МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук,
управління та адміністрування
Кафедра інформаційних технологій

Кваліфікаційна робота бакалавра

на тему: Розробка аналітичної та математичної моделі систем DPI

Виконав студент групи К18
спеціальності 122 Комп'ютерні науки
Жумаєв Атахан

Керівник д.т.н., професор
Казакова Надія Феліксівна

Консультант

Рецензент Копиченко І.Ю.,
регіональний координатор
програми EGAP

Одеса 2022

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АСУ – автоматизована система управління;
ЕОМ – електронно-обчислювальна машина;
ІС − інформаційна система
ІТ − інформаційні технології
КЗЗ – комплекс засобів захисту;
НСД – несанкціонований доступ;
ОС – обчислювальна система;
ПЕОМ – персональна електронно-обчислювальна машина;
ПЗ – програмне забезпечення;
OSI – Open Systems Interconnection;
VPN – Virtual Private Network;
SSH – Secure Shell;
CGI – Common Gateway Interface;
QoS – Quality of service;
DCOM – Distributed Component Object Model.

ВСТУП

Кількість організацій, які застосовують веб-технології для підвищен-ня продуктивності роботи і залучення нових клієнтів, зростає з кожним роком. До таких організацій належать, як комерційні компанії різних форм власності, так і органи державної влади і місцевого самоуправління. Без-сумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберза-гроз. Так, компанія Symantec в своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зломі веб-сайтів зазвичай ви-користовують вразливості веб-додатків, що працюють на сервері, або екс-плуатують деякі вразливості операційної системи, на якій працюють ці до-датки. Наприклад, за допомогою атак типу XSS хакер може перенаправи-ти запити користувачів на шкідливі веб-сторінки, а за допомогою SQL-ін'єкцій – витягувати з баз даних сайту різну конфіденційну інформацію. У відповідь на масові зломи систем безпеки був створений консорціум OWASP – Open Web Application Security Project, це відкритий проект за-безпечення безпеки веб-додатків. Однак і зловмисники, і фахівці в області кібербезпеки продовжують знаходити вразливості в веб-додатках, які мо-жуть привести до серйозних втрат з боку бізнесу. Основною причиною більшості взломів в веб-додатках є написаний розробниками програмний код. Розробники можуть допускати помилки при написанні коду або не усвідомлювати всю важливість використання прийомів безпечного про-грамування – все це призводить до появи вразливостей в додатках. Розповсюдження контрафактних матеріалів, забороненого контенту, покривання злочинних угруповань, незаконні дії з електронними платежами, – це накладає негативний відбиток на всі анонімні мережі. Тому злам таких мереж часто стає метою спецслужб й інших органів охорони правопорядку. [1]

Найефективнішою системою аналізу мережевого трафіку являється DEEP PACKET INSPECTION, яка позволяє на найвищих рівнях моделі OSI

працювати з даними, для блокування заборонених ресурсів або, навпаки, для захисту систем. В дипломній роботі розглянуті питання анонімності в мережі Інтернет, обладнання для систем DPI, питання безпеки в АСУ і SCADA-системах, моделі DPI та техніки обходу.

В більшості випадків для забезпечення певного ступеня анонімності в глобальній мережі застосовують безкоштовне й загальнодоступне програмне забезпечення і віртуальні мережі. Однак чим вища захищеність використовуваної технології, тим нижчі швидкісні показники обміну даними і доступність для розуміння принципів її роботи і застосування.

Хоча систему DPI можливо обійти, але важливо усвідомити, що анонімність впирається в засоби: матеріальні ресурси і час, які можуть бути затрачені на їх компрометацію, тому краще дану технологію розглядати зі сторони захисту мережевого трафіку.

1 АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В МЕРЕЖІ ІНТЕРНЕТ

1.1 Огляд найпоширеніших атак на WEB-ресурси

Види атак на WEB сервіси та способи їх протидії наведені в таблиці 1.1. Найбільш популярною атакою є «Insufficient transport layer protection» — отримання даних під час передавання. Дана атака може бути виконана для 70 % ресурсів. Для виключення можливості проведення таких атак достатньо використовувати протокол HTTPS.

Витік інформації («Information leakage»). Дану атаку можна виконати на 56 % ресурсів. Витік інформації з додатків виникає в результаті відмови або неправильної роботи програми, а також у разі порушення її логіки. Для виключення можливості проведення атаки необхідно ретельно тестувати програмну частину ресурсу, проводити перевірку повідомлень на стороні сервера, моніторинг оповіщень про помилки.

