з’єднання для обміну конфіденційними даними.

Для генерування і перевірки цифрових підписів визначено три алгоритми Стандарту Цифрового Підпису (Digital Signature Standard, DSS):

– Digital Signature Algorithm (DSA) – це вихідний стандарт для створення пар публічних і приватних ключів, а також для генерування і перевірки цифрових підписів.

– Rivest-Shamir Adelman Algorithm (RSA) – це асиметричний алгоритм, який традиційно використовується для генерування і перевірки цифрових підписів.

– Elliptic Curve Digital Signature Algorithm (ECDSA) – це новіша версія DSA, яка забезпечує аутентифікація цифрового підпису разом з неспростовністю, і має додаткові переваги у вигляді ефективності обчислень, менших розмірів підпису і мінімальної пропускної здатності.

Діффі-Хеллман використовує різні групи DH для визначення стійкості ключа, який бере участь у процесі узгодження. Вищий номер групи забезпечує більшу надійність, проте вимагає додаткового часу для обчислення ключа. Нижче наведено характеристики DH-груп, а також відповідні ним значення простого числа:

- DH Група 1: 768 бітів
- DH Група 2: 1024 бітів
- DH Група 5: 1536 бітів
- DH Група 14: 2048 бітів
- DH Група 15: 3072 бітів
- DH Група 16: 4096 бітів

Узгодження ключів DH також може виконуватися за допомогою криптографії еліптичних кривих. DH групи 19, 20 і 24, засновані на криптографії еліптичних кривих.

У 90-х роках, RSE Security Inc. вперше опублікувало стандарти криптографії на основі відкритих ключів (publish public-key cryptography, PKCS). Існувало 15 PKCS, хоча 1 було усунено ще під час написання. RSE опублікувало ці стандарти, оскільки мало патенти на них і хотіло їх популяризувати. PKCS не належать до промислових стандартів, проте широко визнаються у безпековій галузі і нещодавно почали ставати актуальними для таких організацій як робочі групи IETF і PKIX.

Інтернет-трафік складається з передачі даних між двома сторонами. При встановленні асиметричного з’єднання між двома хостами, вони обміняються інформацією про відкриті ключі. В Інтернеті існують довірені треті сторони, які перевіряють автентичність цих відкритих ключів за допомогою цифрових сертифікатів. Третя довірена сторона проводить ретельну перевірку перш ніж надати повноваження. Після такого поглибленого дослідження третя сторона видає посвідчення, яке важко

підробити. З цього моменту всі учасники, які довіряють цій третій стороні, просто приймають посвідчення, які вона видає.

Ці довірені треті сторони надають послуги, подібно до урядових органів ліцензування.

Інфраструктура Відкритих Ключів (Public Key Infrastructure, PKI) є прикладом довіреної третьої сторони, яку ще називають Центром Сертифікації (certificate authority, CA). CA надають послуги, подібно до урядових органів ліцензування. PKI – це структура, яка використовується для безпечного обміну інформацією між сторонами. CA видає цифрові сертифікати, для аутентифікації організацій і користувачів. Ці сертифікати також використовуються для підпису повідомлень, як гарантія того, що їх не було підроблено.

Моніторинг мережі стає значно складнішим, коли пакети шифруються. Проте, аналітики безпеки повинні бути в курсі цих змін і вирішувати їх якнайкраще. Наприклад, при використанні віртуальних приватних VPN-вузлів, Інтернет сервіс-провайдер повинен розміщуватися так, щоб мати можливість відстежувати незашифрований трафік.

Проте, збільшення HTTPS-трафіку в мережі підприємства веде за собою нові виклики. Оскільки, HTTPS впроваджує шифрування HTTP-трафіка між кінцевими точками (через TLS/SSL), не так просто переглядати трафік користувача.

Аналітик безпеки повинен знати як обійти і вирішити ці проблеми. Ось перелік деяких кроків, до яких може вдаватися аналітик безпеки:

– Налаштування правил, аби відрізнити SSL від не SSL-трафіку, HTTPS від не HTTPS SSL.

– Посилення безпеки шляхом перевірки сертифікату сервера за допомогою CRL і OCSP.

– Впровадження захисту проти шкідливих програм і фільтрування URL HTTPS-контенту.

– Використання Cisco SSL Appliance для розшифрування SSL-трафіку з подальшим надсиланням його до системи запобігання втручанням (IPS) для ідентифікації загроз, які часто ховаються у SSL.

Криптографія динамічна і постійно змінюється. Аналітик безпеки повинен добре розуміти криптографічні алгоритми й операції, аби мати можливість розслідувати інциденти безпеки, пов’язані з криптографією.

Існує два основні способи впливу криптографії на безпекові дослідження. По-перше, атаки можуть бути спрямовані на конкретні алгоритми шифрування. Після зламу алгоритму й отримання ключів, нападник може розшифрувати і переглянути будь-які перехоплені зашифровані дані, наражаючи на небезпеку конфіденційну інформацію. Розслідування безпеки також піддається впливу, оскільки дані у відкритому вигляді можна приховати за допомогою шифрування. Наприклад, трафік контролю і керування, зашифрований за допомогою TLS/SSL найбільш імовірно буде непомітний для фаєрвол. Трафік контролю і керування між сервером контролю і керування та ураженим комп’ютером у захищеній мережі неможливо зупинити, якщо він непомітний і нерозпізнаний. Нападник зможе продовжити свою діяльність через використання зашифрованих команд для зараження більшої кількості комп’ютерів і можливим створенням ботнету. Цей тип трафіку можна виявити шляхом розшифрування трафіку і порівняння його із сигнатурами відомих атак, або при детектуванні аномального трафіку TLS/SSL. Це може бути досить складно і затратно по часу, або спрацьовує за принципом "пан або пропав".

Проект вдосконалених методів та засобів побудови та впровадження надійної, продуктивної та захищеної мережевої архітектури.

Організація повинна запроваджувати належні засоби контролю доступу для захисту мережних ресурсів, ресурсів інформаційної системи та інформації.

Моделі контролю доступу можуть бути:

– примусовий контроль доступу (Mandatory access control, MAC) – застосовує найсуворіший контроль доступу і зазвичай використовується у військових або критичних для застосування програмах. При його використанні інформації призначаються мітки безпеки, а користувачам надається доступна основі визначеного рівня захисту.

– контроль доступу на власний розсуд (Discretionary access control, DAC) – полягає в тому, що користувачі, як власники даних, самі контролюють доступ до них. DAC можуть використовувати ACL або інші методи для визначення того, які користувачі або групи користувачів мають доступ до інформації.

– обов'язковий контроль доступу (Non-Discretionary access control) – рішення з надання доступу базуються на ролі особи та її відповідальності всередині організації, цей спосіб також відомий як контроль доступу на основі ролей (role-based access control, RBAC)

– контроль доступу на основі атрибутів (Attribute-based access control, ABAC) – дозволяє доступ на основі атрибутів об'єкта (ресурсу), до якого звертаються, суб'єкта (користувача), який звертається до ресурсу, та зовнішніх факторів щодо того, як і коли слід звертатися до об'єкта, наприклад, час доби.

Ще одна модель контролю доступу використовує принцип найменших привілеїв. При цьому користувачеві або процесу за їх вимогою надається

чітко окреслений доступ до певної інформації та інструменту. Принцип найменших привілеїв передбачає, що користувачам слід надавати мінімальний доступ, необхідний для виконання їх роботи.

Існує поширений експлойт відомий як розширення привілеїв. Він використовує вразливості серверів або систем контролю доступу на предмет надання неавторизованому користувачеві або програмному процесу вищого рівня повноважень ніж їм призначено. Після розширення привілеїв зловмисник може отримати доступ до конфіденційної інформації або взяти систему під контроль.

Всебічна політика безпеки має низку переваг:

– демонструє дотримання організацією вимог безпеки;

– встановлює правила очікуваної поведінки;

– забезпечує послідовність у системних операціях, придбанні програмного й апаратного забезпечення, а також супроводі;

– визначає законні наслідки порушень;

– надає працівникам з безпеки підтримку керівництва.

Політика безпеки використовується для інформування користувачів, персоналу та менеджерів щодо вимог організації для захисту технологій та інформаційних ресурсів. Політика безпеки також визначає механізми, необхідні для задоволення вимог безпеки, і забезпечує основу, за допомогою якої можна придбати, налаштовувати та перевіряти відповідність їй комп'ютерних систем і мереж.

До політики безпеки належать:

– політики ідентифікації та аутентифікації – визначає уповноважених осіб, які мають доступ до мережних ресурсів, та встановлює процедури перевірки;

– політики паролів – забезпечують мінімальні вимоги, яким мають відповідати паролі, а також регулярність їх зміни;

– політика прийнятного використання (AUP) – визначає мережні прикладні програми та застосування, допустимі для організації. Також вона може визначати наслідки в разі порушення політики;

– політика віддаленого доступу – визначає спосіб, у який віддалені користувачі можуть одержувати доступ до мережі, а також те, що доступно через віддалене підключення;

– політика підтримки мережі – визначає процедури оновлення операційних систем мережних пристроїв та прикладних програм кінцевих користувачів;

– процедури обробки інцидентів – описує як обробляються інциденти безпеки.

Однією з найпоширеніших компонентів політики безпеки є політика прийнятного використання (AUP). Її ще називають політикою належного використання. Цей компонент визначає, що дозволено робити користувачам на різних системних компонентах, включно з типом трафіку, який можна передавати мережею. Аби уникнути непорозумінь AUP повинна бути якомога детальнішою. Наприклад, AUP може містити перелік веб сайтів, груп новин або інтенсивних прикладних програм, до яких забороняється мати доступ з комп'ютерів або з мережі компанії. Кожен працівник повинен підписувати AUP, і підписані політики потрібно зберігати протягом всього періоду роботи.

За результатами виконаних досліджень методів та засобів розробки та впровадження надійної, продуктивної та захищеної мережевої архітектури вдалось визначити ключові вимоги до вдосконалення розглянутих вище характеристик інформаційних мереж:

– розробка надійнійного та гнучкого мережевого дизайну;

– дослідження запровадження нових технологій, що базуються на концепції програмно конфігурованих мереж;

– створення пріоритизації трафіку для реалізації QoS;

– впровадження моніторингу роботи компонентів мережі з можливістю подальшого аналізу;

– створення певної надлишковості надійності мережевих компонентів;

– віртуалізація елементів мережі;

– запровадження систем виявлення та протидії загрозам.

Базуючись на дослідженому матеріалі запропоновано вдосконалений мережевий дизайн (рисунок 2.1). За основу взято трирівневу модель дизайну мережі, де в запропонованому проекті можна додати рівень програмно-конфігурованих мереж для здешевлення набору обладнання та автоматизації мережевих функцій. З точки зору найбільшого навантаження цей рівень відповідає за ресурсоємні завданн і тому реалізація такого варіанту дасть змогу швидко вносити необхідні корективи в переналагодження апаратних компонентів через API додатки. Найменші зміни пропонуються на рівні доступу, оскільки він забезпечує під’єднання кінцевих користувачів і його основною характеристикою є кількість портів. Стандартних функцій управління користувачами є достатньо і тільки розробка правильних політик безпеки мережі дасть змогу його ефективного функціонування. Будь-які технічні вдосконалення на цьому рівні будуть збільшувати вартість проекту, а користь від такого підходу буде не настільки очевидною. Кореневий рівень є дуже важливою складовою мережевого дизайну і тому його висока доступність та функціональність є вкрай важливою. Протоколи резервування маршрутизаторів та віртуалізації мережевих шлюзів є одним з варіантів, що можуть покращити роботу на цьому рівні та підвищити надійність, продуктивність та захищеність мережевої архітектури. Забезпечення правильного налаштування годинників виконано через протокол NTP. Моніторинг та ведення статистики через SNMP та Syslog відповідно.

Приклад удосконаленого мережевого дизайну з підвищеною надійністю роботи показано на рисунку 2.1.

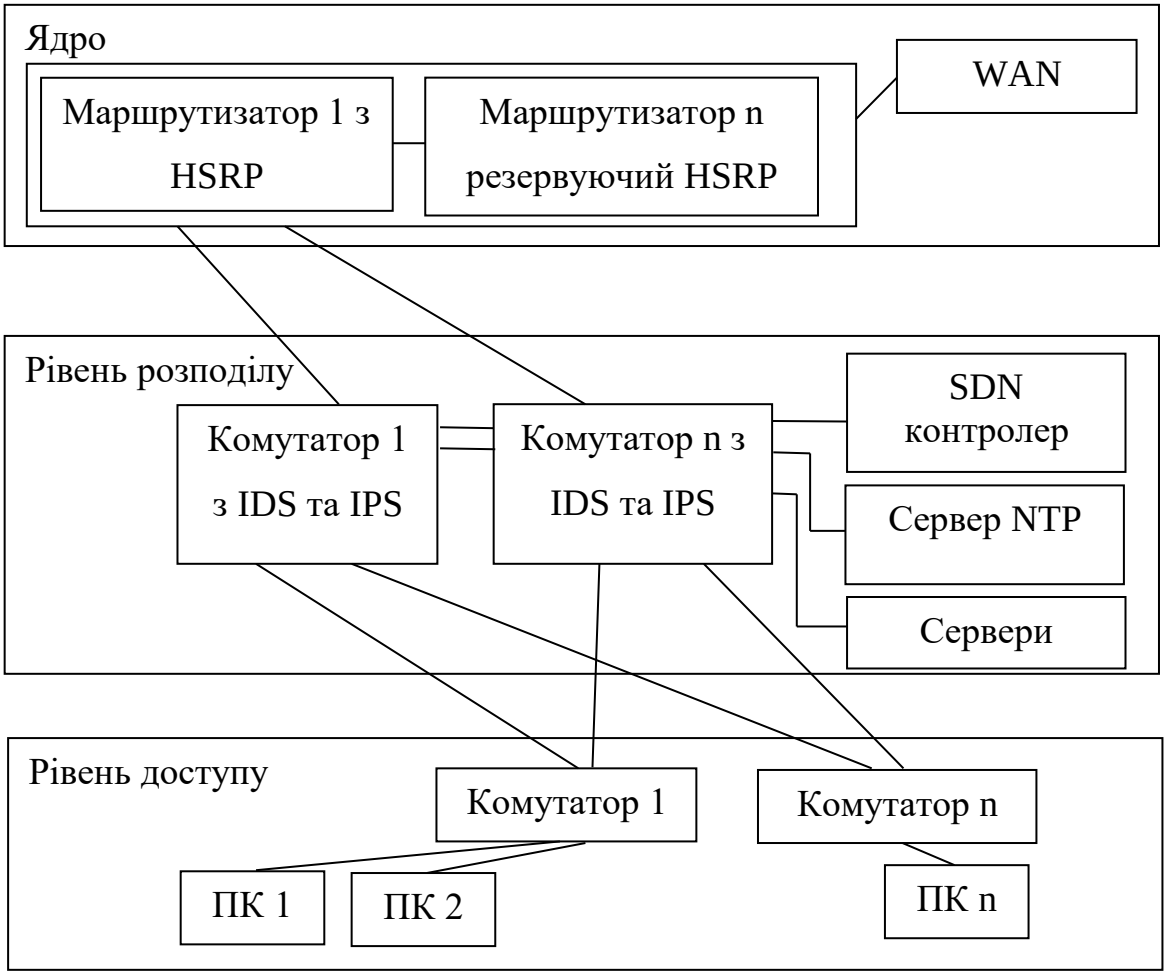

Рисунок 2.1 – Удосконалення надійності, продуктивності та захищеності мережевої архітектури

Запропоновані в роботі рішення покликані вдосконалити методи та засоби розробки та впровадження надійних, продуктивних та захищених мережевих архітектур.

Висновки до другого розділу

В другому розділі дипломної роботи для підвищення надійності функціонування комп'ютерних мереж запропоновано використання методів аналізу та управління трафіком, що базуються на протоколах SNMP та

Syslog, що дало змогу в реальному часі проводити моніторинг роботи мережевих компонентів та аналізувати інциденти з фіксацією часу події. Використано при забезпечені організаційно-технічних засобів забезпечення працездатності мережі впровадити ААА сервери для забезпечення аутинтифікації, а також розроблено рекомендації для створення надійних паролів. Проведено аналіз управління ризиками мережевої безпеки. Подано систему управління безпекою. Наведено алгоритми криптування інформації для покращення роботи системи. Запропоновано проект вдосконалених методів та засобі розробки та впровадження надійної, продуктивної та захищеної архітектури.

СПЕЦІАЛЬНА ЧАСТИНА

Підвищення надійності мереж на основі SDN

Збільшення кількості і різнорідності контенту, розвиток сервісів, масштабів їх охоплення, зростання обсягу трафіку створило проблему пропускної здатності, яка не дає змоги задовольнити зростаючі потреби користувачів. Як результат, запропоновано технологію SDN. Вона покликана підвищити ресурсоємність та покращити функціональність мереж в хмарних обчисленнях, ЦОД і на магістралях мереж. Новітні мережеві технології дадуть змогу зробити мережі більш гнучкими, адаптивними і динамічними, з метою підтримки сучасного темпу розвитку швидко мінливих бізнес-вимог.

В основу технології SDN покладені такі ідеї:

– поділ процесів передачі та управління даними;

– єдиний, уніфікований, незалежний від постачальника інтерфейс між рівнем управління і рівнем передачі даних;

– логічно централізоване управління мережею;

– віртуалізація мережевих ресурсів.

В подальшій роботі проведено дослідження технічної можливості впровадження технології SDN для вирішення проблем, що виникають в сучасних мережах.

Система програмованих мереж (SDN) є новою мережевою архітектурою, в якій управління не пов’язане з передаванням даних, а напряму програмоване. Якщо раніше воно пов’язувалося з окремими мережевими пристроями, то тепер - трансформувалось у форму, що дає змогу окремим прикладним програмам та сервісам бачити базову інфраструктуру мережі як єдину абстракцію або логічне чи віртуальне ціле.

Архітектура SDN містить в собі три рівні:

– інфраструктурний рівень, що надає набір мережевих пристроїв (комутаторів і каналів передачі даних);

– рівень управління, що включає в себе мережеву операційну систему, яка забезпечує додаткам мережеві сервіси і програмний інтерфейс для управління мережевими пристроями і мережею;

– рівень мережевих додатків для гнучкого й ефективного управління мережею.

Сучасні мережеві архітектури на основі програмно конфігурованих мереж надають гнучкість управління специфічними задачами з передавання даних, що в свою чергу підвищує надійність послуг. Наприклад, в мережах “Розумного міста” часто виникає потреба налаштувати певні види сервісів і при цьому операційної системи обладнання не є достатньо для виконання таких завдань. Вирішення такого роду проблем можливе через використання програмованих додатків, що можуть впроваджуватись в мережі SDN.

Дана архітектура графічно представлена на рисунку 3.1

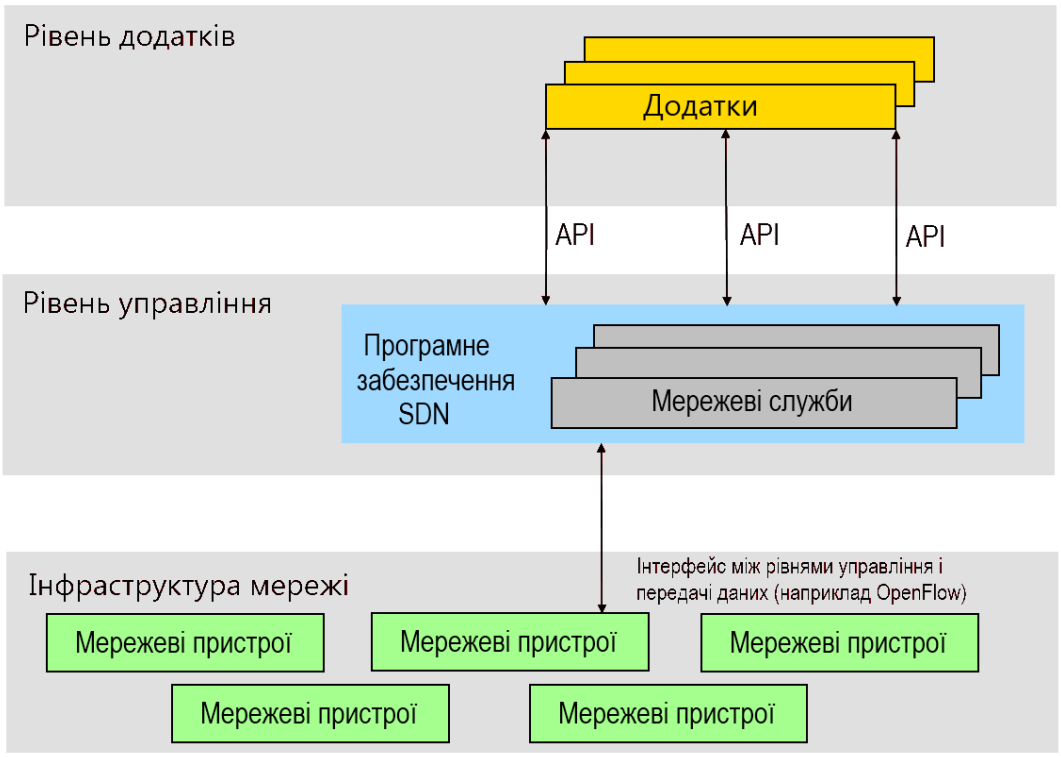

Рисунок 3.1 – Організаційна структура SDN

Для забезпечення функції централізації управління використовується SDN-контролер. На ньому запускаються відповідні мережеві додатки, які виконують функції управління мережею. Адміністратори можуть змінити поведінку мережі в режимі реального часу і розгортати нові додатки, які надаються виробником або розробляються самостійно під конкретні завдання.