Таблиця 1.1 – Види WEB атак та способи їх протидії

№ за/п	Вид атаки	Вразливість веб-ресурсів, %	Протидія
1	Insufficient transport layer protection	70 %	Використання протоколу HTTPS.
2	Information leakage	56 %	Тестування програмної частини ресурсу, перевірка повідомлень на стороні сервера, моніторинг оповіщень про помилки
3	Cross-site scripting	47 %	Очищення та валідація вхідних даних
4	Brute force	29 %	Використання паролів високої складності, налаштування сервера на аналіз вхідних запитів

№ за/п	Вид атаки	Вразливість веб-ресурсів, %	Протидія
5	Content spoofing	26 %	Відмовитися від використання фреймів і не передавати в параметрах абсолютні або локальні шляхи до файлів
6	Cross-site request forgery	24 %	Перевірка вхідних даних з форм
7	URL redirector abuse	16 %	Валідація вхідних даних
8	Predictable resource location	15 %	Контроль доступу до файлів сервера

Атаку «Cross-site scripting» — міжсайтове використання сценаріїв, можливо виконати на 47 % ресурсів. Атака дозволяє передати JavaScript-код на виконання в браузер користувача. Атаки такого роду часто також називають HTML-ін'єкціями, адже механізм їхнього впровадження дуже схожий із SQL-ін'єкціями, але на відміну від останніх, впроваджуваний код виконується в браузері користувача. Для захисту від цього виду атак необхідно проводити очищення та валідацію вхідних даних.

Генерацію великої кількості запитів, або підбір паролів («Brute force») можливо виконати на 29 % ресурсів. Для захисту необхідно забезпечити використання паролів високої складності, налаштування сервера на аналіз вхідних запитів.

Атака «Content spoofing» — підмінна даних через заміну контенту сторінок можлива для 26 % ресурсів. Використовуючи цю техніку, зловмисник змушує користувача повірити, що сторінка згенерована веб-сервером, а не передана із зовнішнього джерела. Для захисту від даного виду атак потрібно відмовитися від використання фреймів і, найголовніше, ніколи не передавати в параметрах абсолютні або локальні шляхи до файлів.

Вид атак на відвідувачів веб-сайтів, який використовує недоліки протоколу HTTP — «Cross-site request forgery». Якщо жертва заходить на сайт,

створений зловмисником, браузер таємно відправляється запит на інший сервер (наприклад, на сервер платіжної системи), який здійснює якусь шкідливу операцію (наприклад, переказ грошей на рахунок зловмисника). Дану атаку можливо виконати на 24 % ресурсів. Для захисту необхідно проводити перевірку вхідних даних з форм, наприклад шляхом додавання унікального прихованого поля.

Перенаправления на інші сайти через підміну початкових посилань («URL redirector abuse»). Цей вид вразливостей, також як і багато інших перерахованих вище, є різновидом помилок перевірки вхідних даних і можлива на 16 % ресурсів. Вирішенням є валідація вхідних даних.

Ще однією популярною атакою є «Predictable resource location» — знаходження прихованого функціоналу та даних. Доступна на 15 % ресурсів і вирішується шляхом контролю доступу до файлів сервера.

Починаючи з 2010 року: більша частина атак використовує: SQL-ін‘єкції – 17.9%, XSS – 13.7%, DDoS – 6.2%, розкриття інформації – 4.6%, передбачуваність інформаційного ресурсу – 4.4%, Brute force – 3.9%, вгадування сесій – 3.2%. Інші – CSRF, фішинг, шкідливе ПЗ, викрадення DNS, викрадення облікових записів і т. д. З кожним роком статистика атак змінюється, так у 2014 році найпопулярнішою була атака «Cross-site scripting», а в 2013 — Витік інформації («Information leakage»).

На лютий 2021 р. лідируючим стало викрадання даних (12%), а ін‘єкції досягли аж 10,7%. Збільшилась кількість спрямованих атак (9,3%) і шкідливе програмне забезпечення (6,7%). Атаки типу DDoS значно менше використовуються, як і спотворення веб-сайтів (4%). На березень 2021 р. викрадання даних стало номером один серед відомих векторів атак з 20,7% (було 12%). Ін‘єкції продовжують лідирувати з 9,8% (у лютому було 10,7%), такий же відсоток спрямованих атак (було 9,3%). DDoS трохи більше використовувалось (7,6%), поширення шкідливого ПЗ через рекламу (5,4%). Спотворення сайтів та шкідливе ПЗ 3,3%.

Виходячи з наведених даних, можна зробити висновки про те, що для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів (Framework), в якому вбудовані механізми перевірки, шифрування та валідації. Найкращим методом захисту від атак на мережеві служби, наприклад, DoS та DDoS є використання хмарних технологій і перевірених конфігурацій серверів.

Як свідчать статистичні результати [33] та запропоновані методи, які орієнтовані на захист від конкретного типу атаки, зловмисна дія на веб-ресурс відбувається, як правило, із використанням відразу декількох різних типів атак. Тому задачею системи менеджменту інформаційної безпеки є розробка ефективної стратегії протидії атакам зловмисників за умови, що вони використовують комбіновані типи атак. Рівень ефективності при цьому визначається замовником веб-ресурсу і задається він специфікою ведення бізнесу підприємством (чи діяльністю організації), параметрами, що характеризують специфіку інформації та баз даних, які належать до конфіденційних і рядом інших параметрів і характеристик. Розробка такої стратегії захисту веб-ресурсу є нетривіальною задачею.

Анонімність в мережі доцільно розглядати з таких точок зору:

1) Соціальна анонімність те, що користувач цілеспрямовано чи несвідомо повідомляє про себе в соціальних мережах, тематичних форумах, спеціалізованих інформаційно-пошукових системах;

2) Технічна анонімність – ті деанонімізуючі дані, які пов’язані з особливостями використання технічних засобів, протоколів роботи та обміну повідомленнями інформаційних систем, програмного забезпечення.