Для з'єднання рівня управління та рівня передачі даних використовують спеціальні протоколи. Найбільш поширеним та стандартизованим протоколом є OpenFlow, який є відкритим, тобто всі деталі внутрішнього алгоритму доступні для розробників. Цей протокол забезпечує прямий доступ і можливість маніпуляції рівнем передавання даних мережевих пристроїв (комутатори і маршрутизатори) з підтримкою мультивендорності.

Актуальність та перспективи розвитку цього рішення підтверджуються тим, що провідні виробники (Cisco, Juniper, IBM, NEC, HP) забезпечують сумісність з протоколом OpenFlow.

Виділення функції управління в окремий рівень та її делегування центральному компоненту націлені на оптимізацію мережних конфігурацій для вирішення прикладних завдань і, зокрема, дозволяють отримати наступні переваги: формати даних, правила обробки та технології передачі в комутаторі не обмежені певним рівнем взаємодії, типом устаткування або виробником; одиниця передачі може бути задана багатовимірним вектором, що включає поля з різних рівнів моделі мережної взаємодії; при побудові правил пересилки пакетів можуть застосовуватися методи автоматизованої корекції потоків залежно від навантаження компонентів та інших критеріїв; контролери мережі можуть об'єднуватися в мережні домени, які дозволяють оптимізувати та резервувати канали передачі.

Інтелектуальні функції мережі зосереджені в централізованому мережному контролері, який відстежує загальний стан мережної

інфраструктури і потоків, що протікають по ній. У такій концепції управління всією мережею відбувається в єдиній логічній точці, що значно спрощує завдання конфігурації та управління. Крім того, простіше виглядає і функціонування мережних пристроїв, тому що на відміну від традиційної моделі не потрібно більше підтримувати та обробляти безліч різних протоколів, а достатньо тільки отримувати та обробляти інструкції від контролерів ПКМ. Для налаштування мережі досить набудувати програмний контролер мережі, замість того, щоб змінювати сотні рядків кодів в безлічі мережних пристроїв мережі. Також поведінку мережі можна змінювати в реальному часі, а нові рішення впроваджувати за набагато коротший час, ніж в традиційній архітектурі. Централізуючи стан мережі в єдиному рівні контролю, ПКМ можуть конфігуруватися за допомогою програмних засобів. Мережні контролери також володіють набором прикладних інтерфейсів, які дозволяють реалізувати типові завдання по маршрутизації, зокрема багатоадресність, безпека, контроль доступу, управління смугою пропускання, якість обслуговування, які дуже вузьконаправлено налаштовані під завдання конкретного споживача.

У комутаторі реалізований тільки рівень передачі даних. Замість контролера використовується набагато простіший пристрій, завдання якого полягає в отриманні даних, які надходять, визначення їх адресів і, якщо адресат є в таблиці комутації, негайної передачі даних комутаційній матриці. Інакше комутатор по захищеному каналу відправляє запит на центральний контролер мережі, і на підставі отриманої від нього інформації, вносить необхідні зміни в таблицю комутації, після чого здійснюється обробка отриманих даних (устаткування не переналаштовується вручну, а налаштовується за допомогою спеціального ПЗ). Ідея ПКМ у створенні уніфікованого, незалежного від виробника мережного устаткування, програмно-керованого інтерфейсу між контролером та транспортним середовищем мережі знайшла віддзеркалення в протоколі OpenFlow, що

дозволяє користувачам самим визначати і контролювати, хто з ким, за яких умов і з якою якістю може взаємодіяти в мережі.

Комутатор OpenFlow послідовно порівнює вміст кадру, що передається із записами ТП (таблиця потоків) і при збігу виконує вказані в записі дії. Якщо збіг не знайдений, то залежно від налаштувань комутатору пакет може бути відкинутий або відправлений OpenFlow-запит контролеру для ухвалення рішення. Контролер може додавати, модифікувати, видаляти записи з таблиць як на основі аналізу пакетів, що отримуються від мережного устаткування, так і виходячи з власних алгоритмів роботи.

Специфікація OpenFlow визначає різноманітний набір інструкцій для обробки одиниць передачі, серед яких пересилка до порту(ів) або контролеру (Output), зміна полів (Set-Field, Change-TTL), робота з тегами IEEE 802.1Q та MPLS (Push-Tag/Pop-Tag), групові операції (Group) та ін. Також існує специфікація гібридного комутатора з підтримкою як OpenFlow-операцій, так і класичної комутації. За допомогою протоколу OpenFlow фахівцям потрібно буде витрачати менше часу на початкові налаштування мережі та передачі її в експлуатацію в практично автоматичному режимі для підтримки заданого QoS. Всі маршрутизатори та комутатори об’єднуються під управлінням Мережевої Операційної Системи (МОС), яка забезпечує програмним забезпеченням доступ до управління мережею, і яка постійно відстежує конфігурацію засобів мережі. Потік даних flow таблиць OpenFlow (OpenFlow pipeline) містить безліч flowтаблиць, які можна об’єднати в деревовидні структури, що дозволяє ефективніше використовувати асоціативну пам’ять TCAM та реалізувати практично будь-які сценарії обробки і просування даних. Процес просування таблиць завжди починається з першої таблиці з номером “0”, а закінчується, якщо немає вказівки на наступну flow-таблицю з вищим номером.

При розгортанні програмно конфігурованих мереж потрібно врахувати можливість виходу з ладу контролера або його дублюючих

елементів. При цьому мережа втрачає гнучкість роботи надану ПКМ і необхідно для забезпечення надійності врахувати альтернативні режими роботи мережі. У випадку правильно розробленої мережевої архітектури та вибору активного мережевого обладнання може спостерігатись певне сповільнення при прийнятті рішень з передачі даних, втрата деяких особливостей, що повинно некритично відобразитись на загальній роботі мережі.

Комутатор з підтримкою OpenFlow є простим комутуючим елементом, який пересилає пакети між портами. Самі правила для комутації визначаються безпосередньо віддаленим контролером. Приклад такого комутатора наведено на рисунку 3.2.

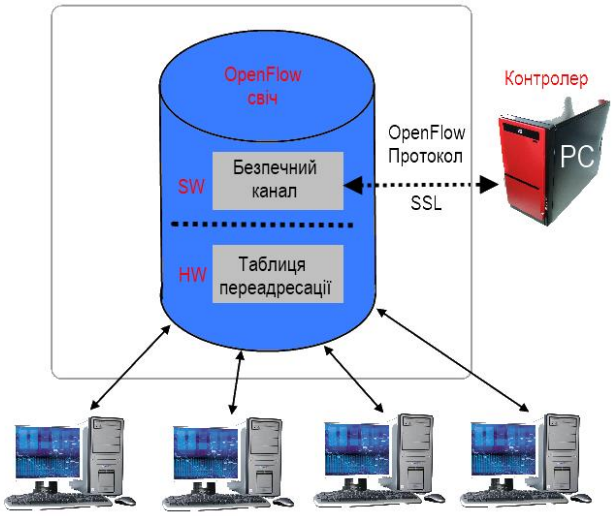

Рисунок 3.2 – Комутатор OpenFlow

Реалізація контролерів може бути на різноманітних апаратних платформах, де за допомогою операційної системи забезпечується зв’язок з додатками, що відповідають за певні функції. Вони включають в себе визначення активних комутаторів в мережі, визначення активних портів на комутаторах, зв'язок з комутаторами за допомогою протоколу OpenFlow та опис логіки комутації і маршрутизації пакетів у всій мережі для заповнення таблиці потоків.

На основі інформації, отриманої через протокол OpenFlow, контролери заповнюють таблиці, які в подальшому використовують для прийняття рішень. Цей процес відбувається через аналіз заголовків пакетів, які отримуються через безпечний канал між пристроями. Кожному елементу таблиці присвоюється певна дія, асоційована з окремим потоком, основні з яких зображені на рисунку 3.3.

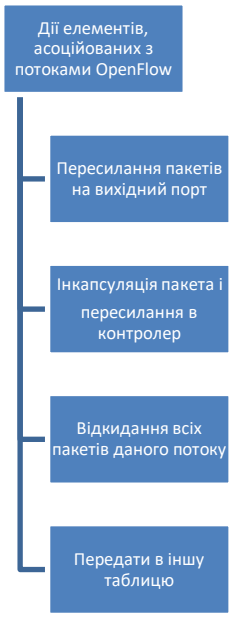

Рисунок 3.3 – Основні дії з потоками OpenFlow

Запис в OpenFlow таблиці містить три елементи:

– заголовок пакета, який визначає потік;

– дія над потоком;

– статистика, що показує кількість пакетів, байтів, а також час пересилки останнього пакета цього потоку, щоб відслідковувати їх активність.

Треба відмітити, що зручність протоколу OpenFlow полягає в тому, що він реалізований на більшості сучасного обладнання і немає потреби оновлювати програмне забезпечення операційних систем. Це зумовлює універсальність при виборі OpenFlow як міжвендорного протоколу для створення програмно конфігурованих мереж.

Отже, мережі, побудовані на основі технології SDN, найчастіше використовують протокол OpenFlow, який забезпечує зв’язок між рівнями логічної архітектури програмованих мереж.

Резервування мережевих ресурсів

Критичними компонентами, які потребують резервування у більшості локальних мереж, є шлюзи та сервери додатків. Функції шлюзу можуть виконувати як прикордонні маршрутизатори, так і міжмережні екрани. Для кінцевих користувачів необхідно, щоб методи та алгоритми резервування вищезгаданих пристроїв були прозорими, тобто їх функціонування не вимагало додаткового програмного забезпечення та додаткових дій щодо налагодження мережних пристроїв.

Особливості резервування критичних компонентів локальних мереж пов’язані з використанням цими компонентами статичних фізичних і логічних адрес та підтримкою одночасного інформаційного обміну з багатьма вузлами мережі. Тобто для того, щоб резервний компонент міг виконувати функції основного, необхідно, щоб його канальні та мережні адреси збігалися з адресами основного компонента, а це суперечить базовим принципам організації інформаційного обміну на канальному та мережному рівнях моделі OSI. Розв’язання зазначеної суперечності потребує застосування спеціальних методів, які повинні забезпечувати:

– формування групи резервування, яка складається з основного і резервного (резервних) пристроїв;

– колективне використання адрес членами групи резервування;

– створення та налагодження віртуального пристрою для забезпечення інформаційного обміну з кінцевими абонентами різних мереж (виконання функцій шлюзу за замовчуванням);

– постійний моніторинг стану основного пристрою іншими членами групи резервування.

Всі вищеперераховані функції, як правило, реалізуються у вигляді програмних модулів, що підтримують роботу відповідних протоколів динамічного резервування на основному та резервному пристроях мережі.

Серед найбільш поширених протоколів динамічного резервування компонентів локальних мереж (відомих як FHRP, First Hop Redundancy Protocols), що використовуються у сучасних мережах, слід згадати такі:

– HSRP, Hot Standby Router Protocol (Cisco Systems Inc.);
– VRRP, Virtual Router Redundancy Protocol;
– CARP, Common Address Redundancy Protocol;
– GLBP, Gateway Load Balancing Protocol (Cisco Systems Inc.);
– IPSTB, IP Standby Protocol (DEC, Digital Equipment Corporation);
– ESRP, Extreme Standby Router Protocol (Extreme Networks);
– R-SMLT, Routed Split Multi-Link Trunking (Avaya);
– NSRP, NetScreen Redundancy Protocol (Juniper Networks);
– XRRP, XL Router Redundancy Protocol (Hewlett Packard).

Протокол HSRP є першим фірмовим протоколом, який був розроблений для динамічного резервування шлюзу у мережах, побудованих на базі маршрутизаторів і багаторівневих комутаторів Cisco. Подібний за функціями відкритий протокол VRRP був розроблений IETF як альтернатива протоколу HSRP. Протокол CARP також є відкритим протоколом, але з обмеженим застосуванням, оскільки він був розроблений лише для резервування серверів для BSDподібних ОС. Решта протоколів – це фірмові розробки відповідних виробників мережного обладнання та ПЗ. Деякі із зазначених протоколів окрім резервування забезпечують балансування (розподіл) навантаження при передачі трафіка (наприклад, GLBP і NSRP) та захист на канальному рівні (ESRP). Сьогодні більшість виробників (окрім

фірми Cisco Systems Inc.) відмовилися від своїх фірмових протоколів резервування шлюзу на користь протоколу VRRP.

Для забезпечення функціонування протоколу HSRP уведено поняття маршрутизатор HSRP (HSRP Router) та група резервування HSRP (HSRP Standby Group). Маршрутизатором HSRP є будь-який маршрутизатор (або багаторівневий комутатор), на одному з інтерфейсів якого активовано використання протоколу HSRP. До групи резервування HSRP входять активний маршрутизатор HSRP (HSRP Active Router) та резервний маршрутизатор HSRP (HSRP Standby Router, HSRP Primary Backup Router). Резервних маршрутизаторів у одній групі може бути декілька. У такому разі обирається один резервний маршрутизатор, решта маршрутизаторів уважаються запасними маршрутизаторами HSRP (HSRP Backup Routers). Для решти вузлів мережі група резервування HSRP подається як один віртуа- 5 льний маршрутизатор HSRP (HSRP Virtual Router), якому відповідає одна віртуальна адреса мережного рівня (HSRP Virtual IPAddress) та одна віртуальна адреса канального рівня (HSRP Virtual MAC Address). Тобто віртуальний маршрутизатор HSRP є шлюзом за замовчуванням для всіх вузлів локальної мережі. Оскільки функції віртуального маршрутизатора HSRP фактично виконує активний маршрутизатор HSRP, то саме через нього здійснюється фізична пересилка IP-пакетів до інших мереж. Слід зазначити, що один реальний маршрутизатор може бути членом кількох груп резервування HSRP, в одних групах він може бути активним, в інших – резервним. За рахунок цієї властивості реалізовуються схеми підключення локальних мереж, у яких необхідне статичне балансування навантаження.

Вибори активного та резервного маршрутизаторів HSRP здійснюються на основі механізму пріоритетів (Priority). Пріоритет маршрутизатора HSRP може набувати значень у діапазоні від 0 до 255. Маршрутизатор із найбільшим пріоритетом вибирається як активний маршрутизатор HSRP, йому призначаються віртуальна IPадреса та віртуальна

MAC-адреса, і на нього покладаються функції маршрутизації. Маршрутизатор із наступним пріоритетом вибирається як резервний маршрутизатор HSRP. Решта маршрутизаторів уважаються запасними маршрутизаторами HSRP. Якщо пріоритети маршрутизаторів, які претендують на роль активного, однакові, то виконується порівняння їх IP-адрес і маршрутизатор із найбільшою адресою стає активним маршрутизатором HSRP. Якщо пріоритети маршрутизаторів, які претендують на роль резервного, однакові, також виконується порівняння їх IP-адрес і маршрутизатор із найбільшою адресою стає резервним маршрутизатором HSRP.

Для підтвердження свого статусу активний маршрутизатор групи резервування HSRP періодично (через інтервал Hello Time) розсилає решті маршрутизаторів повідомлення свого існування HSRP Hello. Якщо резервний і запасні маршрутизатори не отримують повідомлення HSRP Hello через певний проміжок часу (інтервал Hold Time), то вони констатують, що активний маршрутизатор вийшов із ладу (або вимкнений примусово), відповідно резервний маршрутизатор стає активним і серед запасних маршрутизаторів обирається новий резервний. Маршрутизатор, який має намір стати активним, 6 для інформування решти членів групи резервування HSRP розсилає повідомлення наміру проведення перевиборів – повідомлення HSRP Coup. Якщо ж маршрутизатор не має наміру більше бути активним, він повинен розіслати повідомлення відмови від статусу активного маршрутизатора – повідомлення HSRP Resign.

При виконанні операцій протоколу HSRP маршрутизатор групи резервування HSRP може знаходитися в одному з таких станів:

– початковий стан (Initial State);
– стан навчання (Learn State);
– стан прослуховування мережі (Listen State);
– стан передачі повідомлень (Speak State);

– стан резервного маршрутизатора (Standby State/Standby Router);

– стан активного маршрутизатора (Active State/Active Router).

Особливістю протоколу HSRP є те, що в разі його застосування лише один із маршрутизаторів групи резервування HSRP – резервний маршрутизатор, – контролює стан активного маршрутизатора, а, отже, може його замінити при виході з ладу. Решта маршрутизаторів групи – запасні маршрутизатори, контролюють стан резервного маршрутизатора. При виході з ладу резервного маршрутизатора його функції починає виконувати той запасний маршрутизатор, пріоритет якого є найбільшим.

Тому з метою підвищення надійності роботи у протоколі HSRP введені дві взаємозалежні та взаємопов’язані функції: Interface Tracking та Preempt. Функція Interface Tracking забезпечує контроль стану зовнішніх (щодо HSRP-інтерфейсу) інтерфейсів маршрутизатора та динамічну зміну пріоритету маршрутизатора. У разі виходу з ладу зовнішнього інтерфейсу (або виникнення проблем у каналі зв’язку) дана функція зменшує значення пріоритету HSRPмаршрутизатора, а при відновленні роботи – збільшує. Функція Preempt забезпечує швидкі перевибори нових активного та резервного маршрутизаторів після змін пріоритетів пристроїв. Слід зазначити, що згадані функції використовуються одночасно.

Висновки до третього розділу

В даному розділі дипломної роботи розглянуто питання підвищення надійності роботи мереж за рахунок впровадженні технології SDN та резервування ресурсів на базі протоколу HSRP.

ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Основною метою розділу дипломної роботи є проведення розрахунків економічних показників, для визначення економічної ефективності розробки та впровадження методів і засобів надійності, продуктивності та безпеки мережевих архітектур і на основі цього прийняття рішення наступного розвитку і використання або ж недоцільності впровадження відповідної розробки.

Розрахунок норм часу розробки мережевої архітектури

Витрати часу по окремих операціях відображені в таблиці 4.1.

Таблиця 4.1 – Операції технологічного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Витрати праці на створення технічного завдання розробки методів і засобів підвищення безпеки комп’ютерних мереж	Інженер	25
2.	Витрати праці на розробку фізичної топології мережі	Інженер	30
3.	Витрати праці на розробку локальної адресації мережі	Інженер	30
4.	Витрати праці на побудову мережі згідно поставленого завдання	Інженер	100
5.	Витрати праці на підготовку документації	Інженер	20
6.	Приблизний час роботи мережі	Інженер	5000
Разом			5205

Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Рекомендовані тарифні ставки: керівник проекту – 30,00...150,00 грн./год., інженер – 22,41...100,00 грн./год., консультант – 22,41...100,00 грн./год., технік – 22,41...100,00 грн./год., лаборант – 22,41...90,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г, \qquad (4.1)$$

де T_c – тарифна ставка, грн.;

$K_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в даному випадку виконує інженер, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 22,41 \cdot 5205 = 116644,05 \ грн.$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (4.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод.} = 116644,05 \cdot 0,15 = 17496,61 \ грн.$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.}. \quad (4.3)$$

$$В_{о.п.} = 116644,05 + 17496,61 = 134140,66 \ грн.$$

Крім того, слід визначити відрахування на соціальні заходи в розмірі становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{ОП} \cdot 0,235, \quad (4.4)$$

де $Ф_{ОП}$ – фонд оплати праці, грн.

$$В_{с.з.} = 134140,66 \cdot 0,235 = 31523,05 \ грн.$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн. *6=3+4+5*
		Тарифна ставка, грн.	К–сть відпрацьов. год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	Інженер	22,41	5205	116644,05	17496,61	31523,05	165663,71

Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{Bi} = q_i \cdot p_i, \tag{4.5}$$

Де: q_i – кількість витраченого матеріалу і–го виду;

p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{Bi}. \tag{4.6}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю, грн	Затрати матеріалів, грн	Транспортно–заготівельні витрати, грн	Загальна сума витрат на матеріали, грн
1	2	3	4	5	6	7
1. Основні матеріали						
Апаратний брандмауер	штук	3	50000,00	150000,00	4000,00	154000,00

Продовження таблиці 4.3

Кабель	метри	2000	20,00	40000,00	800,00	40800,00
Комп'ютери	штук	8	30000	240000	3000	243000,00
Інше мережеве обладнання та матеріали	-	-	15000	15000	-	15000
2. Допоміжні витрати						
Використання мережі Internet	годин и	–	1400	1400	–	1400
Разом:						454200,00

Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_e = W \cdot T \cdot S \text{ ,} \tag{4.7}$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат–години електроенергії.