Розглянемо лише технічну анонімність, без висвітлення організаційних, соціальних чи юридичних аспектів та труднощів на шляху розкриття анонімності. [2]

1.2 Централізовані засоби забезпечення анонімності

В архітектурі централізованих засобів обов'язковим компонентом є один або декілька центральних вузлів, що здійснюють перенаправлення мережного трафіку, приховування реальних адресів і реквізитів користувача, координацію всієї множини вузлів. Ці засоби вирізняються високою швидкістю роботи, однак наділені невисокою надійністю. До них, зокрема, відносять: http-проксі-сервери, SOCKS-проксі-сервери, VPN-сервіси, SSH-тунелі.[3], [4]

В більшості випадків під проксі-сервером розуміють віддалений комп'ютер і комплекс програм на цьому комп'ютері, що виступає посередником між клієнтом і адресатом для забезпечення обміну повідомленнями між ними.

У контексті забезпечення анонімності виділяють такі проксі-сервери [5]):

- http-проксі-сервери: пропускають через себе лише http-трафік, додаючи інформацію про застосування проксі;
- SOCKS-проксі-сервери, реалізований на сеансовому рівні OSI: передають всю інформацію без додавання інших даних;
- CGI-проксі або «анонімайзер»: пропонує форму для введення необхідної адреси сайту, може застосовувати протокол https для захисту каналу зв'язку до клієнта.

Переваги:

- послуга дешева, доступні безкоштовні проксі-сервери.

Недоліки:

- необхідно довіряти проксі-сервери;
- необхідність налаштування проксі-сервера;
- протоколи проксі не підтримують шифрування між HTTP/SOCKS/Elite/Anonymous-проксі і клієнтом;

– для http-проксі необхідно фільтрувати http-заголовки.

VPN-з’єднання – технологія емуляції з’єднання «точка-точка» через мережу загального призначення, при цьому між клієнтським комп’ютером і провайдером створюється так званий тунель [6]. Віртуальні приватні мережі часто застосовують для створення безпечних і надійних каналів, що поєднують локальні мережі та забезпечують доступ до них користувачам, які постійно змінюють своє місцезнаходження. Канали VPN захищені алгоритмами шифрування, закладеними в стандарти протоколу безпеки IPSec, який забезпечує захист на мережному рівні.

Часто технологію VPN реалізують через SSH – мережний протокол прикладного рівня, через який можна здійснювати віддалене управління операційною системою й тунелювання TCP-з’єднань [7]. Весь трафік і паролі при цьому зашифровуються за допомогою алгоритмів, доступних для вибору. SSH дає змогу безпечно передавати по незахищеному середовищу практично будь-який інший мережний протокол.

У контексті анонімності, без врахування деяких відмінностей, основний принцип функціонування VPN і SSH однаковий.

Переваги:

– не потрібно додатково налаштовувати програмне забезпечення.

Недоліки:

– необхідно довіряти VPN/SSH-серверу/провайдеру.

Більшість додатків для браузерів і «програм для анонімності» ґрунтуються на роботі проксі-серверів та VPN-серверів з метою приховування IP-адреси користувача.

1.3 Схеми анонімності TOR та I2P

Децентралізація – відсутність єдиного центру контролю та єдиної точки відмови в обслуговувані. Децентралізовані мережі поділяють на структуровані і неструктуровані [8]. У першому випадку топологію мережі будують за певними правилами, за допомогою яких здійснюється швидкий пошук даних за точним збігом. У неструктурованих мережах наперед невідомо, куди можна відправити запит, тому у найпростішому випадку застосовується варіант флуд-запитів. Однак масштабованість неструктурованих мереж є доволі проблемною.

Сервіс можна вважати повністю децентралізованим, якщо для його запуску достатньо лише завантажити програмне забезпечення без подальшого введення будь-яких даних для підключення. Такий сервіс має задовольняти базовим принципам [9]:

- OpenSource – програмне забезпечення з відкритим вихідним кодом;
- Zero-Config – запуск програмного забезпечення без додаткових налаштувань;
- нульова довіра – захист від атаки MITM на рівні протоколу;
- низький поріг входу для розуміння технології;
- повністю децентралізований алгоритм роботи.

Недоліки:

- необхідні певні алгоритми маршрутизації та пошуку, які часто не гарантують достовірність результату;
- для ввімкнення у таку мережу потрібно знати координати хоча б одного вузла, відповідно і списки з кількістю адресних даних учасників мережі необхідно публікувати в загальнодоступних джерелах.

Переваги:

- відсутність сервера дає змогу мережі бути відмовостійкою, навіть за

значної динаміки кількості користувачів;

- вища ступінь захищеності від цензури.

I2P – це анонімна, самоорганізуюча розподілена мережа, побудована над Інтернет, використовує модифікований DHT Kademlia зі збереженням хешованих адрес вузлів, зашифровані AES IP-адреси, а також публічні ключі шифрування, причому з'єднання також зашифровані [10, 11]. Ця мережа надає програмам простий транспортний механізм для анонімного та захищеного пересилання повідомлень.

Переваги:

- висока ступінь анонімності користувача;
- повна децентралізація;
- конфіденційність даних: наскрізне шифрування між клієнтом та адресатом.