Вартість кіловат–години електроенергії слід приймати згідно існуючих на даний час тарифів (0,203 грн. + 20% ПДВ за 1 кВт). Отже, 1 кВт з ПДВ коштує 0,2436 грн.

Потужність мережевого обладнання – 6 кВт, кількість годин роботи обладнання згідно таблиці 4.1 –5205 годин.

Тоді, $З_e = 6 \cdot 5205 \cdot 0{,}2436 = 7607{,}63$ *грн.*

Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (4.8)$$

де A – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %.

Для даного проекту вартість обладнання становить 30000 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = \frac{30000 \cdot 5\%}{100\%} = 1500{,}00 \ грн.$$

Оскільки робота мережі 5205 годин, то амортизаційні відрахування будуть становити:

$$A = \frac{750{,}00 \cdot 5205}{150} = 52050{,}00 \ грн.$$

Обчислення накладних витрат

Накладні витрати пов’язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно–правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6, \qquad (4.9)$$

де H_B – накладні витрати.

Отже, накладні витрати:

$H_в = 134140{,}66 \cdot 0{,}2 = 26828{,}13$ *грн.*

Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Витрати на оплату праці (основну і додаткову заробітну плату)	134140,66	18,99
Відрахування на соціальні заходи	31523,05	4,46
Матеріальні витрати	454200,00	64,3
Витрати на електроенергію	7607,63	1,08
Амортизаційні відрахування	52050,00	7,37
Накладні витрати	26828,13	3,8
Собівартість	706349,47	100

Собівартість (C_B) мережі розрахуємо за формулою:

$$C_B = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + A + H_в. \quad (4.10)$$

Отже, собівартість локальної мережі дорівнює:

$C_B = 134140,66 + 31523,05 + 454200,00 + 7607,63 + 52050,00 + 26828,13 = 706349,47$ *грн.*

Розрахунок ціни мережі

Ціну мережі можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) + K \cdot B_{н.і.}}{K} \cdot (1 + ПДВ), \quad (4.11)$$

де $P_{рен.}$ – рівень рентабельності, 30 %;

K – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

ПДВ – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Вн.і. , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (4.12)$$

Звідси ціна на проект складе:

$$Ц = 706349,47 \cdot (1+0,3) \cdot (1+0,2) = 1101905,18 \text{ грн.}$$

Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_р = \frac{П}{C_В}, \tag{4.13}$$

де $П$ – прибуток;

$C_В$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_В. \tag{4.14}$$

Розраховуємо плановий прибуток:

$$П_{пл} = 1101905,18 - 706349,47 = 395555,70 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{Св}. \tag{4.15}$$

Тоді, $E_р = \frac{395555,70}{706349,47} = 0,56$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (Тр):

$$T_p = \frac{1}{E_p}, \tag{4.16}$$

Термін окупності дорівнює:

$T_p = \frac{1}{0,56} = 1,8$ роки

Висновки до п’ятого розділу

В цьому розділі дипломної роботи було розраховано основні техніко–економічні показники від впровадження методів та засобів підвищення надійності, продуктивності та безпеки комп’ютерних мереж (таблиця 4.5).

Розраховане значення економічної ефективності становить 0,56, що є прийнятним значенням.

Так само нормальним є термін окупності. Для даної мережі він становить 1,8 років.

Таблиця 4.5 – Техніко–економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	706349,47
2.	Плановий прибуток, грн..	395555,70
3.	Ціна, грн.	1101905,18
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Отже, дані методи та засоби підвищення надійності, продуктивності та безпеки комп’ютерних мереж можуть бути впроваджені та мати подальший розвиток, оскільки вони є економічно вигідним за всіма основними техніко–економічними показниками.

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Охорона праці

Освітлення робочого місця

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: “Про охорону праці”, “Про охорону здоров’я”, “Про пожежну безпеку”.

Приміщення, в яких встановлені персональні комп’ютери, повинні мати природне та штучне освітлення відповідно до СНиП II-4-79.

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%. Розраховується КПО за методикою, викладеною в СНиП II-4-79.

Штучне освітлення в приміщеннях з робочими місцями має здійснюватись системою загального рівномірного освітлення. У разі переважної роботи з документами, допускається застосування системи комбінованого освітлення (крім системи загального освітлення додатково встановлюються світильники місцевого освітлення). Зазначення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500лк. Якщо ці значення освітленості неможливо забезпечити системою загального освітлення, допускається використовувати місцеве освітлення. При цьому світильники місцевого освітлення слід встановлювати таким чином, щоб не створювати відблисків на поверхні екрана, а освітленість екрана має не перевищувати 300лк. Як джерела світла в разі штучного освітлення мають застосовуватись переважно люмінесцентні лампи типу ЛБ. У разі влаштування відбитого освітлення у приміщеннях, де переважним чином працюють з документами, допускається застосування металогалогенних ламп потужністю

250Вт. Допускається застосування ламп розжарювання у світильниках місцевого освітлення. Система загального освітлення має становити суцільні або переривчасті лінії світильників, розташовані збоку від робочих місць (переважно ліворуч), паралельно лінії зору працюючих.

Допускається використання світильників таких класів світлорозподілу:

– прямого світла — П;
– переважно прямого світла — Н;
– переважно відбитого світла — В.

Для загального освітлення слід застосовувати світильники серії ЛПО 3б із дзеркальними гратами, що укомплектовані високочастотними пускорегулювальними апаратами (ВЧ ПРА). Допускається застосовувати світильники цієї серії без ВЧ ПРА тільки в модифікації «Кососвітло».

При відсутності світильників серії ЛПО36 з ВЧ ПРА і без ВЧ ПРА модифікації «Кососвітло» допускається застосування світильників загального освітлення серії:

– ЛПО13 — 2×40/Б — 01;
– ЛПО13 — 4×40/Б — 01;
– ЛПО13 — 2×40 — 06;
– ЛПО13 — 2×65 — 06;
– ЛСО05 — 2×40 — 001;
– ЛСО05 — 2×40 — 003;
– ЛСО04 — 2×36 — 008;
– ЛПО34 — 4×36 — 002;
– ЛПО34 — 4×58 — 002;
– ЛПО31 — 2×31 — 002,

а також їх вітчизняні та зарубіжні аналогів.

Застосування світильників без розсіювачів та екрануючих грат заборонено. Яскравість світильників загального освітлення в зоні кутів випромінювання від 50 до 90 градусів з вертикаллю в повздовжній та

поперечній площинах має становити не більше ніж 200 кд/м2, захисний кут світильників — не менше ніж 40 градусів. Світильники місцевого освітлення повинні мати відбивач, що просвічує, із захисним кутом, не меншим ніж 40 градусів.

Слід передбачити обмеження прямої блискості від джерел природного та штучного освітлення. При цьому яскравість світлих поверхонь (вікна, джерела штучного освітлення), що розташовані в полі зору повинна бути не більше ніж 200 кд/м2. Необхідно обмежувати відбиту блискість на робочих поверхнях відносно джерел природного і штучного освітлення. При цьому яскравість відблисків на екрані ВДТ має не перевищувати 40 кд/м2, а яскравість стелі в разі застосування системи відбитого освітлення – 200 кд/м2.

Показник осліпленості у разі використання джерел загального штучного освітлення у виробничих приміщеннях має не перевищувати 20, а показник дискомфорту в адміністративно-громадських приміщеннях має бути не більше за 40. Необхідно обмежувати нерівномірність розподілу яскравості в полі зору працюючих з ВДТ. При цьому співвідношення яскравостей робочих поверхонь має бути не більшим ніж 3:1, а співвідношення яскравостей робочих поверхонь та поверхонь стін, обладнання тощо — 5:1. Коефіцієнт запасу для освітлювальних установок загального освітлення має дорівнювати 1,4. Коефіцієнт пульсації має не перевищувати 5%, що забезпечується застосуванням газорозрядних ламп у світильниках загального та місцевого освітлення з ВЧ ПРА для світильників будь-яких типів. Якщо не має світильників з ВЧ ПРА, то лампи багатолампових світильників або світильники загального освітлення, розташовані поруч, слід вмикати на різні фази трьохфазної мережі. Для забезпечення нормованих значень освітленості у приміщеннях з ВДТ ЕОМ та ПЕОМ слід чистити шибки і світильники принаймні двічі на рік і вчасно замінювати лампи, що перегоріли.

Режими праці та відпочинку

При організації праці, що пов’язана з використанням персональних комп’ютерів, для збереження здоров’я працюючих, запобігання професійним захворювання і підтримки працездатності слід передбачити внутрішньозмінні регламентовані перерви для відпочинку. Внутрішньозмінні режими праці і відпочинку мають передбачати додаткові нетривалі перерви в періоди, що передують появі об’єктивних і суб’єктивних ознак стомлення і зниження працездатності. За основну роботу з персональним комп’ютером слід вважати таку, що займає не менше 50% часу впродовж робочої зміни. Протягом дня мають передбачатися:

– перерви для відпочинку і вживання їжі (обідні перерви);

– перерви для відпочинку і особистих потреб (згідно з трудовими нормами);

– додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

Тривалість обідньої перерви визначається чинним законодавством про працю і Правилами внутрішнього трудового розпорядку.

Встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

– для розробників програм слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи за персональним комп’ютером;

– для операторів персональних комп’ютерів слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години;

– для операторів комп’ютерного набора слід призначати регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи за персональним комп’ютером.

У всіх випадках, коли виробничі обставини не дозволяють застосувати регламентовані перерви, тривалість безперервної роботи з персональним комп'ютером не повинна перевищувати 4 години. При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин.

З метою зменшення негативного впливу монотонності є доцільним застосовувати чергування операцій усвідомленого тексту і числових даних (зміна змісту роботи), чередування вводу даних та редагування текстів. Для зниження нервово-емоційного напруження, стомлення зорового аналізатору, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільні деякі перерви використовувати для виконання комплексу вправ. В окремих випадках – при хронічних скаргах працюючих на зорове стомлення, незважаючи на дотримання санітарно-гігієнічних вимог до режимів праці і відпочинку, а також застосування засобів локального захисту очей – допускаються індивідуальних підхід до обмеження часу робіт з персональним комп'ютером, зміни характеру праці, чергування з іншими видами діяльності, не пов'язаними з персональним комп'ютером. Активний відпочинок має полягати у виконанні комплексу гімнастичних вправ, спрямованих на зняття нервового напруження, м'язове розслаблення, відновлення функцій фізіологічних систем, що порушуються протягом трудового процесу, зняття втоми очей, поліпшення мозкового кровообігу і працездатності. За умови високого рівня напруженості робіт з персональним комп'ютером показане психологічне розвантаження у спеціально обладнаних приміщеннях (в кімнатах психологічного розвантаження) під час регламентованих перерв або в кінці робочого дня.