Недоліки:

- низька швидкість передачі даних;
- «свій Інтернет»

Tor – відкрите програмне забезпечення і система проксі-серверів, яка дає змогу встановити анонімне мережеве з'єднання, захищене від прослуховування. Розглядається як анонімна мережа віртуальних тунелів, що передає дані в зашифрованому вигляді [10-13]. За допомогою Tor користувачі зможуть зберігати анонімність в Інтернет під час відвідування сайтів, публікації матеріалів, відправлення повідомлень. Анонімізація трафіку забезпечується завдяки використанню розподіленої мережі серверів, так званих багатошарових маршрутизаторів. Технологія забезпечує також захист від механізмів аналізу трафіку, що загрожують конфіденційності комерційних таємниць і ділових контактів. Загалом технологія Tor забезпечує роботу в Інтернет у достатньо захищеному режимі, однак для більшої її ефективності необхідний потужний канал зв'язку, оскільки запити проходять через численних користувачів.

Переваги:

- висока ступінь анонімності клієнта за умови дотримання усіх правил;
- простота використання.

Недоліки:

- вихідний трафік прослуховується;
- низька швидкість;
- наявність керуючих серверів.

Варто зазначити, що технологія Tor наділена однією особливістю – приховані сервіси [14]. Користувачі Tor можуть надавати різноманітні послуги – веб-доступ, системи миттєвого обміну повідомленнями, – не розкриваючи свого істинного місцезнаходження. Ця можливість реалізується через спеціальні псевдо-домени .onion верхнього рівня.

1.4 Складові деанонімізації користувачів

Ідентифікаційну інформацію, яку користувач «залишає» про себе під час роботи в мережі Інтернет [17], і пропозиції щодо запобігання витокам даних представлено у вигляді таблиці 1.1

Окремої уваги заслуговує факт одночасного підключення комп'ютера до мережі по анонімному і відкритому каналах. До прикладу, в такому випадку внаслідок розриву інтернет-з'єднання станеться розрив обох з'єднань клієнта з одним і тим самим ресурсом. За цим фактом серверу нескладно буде обчислити і порівняти два одночасно завершених з' єднання до ресурсу по анонімному і відкритому каналах. Таку ситуацію можна вважати деанонімізуючою інформацією й для забезпечення анонімності варто не допускати. В табл. 1.2 наведено порівняння способів анонімізації та їх характеристик

Таблиця 1.2 − Порівняння способів анонімізації та їх характеристик

«Ідентифікатор»	Зміст ідентифікуючих даних	Спосіб анонімізації
IP-адреса	Як мінімум інформація про провайдера та країну користувача	VPN, Proxy, SSH, Tor, I2P, P2P-анонімайзери
DNS leaks	Витоки інформації від служби доменних імен; протоколювання активності клієнта виникає, якщо програмне забезпечення відправляє DNS-запити через DNS-сервер провайдера	Використання анонімних мереж; під час роботи через VPN використання примусово статичних DNS-серверів, що належать VPN-провайдеру
MAC-адреса	При підключені до публічної Wi-Fi точки доступу фіксується MAC-адрес мережного інтерфейсу користувача	Зміна MAC-адреси до сеансу підключення
«Профілювання»	Співставлення великого обсягу трафіку, який виходить через один вузол, із конкретним користувачем	Відмова від використання постійних схем (ланцюгів) Tor, регулярна зміна вихідних вузлів
Соціальна активність в анонімному сеансі	Розкриття особи користувача під час відвідування ним власного профілю соціальної мережі, незважаючи на засоби анонімності	Недопущення неузгодженої активності в анонімному сеансі

Ще одним випадком деанонімізації користувача є передавання програмним забезпеченням, зокрема оглядачами (браузерами), різного роду даних, що зазвичай передбачено специфікацією до програмного продукту. Це обумовлено закладеного у проект програм врахування нормальної і ефективної роботи в складних мережних умовах – обходу блокуючих між мережевих екранів, проксі-серверів тощо.

Типовий оглядач містить наступні функціональні компоненти і технологічні категорії [17]:

– cookies – це текстові файли з деякими даними, що їх зберігають

прикладні програми для різних задач, наприклад, аутентифікації. Розкриття анонімного клієнта настає, якщо він спочатку відвідав ресурс через відкритий сеанс, браузер зберіг cookies, а потім користувач з’єднався через анонімний сеанс. В результаті серверу доступно співставлення cookies і, як наслідок, деанонімізація клієнта;

- Flash, Java – плагіни, що ґрунтуються на цих технологіях, завантажуються від імені користувача як окреме програмне забезпечення та можуть працювати в обхід проксі, зберігати свої cookies й інші налаштування;
- відбиток (fingerprint) браузера – оглядач представляє серверу десятки категорій даних, що дає змогу сформувати унікальний цифровий відбиток браузера, за яким його можна ідентифікувати серед багатьох інших навіть в анонімному сеансі (найчастіше застосовується з метою цільової реклами);
- скрипти JavaScript – код, що виконується на стороні клієнта, здатен накопичувати для сервера ідентифікуючу інформацію, а також, за умови вразливості цільового для користувача ресурсу, створює умови для проведення успішних атак на інформаційний ресурс;
- http-referrer – за допомогою цього http-заголовку цільовий для користувача веб-сайт може визначити, ким було сформовано трафік.

Вирішенням цієї проблеми є налаштування параметрів безпеки оглядача, включаючи блокування кожної із наведених категорій ідентифікації даних, та відмова під час анонімного сеансу від неперевіреного програмного забезпечення.

Висновки до розділу 1

Для забезпечення анонімності в Інтернет існують спеціалізовані утиліти, які дають змогу користувачам входити в анонімну та, зазвичай,

децентралізовану мережу. Більшість з таких мереж – безкоштовні програми з відкритим кодом, що, зрештою, має як позитивні, так і негативні наслідки. Зокрема, вільний доступ до вихідного коду є позитивним моментом оскільки створює умови для швидкого виокремлення інсайдерського коду, якщо таке має місце. Негативним наслідком безперечно є можливість зламу діючої мережі на основі проблемного коду, що призведе до деанонімізації клієнтів цієї мережі.

У кожного із проаналізованих механізмів є свої переваги та недоліки, а проблема анонімності зводиться до вибору між оверлейними (overlay) мережами та децентралізацією із застосуванням криптографії в обох випадках.

Централізовані сервіси слабо протидіють як цілеспрямованим атакам, так і ненавмисним впливам зовнішнього середовища, та мають низьку відмовостійкість. Окрім того жодне централізоване рішення не може забезпечити високого рівня анонімності, так як потрібно довіряти центральному вузлові.

Застосування децентралізованих механізмів дає змогу повністю ліквідувати серверну частину, а для того, щоб «зламати» мережу й демаскувати дані, потрібно скористатися технологіями аналізу трафіку, зокрема Deep Packet Inspection. Тому найкращим шляхом досягнення анонімності в глобальній мережі є поєднання технологій: оверлейні мережі, децентралізація мереж, маскування і шифрування трафіку.

Незважаючи на те, що нині існує достатньо способів залишатися анонімним в Інтернет-мережі, досягнення абсолютної анонімності неможливе – практично у будь-якій ситуації можна дібрати технічні засоби для ідентифікації користувача, бо єдиною перешкодою для цього є матеріальні ресурси і час.

2 ТЕХНОЛОГІЯ DEEP PACKET INSPECTION

Система Deep Packet Inspection (DPI, також complete packet inspection і Information eXtraction або IX) — технологія накопичення статистичних даних, перевірки і фільтрації мережевих пакетів по їх вмісту. На відміну від брандмауерів, Deep Packet Inspection аналізує не лише заголовки пакетів, але і повний вміст трафіку на рівнях моделі OSI з другого і вище. Deep Packet Inspection здатна виявляти і блокувати віруси, фільтрувати інформацію, що не задовольняє заданим критеріям, виконує глибокий аналіз усіх пакетів, що проходять через неї. Термін «глибокий» має на увазі аналіз пакету на верхніх рівнях моделі OSI, а не тільки по стандартних номерах портів. Окрім вивчення пакетів по деяких стандартних патернах, по яких можна однозначно визначити приналежність пакету певному застосуванню, скажімо, по формату заголовків, номерам портів і тому подібне, система DPI здійснює і так званий поведінковий аналіз трафіку, який дозволяє розпізнати додатки, що не використовують для обміну даними заздалегідь відомі заголовки і структури даних. Скільки виробників такого обладнання — стільки і інтерпретацій поведінкових моделей відповідних протоколів, а значить і точність детектування також різниться.

Найбільш великими гравцями і їх продуктами на ринку standalone DPI є Allot Communications, Procera Networks, Cisco, Sandvine. Все більш і більш популярними стають інтегровані в маршрутизатори рішення DPI. Так поступають — Cisco, Juniper, Ericsson і так далі. Такі рішення, як правило, досить компромісні, і не можуть надати весь спектр сервісів, доступних standalone рішенням. Проте, для більшості завдань цього цілком достатньо. Програмні продукти, такі як OpenDPI, їх ринок дуже вузький і, як правило, обмежується корпоративними/кампусними мережами. Важливою особливістю сьогодення DPI є можливість аналітики трафіку за рахунок збору різного роду статистики з

розбиттям по додатках, по тарифних планах, по регіонах, по типах абонентських пристроїв і так далі.

2.1 Типи підключення систем DPI

Не існує єдиного стандарту на DPI, існує велика кількість реалізацій від різних постачальників DPI рішень, що відрізняються за типом підключення і типом роботи.

Існує два поширені типи підключення DPI : активний і пасивний.

Активний DPI — DPI, підключений в мережу провайдера звичним чином, як і будь-який інший мережевий пристрій. Провайдер налаштовує маршрутизацію так, щоб система DPI отримувала трафік від користувачів до заблокованим IP адресам або доменам, а DPI вже приймає рішення про пропуск або блокування трафіку. Активна система DPI може перевіряти як вихідний, так і прохідний трафік, проте, якщо провайдер застосовує DPI тільки для блокування сайтів з реєстру, частіше за все у нього налаштований на перевірку тільки вихідний трафік.