Таким чином, нами детально було розглянуто вимоги, які пред'являє чинне законодавство України до охорони праці офісних співробітників. На

сьогоднішній день ми спостерігаємо прикру тенденцію, коли в більшості офісів такі вимоги не виконуються, а інколи взагалі ігноруються. Це ми можемо неозброєним оком побачити, зокрема, на прикладі вимог до площі офісного приміщення. Чи багато існує офісів, в яких на один персональний комп'ютер припадає не менше ніж шість метрів квадратних? Інколи на такій площі розташовують по три робочих місця з персональними комп'ютерами. Часом приміщення офісів розташовуються в підвалах та/або взагалі не мають природного освітлення. Чи часто ми бачимо робочі місця обладнані підставками для ніг? На жаль, таких прикладів досить багато.

Проте, недобросовісним роботодавцям не варто забувати про відповідальність, яка встановлена чинним законодавством України за порушення вимог щодо охорони праці. У відповідності до ст. 43 Закону України «Про охорону праці» за порушення законодавства про охорону праці юридичні та фізичні особи, які відповідно до законодавства використовують найману працю, притягаються органами виконавчої влади з нагляду за охороною праці до сплати штрафу в порядку, встановленому законом. Сплата штрафу не звільняє юридичну або фізичну особу, яка відповідно до законодавства використовує найману працю, від усунення виявлених порушень у визначені строки. Максимальний розмір штрафу не може перевищувати п'яти відсотків середньомісячного фонду заробітної плати за попередній рік юридичної чи фізичної особи, яка відповідно до законодавства використовує найману працю. Відповідно до ч. 2 ст. 41 Кодексу України про адміністративні правопорушення порушення вимог законодавчих та інших нормативних актів про охорону праці тягне за собою накладення штрафу на працівників від чотирьох до десяти неоподатковуваних мінімумів доходів громадян і на посадових осіб підприємств, установ, організацій незалежно від форм власності та громадян – суб'єктів підприємницької діяльності від двадцяти до сорока неоподатковуваних мінімумів доходів громадян. Порушення вимог законодавчих та інших нормативно-правових актів про

охорону праці службовою особою підприємства, установи, організації або громадянином – суб'єктом підприємницької діяльності, якщо це порушення заподіяло шкоду здоров'ю потерпілого, карається штрафом від ста до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк (ст. 271 Кримінального кодексу України). Те саме діяння, якщо воно спричинило загибель людей або інші тяжкі наслідки, карається виправними роботами на строк до двох років або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до семи років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого.

Безпека в **надзвичайних** ситуаціях

Функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуації мирного та воєнного часу

Моніторинг довкілля – це система спостереження, збирання та аналізу інформації про ситуацію, що може скластись під час надзвичайних ситуацій мирного та воєнного часу. Також це система спостереження за визначеними об'єктами, явищами та процесами з метою оперативного оцінювання їх стану, виявлення результатів впливу на них зовнішніх чинників та прийняття відповідних управлінських рішень (ДСТУ 3891:2013) (див. ДСТУ 7295:2013).

Моніторинг потенційно небезпечних об'єктів це спостереження, контролювання за зміною параметрів технологічних режимів з метою збирання, збереження, передавання та аналізування інформації щодо поточного стану потенційно небезпечних об'єктів, наявності та кількості порушень вимог безпеки, відпрацювання рекомендацій щодо проведення

робіт із запобігання та ліквідування техногенних надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг джерел надзвичайних ситуацій це система спостереження за об’єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації стосовно стану об’єктів моніторингу та розроблення науково-обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування надзвичайних ситуацій (ДСТУ 7295:2013).

Моніторинг довкілля це систематичні спостереження і контролювання, які проводять регулярно, за єдиною програмою для оцінювання стану довкілля, аналізування процесів, які відбуваються в ньому і своєчасне виявлення тенденцій його змінювання (ДСТУ 7295:2013).

Моніторинг надзвичайних ситуацій (НС) – система спостереження за об’єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації щодо об’єктів моніторингу та розроблення науково обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування НС.

Моніторинг небезпечних явищ та процесів це система спостереження та контролювання за розвитком небезпечних та стихійних природних явищ і процесів, чинниками, які спричинюють їх формування та розвиток, аналізування, збереження та передавання інформації щодо виявлення тенденцій їх змінювання, розроблення комплексу заходів щодо запобігання природним надзвичайним ситуаціям та ліквідування їх наслідків. Небезпечні природні явища і процеси підрозділяють на геофізичні, геологічні, гідрологічні, метеорологічні, медико-біологічні та пожежі в природних екосистемах (ДСТУ 7295:2013).

Моніторинг пожеж в екосистемах це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо

пожежної небезпеки в природних екосистемах (умов погоди, стану горючих матеріалів, інших пожежонебезпечних чинників), з метою своєчасного планування та здійснення заходів щодо запобігання виникненню і ліквідування пожеж та їх наслідків (ДСТУ 7295:2013).

Моніторинг радіаційної безпеки це спостереження і контролювання рівня радіоактивного забруднення місцевості, повітря, води, продовольства, об'єктів господарювання, дозових навантажень на населення з метою прийняття оперативних рішень щодо запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг хімічної небезпеки це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо визначення ступеня і характеру хімічного забруднення довкілля, санітарно-гігієнічний нагляд за дотриманням установлених нормативів з метою виявлення джерела надходження небезпечних хімічних речовин, запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013)

Збір та аналіз інформації про стан довкілля під час мирного та воєнного стану дає можливість приймати оперативні рішння для адекватного реагування на ситуацію.

ЕМІ-обстановка та її вплив на стійкість автоматизованих комп'ютерних систем в умовах не воєнного часу

Відомо, що електромагнітне випромінювання (ЕМВ) комп'ютерів, іншої побутової електроніки, стільникових телефонів згубно для здоров'я людини. Багато наївно вважають, що для ослаблення шкідливого впливу потрібно будь-якими способами знизити інтенсивність ЕМІ. Дійсно, якщо знизити інтенсивність потужного ЕМІ, його шкідливість знижується, але інтенсивність ЕМІ комп'ютерів, стільникових телефонів тепер мала. Дослідження вчених інституту біофізики клітини показують, що надзвичайно

слабкі ЕМІ, ледь уловлювані фізичними приладами, можуть надавати на біологічні об’єкти набагато більш сильний вплив, ніж потужні ЕМІ. Захисні екрани побутової електроніки не знижують, а часто підвищують згубність ЕМІ.

Поля, що створюються електромагнітними полями через короткочасне існування називають електромагнітним імпульсом (ЕМІ). Основною причиною виникнення ЕМІ тривалістю до 1 с вважають взаємодію гамма-променів і нейтронів з атомами газів повітря, внаслідок чого з них вибиваються електрони і хаотично розлітаються в середовищі позитивно заряджених атомів газів. Важливе значення має також виникнення асиметрії в розподілі просторових електричних зарядів, пов’язаних з особливостями поширення гамма-променів і утворення електронів.

Вражаюча дія ЕМІ обумовлена виникненням напруги і струмів у провідниках різної довжини, розміщених у повітрі, землі. ЕМІ захвачують спектр частот від десятків до кількох сотень мегагерц, тобто діапазон, в якому працюють установки електропостачання, зв’язку і радіолокації. В момент приходу ЕМІ чутливе електронне обладнання одержує дуже велике перевантаження, внаслідок якого перегоряє. Особливо чутливими до впливу ЕМІ є 6 основних груп об’єктів і систем:

– системи передачі електроенергії: повітряні лінії електропередач, кабельні лінії, різні види з’єднувальних ліній і повітряна електропроводка;

– системи виробництва, перетворення і накопичення енергії: електростанції, генератори постійного і змінного струму, трансформатори, перетворювачі струмів і напруг, комутатори і розподільні пристрої, електричні бата- 66 реї і акумулятори, паливні, сонячні й термоелементи;

– системи регулювання і управління: електромеханічні, електронні датчики та ін. елементи автоматики, комп’ютерні установки, мікропроцесори;

– системи споживання електроенергії: електродвигуни і електромагнітні, нагрівальні, холодильні, венти- ляційні, освітлювальні установки, кондиціонери;

– системи електротяги: електроприводи, напівпровідникові та ін. типи перетворювачів;

– системи радіозв’язку, передачі, зберігання і накопичення інформації: антени, хвилеводи, коаксіальні кабелі, електронні прилади, радіопередавачі, радіоприймачі, установки автономного електропостачання, змішувачі, телефонні апарати, телеграфні установки, заземлені кабелі й проводи, АТС.

Висновки до п’ятого розділу

В даному розділі дипломної роботи розглянуто питання освітлення робочого місця та режимів праці і відпочинку. В безпеці в надзвичайних ситуаціях висвітлено питання функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного часу; ЕМІ-обстановка та її вплив на стійкість автоматизованих комп’ютерних систем в умовах не воєнного часу.

ЕКОЛОГІЯ

Вимоги до моніторів (ВДТ) і ПЕОМ

Відеодисплейний термінал (ВДТ) є пристроєм, що використовується для візуалізації інформації, яка знаходиться в електронній формі. ВДТ уможливлює швидке введення алфавітно-цифрової або графічної інформації. Основними його елементами є: екран, забезпечений пристроєм опрацювання виведеної інформації, засобів управління і введення даних. Робота ВДТ може відбуватись через підключення до інших пристроїв (наприклад, до комп'ютерів) або автономно.

Розглядаючи питання впливу на здоров’я користувачів ВДТ можна поділити за апаратниим особливостями і характеристиками самого пристрою (наприклад, виведення багато-кольорового, позитивного або негативного зображення, розміри і т.д.). Картинка на ВДТ показується використовуючи електронно-променеві трубоки (ЕПТ) і тому такі засоби відображення подібні з екранами телебачення. Іншими варіантами ВДТ є плазмові і рідкокристалічні.

Принцип роботи рідкокристалічних дисплеїв полягає заломленні світла в рідких кристалах, де електричне поле формує рефракційні властивості. Характерною властивістю є те, що такі екрани не випромінюють світло і потребують зовнішнього освітлення. Це створює додаткові вимоги до характеристик освітлення приміщення.

Роздільна здатність монітора визначає чіткість і різкість зображення, що залежить від числа дискретних елементів зображення (пікселів), які монітор може відтворити по горизонталі і вертикалі. Збільшення роздільної здатності підвищує точність та чіткість зображення на екрані і тим самим полегшує сприйняття інформації та зменшує зорову втому.

Стандартні значення роздільної здатності постійно вдосконалюються з впровадженням нових моніторів та технологій: “640x480 (VGA); 800x600 (SVGA); 1024x768 (XGA); 1280x1024 (EVGA); 1600x1200”.