Пасивний DPI — DPI, підключений в провайдерску мережу паралельно або через пасивний оптичний спліттер, або з використанням зеркалювання вихідного від користувачів трафіку. Таке підключення не уповільнює швидкість роботи мережі провайдера у разі недостатньої продуктивності DPI, тому застосовується у мережах великих провайдерів. DPI з таким типом підключення технічно може тільки виявляти спробу відвідати заборонений контент, але не блокує його. Щоб обійти це обмеження і заблокувати доступ на заборонений сайт, DPI відправляє користувачеві, що запитує заблокований URL, спеціально сформований HTTP пакет з перенаправленням на сторінку-заглушку провайдера, немов таку відповідь прислав сам запрошений ресурс (підробляється IP адреса відправника і TCP sequence). Через те, що DPI фізично розташований

ближче до користувача, ніж запрошений сайт, підроблена відповідь доходить до пристрою користувача швидше, ніж справжня відповідь від сайту.

Іноді пасивний тип DPI застосовується для підміни відповіді DNS – сервера, а не самого сайту.

Підроблені пакети, сформовані DPI, легко виявити аналізатором трафіку, наприклад, WireShark. Блокування таких пакетів теж не представляє особливої складності

Під "звичайним" типом DPI розуміється такий DPI, який фільтрує певний тип трафіку тільки на найпоширеніших портах для цього типу. Наприклад, "звичайний" DPI виявляє і блокує заборонений HTTP трафік тільки на порту 80, HTTPS трафік на порту 443. Цей тип DPI не відстежуватиме заборонений контент, якщо ви відправите запит із заблокованим URL на незаблокований IP або нестандартний порт.

На відміну від "звичайного" типу DPI, цей тип DPI класифікує трафік незалежно від IP адреси і порту. Таким чином, заблоковані сайти не відкриватимуться, навіть якщо ви використовуєте проксі-сервер на абсолютно іншому порту і незаблокованій IP адресі.

Основна проблема усіх існуючих рішень DPI полягає в тому, що для того, щоб однозначно визначити приналежність того або іншого потоку даних до одного з мережевих застосувань, пристрій, що здійснює аналіз трафіку, повинен побачити обидва напрями сесії. Іншими словами, трафік, що входить і вихідний, в межах одного потік повинні пройти через один і той же пристрій. Якщо DPI розуміє, що бачить тільки один напрям у рамках сесії, вона не має можливості співвіднести цей потік з якою-небудь відомою категорією трафіку з усіма витікаючими наслідками. У зв'язку з цим, коли мова заходить про контроль трафіка від клієнта, встає дуже логічне питання про асиметричний трафік, який для більш-менш великих операторів є не екзотикою, а повсякденністю. Різні вендори вирішують цю задачу по-різному:

Cisco задовольняється половинкою сесії і намагаються визначити тип мережевого застосування, використовуючи лише ці дані. Очевидно, що при цій методиці страждає точність детектування додатків, особливо тих, для яких потрібно поведінкові моделі аналізу. Також в такій реалізації є ряд обмежень, що накладаються на можливості управління таким трафіком, у кожного вендора вони свої.

Sandvine для вирішення проблеми асиметричного трафіку використовує наступну ідею — весь трафік, що є асиметричним, за допомогою інкапсуляції в broadcast фрейми пересилається на усі пристрої DPI, що знаходяться в єдиному домені. У результаті цієї пересилки пристрої, що обробляли до цього лише один напрям у рамках сесії, зафіксують і другий, на підставі чого можна буде здійснити повний комплекс заходів по аналізу і управлінню трафіком. Недолік цієї схеми очевидний — при великих об'ємах асиметричного трафіку на мережі пред'являються серйозні вимоги до каналів зв'язку, що сполучають пристрої DPI на різних сайтах. В деяких випадках, коли йдеться про асиметрію порядків декількох гігабіт (чи десятків гігабіт) в секунду, ця методика непридатна у зв'язку з високими накладними витратами на організацію каналу між сайтами.

Розумніше за усіх поступають Procera і Allot. Ідея схожа на реалізацію Sandvine з тією відмінністю, що між сайтами пересилається не асиметричний трафік, а метадані, що явно характеризують його. У загальному випадку можна вважати, що це протокольні заголовки, хоча насправді усе трохи складніше. За рахунок подібної оптимізації вимоги до каналів зв'язку набагато гуманніші, відносно реалізації Sandvine виграш може бути до 95%.

Ще один важливий момент, який є критичним для деяких замовників, — це періодичність оновлення файлів сигнатур, на підставі яких здійснюється аналіз трафіку. Деякі вендори роблять оновлення раз на квартал, деякі — раз на тиждень. У разі потреби критичне оновлення (що містить методики виявлення нової версії) може вийти раніше календарного терміну. Як правило, усі

вендори адекватно відносяться до бажань замовників додати якийсь новий протокол в список підтримуваних і всіляко допомагають в цьому. Не секрет, що на кожному локальному ринку існують специфічні застосування, практично відсутні в інших країнах.