Крок люмінофора визначає чіткість зображення (dot pitch), що є відстанню між дискретними точками люмінофора одного кольору зсередини поверхні екрану. Апертурна гратка – це віддаль між полосами одного кольору, а тіньова маска є лінія мінімальної відстані між крапками одного кольору і утворює з горизонталлю кут 30º. У залежності від моделі моніторів крок люмінофора знаходиться в межах від 0,25 до 0,41 мм. При роботі з високоточною графікою з заданою роздільною здатністю вище 1024x768 крок може становити від 0,25 до 0,26 мм. При офісному чи домашньому використанні для більшості прикладних додатків, що використовують роздільну здатність 1024x768 або нижче, достатній крок 0,27 або 0,28 мм.

Важливою характеристикою роботи монітора є частота оновлення картинки, або по іншому частота зміни кадрів (або частота вертикальної розгортки). При високій частоті зображення видається незмінним при тому, що фактична яскравість для будь-якої точки зображення змінюється. Інерційність зору людини і інерційність монітора створюють ефект стабільного зображення.

Типо люмінофора визначає інерційність монітора. Максимальна яскравість будь-якої точки на екрані може бути тільки в один момент за період зміни кадру. На основі експоненціального закону яскравість свічення плавно спадає до мінімального значення. При великій інерційності люмінофорів післясвічення продовжується довше, ніж у люмінофорів з малою інерційністю.

Максимальна частота, коли починає сприйматись незмінність зображення є неоднаковою для різних людей при одних і тих самих умовах. Використовуючи цей параметр розраховують частоту зміни кадрів таким чином, що вона підходила для 95% користувачів. Використовуючи методику

MPR розрахували крайню нижню межу частоти зміни кадрів, яка становить 75Гц для позитивного зображення і 67 Гц – для негативного. Для нових моніторів при роздільній здатності 1024x768 вона може бути 110…120 Гц. При цьому роздільна здатність та частота оновлення кадрів є взаємозв'язаними величинами.

Яскравість свічення монітора є характеристикою яскравості зображення на екрані в заданих умовах освітлення. При збільшенні цього показника, зростає яскравість зображення, що формується монітором з збереженням різкості та контрасту. На яскравість впливає інтенсивність електронного пучка, що має можливість регулюватись при налаштуваннях екрану.

Іншими параметрами, що впливають на якість зображення є апертурна гратка, що разом з тіньовою маскою забезпечують помітне збільшення яскравості.

Суттєвим показником якості монітору є покриття екрану, що зменшує відблиски, оскільки при відблискуванні людина погано сприймає інформацію, змінює положення тіла, перенапружує зір. Загалом такі монітори приводять до швидкого стомлювання всього організму.

При розробці сучасних моніторів велику увагу приділяють елементам, що зменшують віддзеркалення за рахунок спеціальних покриттів екрану. Іншим варіантом є використання спеціальних окулярів, що містять у собі фільтри для зменшення шкідливого впливу випромінювання та світла.

Для зменшення відблисків можна нанести на поверхню монітора шар діелектрика з малим показником заломлення і низьким коефіцієнтом віддзеркалення. Нанесення перехідного шару, коефіцієнт заломлення якого середній між склом і зовнішнім шаром збільшує інтенсивність корисного світла і зменшує статичний заряд.

Регламентування рівнів безпечності випромінювання відбувається на основі норм MPR II 1990:10 Шведського Національного Комітету з вимірювань і випробувань та TCO 92,95 Шведської конференції профспілок.

Монітори, які не відповідають вимогам екологічної безпеки дообладнуються наступними елементами:

1. Для послаблення змінного електричного та статичного полів – захисний фільтр екрану.

2. Для індивідуального використання в один ряд – захисне покриття на передню панель і бічні стінки.

3. При розміщенні таким чином, що сусідні монітори створюють поля, які накладаються – захисне покриття задньої і бічних стінок, монтування спеціальних екрануючих панелей, встановлення переділу між сусідніми користувачами.

Підсумовуючи вище сказане, прилади ВДТ повинні відповідати сучасним стандартам, а у випадку невідповідності – дообладнуватись необхідними елементами захисту.

Дисперсійний аналіз в екології

Всі явища в природі є взаємопов’язаними і тому їх дослідження не може бути виконане виокремлено від інших навколишніх явищ. Зокрема, якщо розглядати результативні ознаки в екології (викиди, скиди т.д.), то вони потрапляють під вплив різноманітних факторів таких як: число підприємств, які забруднюють; об’єми викидів та скидів кожного з них. Як результат міжрегіональна та внутрішньорегіональна диференціація має значний вплив на ці результативні ознаки. Їх змінність можлива навіть в межах одного регіону.

Суть і розвиток явищ розкривається при дослідженні взаємопов’язаності явищ. Для вивчення взаємозв’язків у суспільних явищах

та процесах використовується статистика, яка використовує числові вирази для закономірностей. Залежності між факторними та результативними ознаками отримуються на основі розрахунку ряду статистичних характеристик. Дисперсійний аналіз застосовується для кількісної оцінки взаємозв'язків і їхньої суттєвості за невеликої кількості спостережень.

Головна мета дисперсійного аналізу – використовуючи статистичні методи виявити вплив різних факторів на змінність ознаки, яка розглядається. При роботі з експериментальними даними дисперсійний аналіз, або аналіз розкиду досліджуваних даних, показує себе як найбільш досконалий метод статистичної обробки. Дані, що отримуються за результатами дисперсійного аналізу характеризують розкид, або дисперсію ознак, що потрапляють під вплив дії всіх факторів; часткову або факторну дисперсію, що виникла за рахунок спланованих і підготовлених дослідником факторів; та залишкову дисперсію, яка виникає внаслідок незапланованих та випадкових чинників, які невідомі експериментатору.

Дисперсійний аналіз можна віднести до математично-статистичного методу вивчення результатів спостереження, які потрапляють під залежність від різноманітних одночасно діючих факторів.

Дисперсний аналіз є методом дослідження залежностей між явищами коли число спостережень невелике. Багато важливих завдань вирішується на основі даного методу. Основним завданням цього методу є статистичне виявлення впливу факторів на змінність ознаки, котра потребує вивчення та провести визначення впливу різних факторів окремо і сумарно на змінність ознаки. Важливість дисперсійного аналізу проявляється при вивченні ознак коли їх зміна зумовлена дією багатьох факторів з різною часткою впливу. Основні завдання, що вирішуються даним методом є:

– числове визначення сили впливу факторних ознак та їх поєднань на результативну;

– визначення достовірності впливу та довірчих меж;

– аналіз середніх значень та статистична оцінка їх різниць. Змінність експериментальних даних можна:

– розділяти методом дисперсійного аналізу на складові частини, які відповідають дуже важливим джерелам змінності одержуваних цифр.

Дисперсійний аналіз базується на законі розкладання варіацій, що можна показати як: Оо = Осис + Овип, де (Оо - загальний обсяг варіації; Осис - обсяг варіації, що визваний дією систематичних факторів; Овип – обсяг варіації, що визваний дією випадкових факторів.

Загальна варіація – це сумарна варіація результативної ознаки, зумовлена всіма причинами як систематично діючими, так і випадковими. В нашому прикладі це буде сумарна варіація досліджуваної сукупності.

Систематична варіація – це частина загальної варіації результативної ознаки, яку можна пояснити і яка викликана систематичною дією факторних ознак.

Випадкова варіація – це варіація, яку неможливо пояснити, тобто частина загальної варіації результативної ознаки, викликана дією випадкових факторів. Випадкову варіацію іноді називають залишковою, оскільки вона відбиває варіацію результативної ознаки, викликану усіма іншими факторами, не врахованими в обсязі систематичної варіації. Її завжди можна легко обчислити.

Як наслідок дисперсійний аналіз використовують для оцінок ступенів впливу випадкових факторів, оцінки достовірності взаємодії ніж ними, оцінки достовірності відмінностей між парами середніх значень. Розрахунок достовірності варіації дає змогу з заданим ступенем імовірності визначити, чи варіація викликана системно діючим фактором, чи дією випадкових факторів.

Передумовою застосування дисперсійного аналізу є наявність сукупності, розчленованої за однією або декількома ознаками на певні групи. У результаті при групуванні даних загальна варіація розчленовується на такі

складові частини: Оо = Ом + Ов, де Ом – обсяг міжгрупової варіації; Ов – обсяг внутрішньогрупової (залишкової) варіації.

Отже, міжгрупова варіація є систематичною варіацією і характеризує вплив на результативну ознаку систематичних факторів. Вона являє собою варіацію між групами. Сума квадратів відхилень групових середніх від загального середнього становитиме міжгрупову варіацію.

Внутрішньогрупова варіація є випадковою залишковою варіацією і характеризує дію на результативну ознаку випадкових неврахованих факторів. Вона являє собою варіацію результативної ознаки в середині кожної групи.

Такою є загальна схема розкладання варіації, коли вивчається варіація результативної ознаки під дією одного фактора. Однак, як відомо, варіація результативної ознаки зумовлюється не одним, а багатьма факторами. Схема розкладання варіації при багатофакторному аналізі буде більш складною.

Обсяги варіацій визначаються за допомогою загальної дисперсії (Do) яка має тіж самі властивості розкладання на складові дисперсії згідно закону розкладання дисперсій: Do = Dм + Dв, де Do - загальна дисперсія; Dм – міжгрупова дисперсія; Dв – внутрішньогрупова (залишкова) дисперсія.

Загальна дисперсія складається під впливом безлічі факторів і характеризує варіацію числових значень результативної ознаки, пов'язану з варіацією всіх факторів, що на неї впливають.

Міжгрупова дисперсія характеризує варіацію групових середніх, тобто варіацію результативної ознаки, яка пов'язана з варіацією групувальної ознаки, що обумовлена дією систематичних факторів.

Внутрішньогрупова дисперсія характеризує варіацію ознаки всередині конкретної групи, що обумовлена дією випадкових факторів.

Таким чином, використовуючи метод дисперсійного аналізу, дослідник може оцінити (у відсотках) частку впливу того чи іншого фактора на варіацію вивчаємої ознаки.

До завдань дисперсійного аналізу можна віднести:

– оцінювання сили та ступеня впливу одного або декількох факторів;

– оцінювання сили і ступеня впливу випадкових факторів;

– оцінювання вірогідності взаємодії між ознаками.

Висновки до шостого розділу

В даному розділі розглянуто питання вимог до моніторів ВДТ та ПЕОМ, а також роль дисперсійного аналізу в екології.