З точки зору експлуатації, оператор може контролювати підключених через DPI канали на рівні додатків. Раніше завдання реалізації QoS (Quality of Service) вирішувалися виключно засобами побудови черг на підставі маркування трафіку службовими бітами в заголовках IP, 802.1q і MPLS, виділяючи найбільш пріоритетний трафік (різного роду VPN, IPTV, SIP і так далі), і гарантуючи йому певну пропускну спроможність у будь-який момент часу. Трафік типу Best Effort, до якого відноситься увесь Інтернет трафік домашніх абонентів (HSI — High Speed Internet), залишався фактично без контролю, що давало можливість тому ж Bittorrent забирати собі усю вільну смугу, що, у свою чергу, вело до деградації будь-яких інших веб-сервісів. З використанням DPI у оператора з'являється можливість розподілити канал між різними застосуваннями.

За допомогою DPI спецслужби можуть вести спостереження за мережевою активністю того або іншого користувача. Можна заблокувати VPN, HTTPS і інші технології, що роблять неможливим аналіз контенту. Зрозуміло, можна закривати доступ користувачів до сайтів, що дуже актуально у зв'язку з останніми подіями в законотворчій діяльності України.

2.2 Апаратні засоби систем DPI

Основною функцією систем DPI є фільтрація трафіку, і виконує її програмний комплекс, який установлений на апаратну платформу.

Часто виробник поставляє готовий комплект сервера з установленим ПЗ. Але такий сервер значною мірою відрізняється від стандартних рішень для обробки даних, на додаток до нього може поставлятися система зберігання

даних для здійснення функцій кешування контенту або збору статистики усього трафіку для реалізації вимог законодавства.

Сервер для DPI – це спеціальна мережева платформа. Вона виглядає як звичайний сервер 1U (рис. 2.1), але акцент в організації її апаратних компонентів зроблений на мережеву складову, а не на жорсткі диски або оперативну пам'ять.

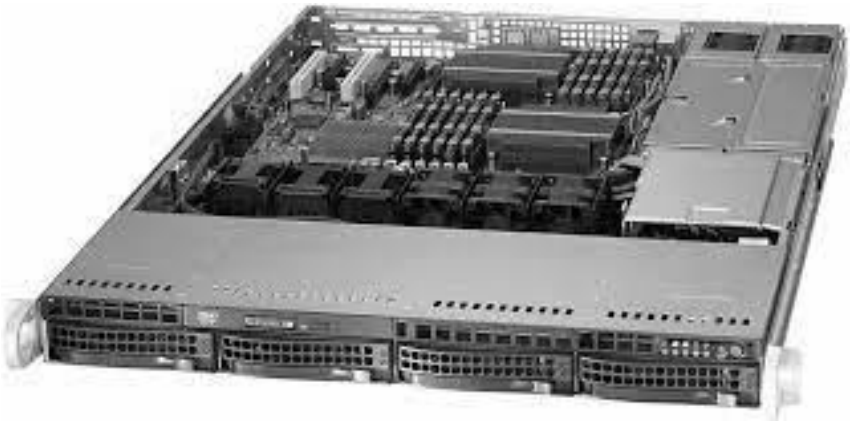

Рисунок 2.1 – Вигляд звичайного серверу 1U

У стандартній комплектації, окрім мережевих інтерфейсів для управління присутні 4 x 1 GbE RJ45 порти і 2 x 10 GbE SFP+, а також від 2 до 4 NMC modules with PCIex8 gen.3, куди можуть бути встановлені мережеві модулі розширення (рис. 2.2), кожен з яких збільшує число мережевих портів до 8 x 1 GbE RJ45, 4 x 10 GbE SFP+ або 2 x 40 GE QSFP+.

Рисунок 2.2 – Вигляд мережевих модулів розширення

Одна з обов'язкових умов для мережевих карт, використовуваних в системі DPI (при установці DPI «в розрив»), – наявність режиму Bypass.

Bypass сполучає мережеві інтерфейси на першому рівні OSI, це означає, що якщо на сервері пропадає живлення, то з'єднання між портами продовжує працювати і пропускати через себе трафік без функції фільтрації за допомогою живлення від батареї, при цьому швидкість перемикання на Bypass – менше 60 мікросекунд.

Також такий сервер має поліпшену систему моніторингу стану роботи (Advanced Lights Out Management), що дозволяє візуально на дисплеї і видалено контролювати усі параметри системи. BIOS материнської плати апаратно продубльований і має функцію дистанційного оновлення. Два блоки живлення резервують один одного і підтримують гарячу заміну.

Для установки програмного комплексу досить пари жорстких дисків в RAID1, а один або два процесори Intel® Xeon® E5 – 2600 v4 справляються із завданням глибокої фільтрації трафіку і споживають всього 145 W, економлячи електроенергію і не виділяючи багато тепла.

Для організації роботи по зберіганню статистики трафіку або кешуванню контенту (відео, оновлення, фотографії) до системи DPI може підключатися зовнішня система зберігання. Оскільки об'єми даних, що зберігаються, вимірюються десятками терабайт, а швидкість доступу до них не грає такої істотної ролі, як при роботі з базами даних, застосовують рішення, засноване на одній системі зберігання даних і підключених до неї дискових масивів.

Головний пристрій з двома контролерами на базі процесора Intel® Xeon® E5 – 2600 V4 (Broadwell – EP) і двома блоками живлення для забезпечення відмовостійкості, до 24 x 2.5″ HDD/SSD дисків і 2 вбудованих 2.5″ SATA SSD диска в RAID1 для установки ОС. Кожен контролер оснащується 2 x 10 GbE портами для підключення до мережі і портами SFF 8644 mini – SAS для підключення розширення.