ВИСНОВКИ

В дипломній роботі проведено дослідження методів та засобів розробки та впровадження надійної, продуктивної та захищеної мережевої архітектури. За результатами цього отримано наступні результати:

– здійснено дослідження надійних мережевих архітектур, що дало змогу визнати напрямки вдосконалення мережевих дизайнів;

– проаналізовано процес створення мережі;

– виконано аналіз особливостей організації мережевої безпеки та методів захисту мереж;

– здійснено підвищення надійності роботи мережі за рахунок впровадження протоколів аналізу та управління трафіком;

– подано організаційно-технічні методи та засоби забезпечення працездатності мережі;

– запропоновано методи управління ризиками мережевої безпеки та систему управління безпекою;

– подано проект вдосконалених методів та засобів побудови та впровадження надійної, продуктивної та захищеної мережевої архітектури.

В розділі «Спеціальна частина» проведено огляд питання підвищення надійності мереж на основі технології SDN та резервування мережевих ресурсів на базі протоколу HSRP.

В розділі «Обгрунтування економічної ефективності» проведено розрахунок основних техніко-економічних показників доцільності запровадження методів та засобів розробки та впровадження надійної, продуктивної та захищеної мережевої архітектури.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання освітлення робочого місця; режиму праці та відпочинку; функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного

та воєнного часу; ЕМІ-обстановка та її вплив на стійкість автоматизованих комп’ютерних систем в умовах невоєнного часу.

В розділі «Екологія» висвітлено питання вимог до моніторів (ВДТ) і ПЕОМ, а також дисперсійного аналізу в екології.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. E. Knipp et al., Managing Cisco Network Security. Elsevier Inc., 2002, ISBN: 978-1-931836-56-2

2. S. Wilkins and T. Smith, CCNP Security. SECURE 642-637 Official Cert Guide. Cisco Press, 2011, ISBN: 978-1-58714-2802.

3. V. Olifer and N. Olifer, Novye tekhnologii i oborudovanie IP-setei [New technologies and equipment of IP-networks]. St.-Peterburg, Russia: Bhv, 2000, ISBN: 5-8206-0053-3

4. A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/.

5. T. King et al., “BLACKHOLE Community,” Internet Engineering Task Force (IETF), 2016. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7999. – Назва з екрану. – Дата звернення: 4.04.2020.

6. D. S. Ms. Charjan, P. S. Ms. Bochare, and Y. R. Bhuyar, “An Overview of Secure Sockets Layer,” Int. J. Comput. Sci. Appl., vol. 6, no. 2, pp. 388–393, 2013

7. “Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco.” [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nacappliance-cleanaccess/product_data_sheet0900aecd802da1b5.html. – Назва з екрану. – Дата звернення: 14.04.2020

8. M. Kozlova (AKA M. Kozlova, “7 luchshikh servisov zashchity ot DDoS-atak dlya povysheniya bezopasnosti [The 7 best services of protecting from DDoS- attacks for the increase of safety],” HOSTING.cafe, 2017. [Електронний

ресурс]. – Режим доступу: https://habrahabr.ru/company/hosting-cafe/blog/324848/. – Назва з екрану. – Дата звернення: 15.04.2020

9. Приїхав до Польщі – користуйся Інтернетом! [Електронний ресурс] – Режим доступу: http://naszwybir.pl/internet/. – Назва з екрану. – Дата звернення: 15.04.2020

10. V. F. Shangin, Informatsionnaya bezopasnost [Information Security]. Moscow, Russia: DMK Press, 2014.

11. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков – Юніор, 2005. – 397 с.

12. Вишневський В. М. Теоретичні основи проектування комп'ютерних мереж / В. М. Вишневський – Техносфера, 2004. – 512 с.

13. Cisco Systems Руководство по технологиям объединенных сетей / Cisco Systems - 3-е издание. СПб: “Вильямс”, 2002. – 1040 с.

14. Дебра Литтлджон Шиндер Основы компьютерных сетей / Дебра Литтлджон Шиндер - СПб: "Вильямс", 2002. – 656 с.

15. Коротыгин С. Стандарт IEEE 802.11 и его расширения / С. Коротыгин, А. Нежуренко - Сети и телекоммуникации, вып. 6(25), 2002 г.

16. Марк А. Спортак Компьютерные сети. Книга 1. High-Perfomance Networking. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

17. Марк А. Спортак Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

18. Беркман Л. Н. Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі / Л. Н. Беркман, С. В. Толюпа // Зб. наук. праць ВІТІ НТУУ ―КПІ‖. – 2007. – №3. – С. 9-17.

19. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

20. Беркман Л. Н. Проблеми створення сучасної конвергентної мережі на базі концепції FMC (Fixed-Mobile Convergence) / Л. Н. Беркман, О. І. Чумак, В. В. Григорович, П. Ю. Дещинський // Вісник УНДІЗ. – 2008. – №2. – С. 61-63.

21. Толюпа С. В. Структура інформаційної мережі та показники її ефективності / С. В. Толюпа, А. В. Сухін. // Зб. наук. праць КВІУЗ. – 2001. – №3. – С. 68-73.

22. Мурай А. В. Оценка качества телекоммуникационных услуг с учетом степени удовлетворения ожиданий и требований пользователей / А. В. Мурай // Наукові записки УНДІЗ. – 2013. – № 2(26). – С. 68-75.

23. Гребенніков В. О. Проблема загальнодоступності основних телекомунікаційних і інформаційних послуг в Україні та загальні підходи до її розв'язання / В. О. Гребенніков, Г. Ф. Колченко // Наукові записки УНДІЗ. – 2013. № 1(25). – С. 5-13.

24. Фрзнк Г. Сети, связь и потоки / Г. Фрзнк, И. Фриш ; пер. с англ. под ред. Д. А. Поспелова. – Москва : Связь, 1978. – 448 с.

25. Колченко Г. Ф. Розроблення нормативних документів для забезпечення функціонування системи оперативно-технічного управління телекомунікаційними мережами / Г. Ф. Колченко, І. В. Шестак // Наукові записки УНДІЗ. – 2012. – № 2(24). – С. 5-8.

26. Система управління сучасними телекомунікаційними мережами : монографія : у 2 ч. / [Кривуца В. Г., Беркман Л. Н., Климаш М. М. та ін.]. – Київ : ДУІКТ, 2009. – 268 с.

27. Шерстнева О. Г. Подходы к оценке качества управления связью / О. Г. Шестернева // Сети и системи связи. – 2008. – №11. – С. 35-41.

28. Стеклов В. К. Проектування телекомунікаційних мереж / В. К. Стеклов, Л. Н. Беркман. ; під ред. В. К. Стеклова – Київ : Техніка, 2002. – 792 с.

29. Кульгин М. Технология корпоративных сетей / М. Кульгин. – Санкт- Петербург : Питер, 1999. – 704 с.

30. Шварц М. Сети связи: протоколы, моделирование и анализ / М. Шварц. – ч.2. – Москва : Наука, 1992. – 272 с.

ДОДАТКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Національна академія наук України
Університет імені П'єра і Марії Кюрі (Франція)
Маріборский університет (Словения)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Шяуляйська державна колегія (Литва)
Жешувський політехнічний університет ім. Лукасевича (Польща)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Національний університет біоресурсів і природокористування України (Україна)
Наукове товариство ім. Шевченка
ГО «Асоціація випускників Тернопільського національного технічного університету імені Івана Пулюя»

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том II

VIII Міжнародної науково-технічної конференції молодих учених та студентів

27-28 листопада 2019 року

УКРАЇНА
ТЕРНОПІЛЬ – 2019

УДК 004.72
В.В. Панчук, В. В. Думітрак, А.О. Дубчак
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ МАРШРУТИЗАЦІЇ В МЕРЕЖАХ РІЗНОЇ ГЕТЕРОГЕННОЇ СТРУКТУРИ ДЛЯ ОДНІЄЇ АВТОНОМНОЇ СИСТЕМИ

V.V. Panchuk, V. V. Dumitrak, A.O. Dubchak

ROUTING INVESTIGATION IN THE NETWORKS OF DIFFERENT HETEROGENIC STRUCTURES FOR ONE AUTONOMOUS SYSTEM

Створення та побудова сучасних комунікаційних мереж вимагає розгляду цілого ряду питань пов'язаних з організацією каналів, управлінням потоками даних, забезпечення якості сервісів та захищеності обміну даними. Фізична інфраструктура мережі в основному залежить від технічного розвитку існуючих технологій виготовлення компонентів, в той час як налаштування маршрутизації опирається на вимоги до роботи мережі та зв'язана з теперішніми архітектурними рішеннями. При аналізі та створенні вимог до маршрутизації в мережах різної гетерогенної структури необхідно дослідити ряд факторів пов'язаних з наступними областями роботи:

- розмір та складність мережі;
- необхідність забезпечення якості сервісів;
- складність впровадження різних протоколів.

Аналізуючи першу складову можна визначити де статична маршрутизація буде мати місце, а де протоколи динамічної маршрутизації будуть використовуватись. У випадку використання протоколів динамічної маршрутизації необхідно провести аналіз підтримки версійності та сумісності їх роботи при використанні обладнання від різних виробників.

Якість сервісів в більшості сучасних мереж є необхідною для впровадження складовою, яка повинна забезпечувати належну роботу сервісів, що потребують особливих умов обслуговування. При розробці та впровадженні рішень щодо маршрутизації необхідно провести дослідження впливу затримок викликаних алгоритмами роботи динамічної маршрутизації при прийнятті рішень з побудови та зміни маршрутів.

Наступна складова визначає необхідність впровадження віртуалізації мережевих ресурсів або побудови програмно конфігурованих мереж. Даний підхід є найбільш популярним в сучасних мережах але пов'язаний з певними труднощами як розгортання так і обслуговування. Суттєво зростають вимоги до кваліфікації обслуговуючого персоналу, що в свою чергу піднімає вартість таких проектів.

Проведений аналіз дає змогу підсумувати, що сучасні мережі різної гетерогенної структури можуть містити вище згадані компоненти як складові однієї системи так і бути організовані модульно, коли певні частини мережі мають спрощені налаштування для здешевлення, а ключові повноцінно організовані. Програмно конфігуровані мережі дають найбільшу гнучкість управління, оскільки мають змогу реалізації різних сценаріїв в залежності не тільки від фізичної інфраструктури, а й на основі аналізу поведінки мережі при заданих параметрах та в реальному часі. Незважаючи на певні складноші їх розгортання, переваги, що надаються такими рішеннями, уможливлюють здійснення сценаріїв, які при класичному підході реалізувати важко або й неможливо.

Література

1. Смелянский Р. В. Программно-конфигурируемые сети [Електронний ресурс] / Р. В. Смелянский // Открытые системы. – 2012. – № 9. – Режим доступу: http://www.osp.ru/os/2012/09/13032491 (20.11.2019 р.).