Управління дисками здійснює open source ОС SmartOS, встановлена на кожного з контролерів і налаштована на роботу в кластері. Використання сучасної файлової системи ZFS і технології RAID-Z забезпечує повний контроль над усіма фізичними і логічними дисками, високу швидкість доступу до них, контроль їх цілісності і мінімізацію фрагментації даних.

Для збільшення об'єму даних, що зберігаються, до головного пристрою підключаються додаткові JBOD (рис 2.3).

Рисунок 2.3 – Вигляд дискового масиву JBOD

Один такий кластер додає системі до 70 дисків 3.5″/2.5″ 12 Gb/s SAS HDD або SSD, підключається до кожного контролера на швидкості до 12 Gb/s і управляється ОС контролера.

Відмовостійкість системи забезпечується надмірним підключенням кожного пристрою один до одного (рис 2.4).

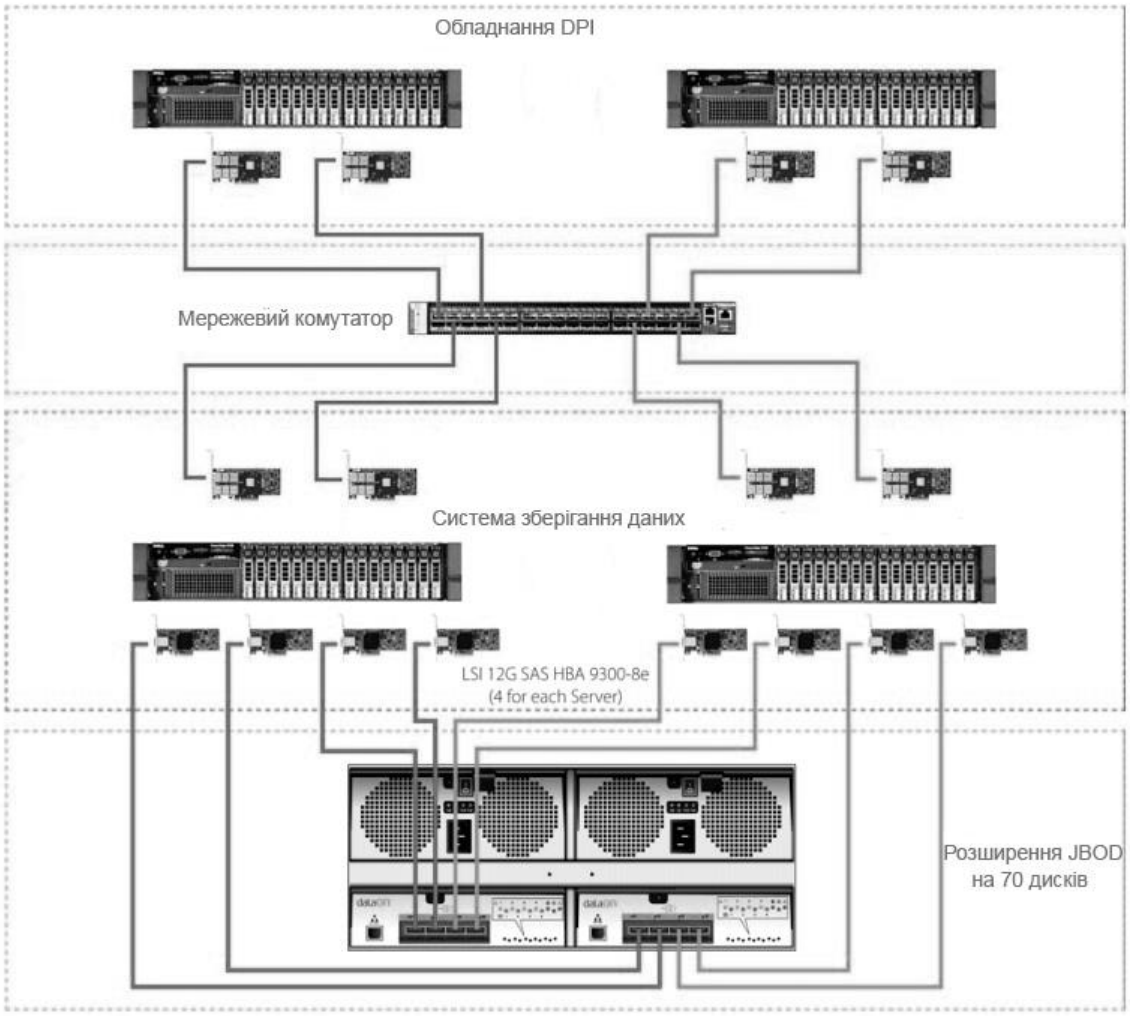

Рисунок 2.4 – Схема резервування системи DPI

Виробники систем глибокого аналізу трафіку пропонують свої референсні схеми підключення обладнання і його конфігурації, але значно зручніше, коли це рішення не є закритою платформою з дорогими додатковими компонентами, а побудовано на стандартних платформах з можливістю легкої модернізації і збільшення продуктивності.

Нині на ринку присутні декілька великих виробників, що пропонують спеціалізоване обладнання для DPI (Allot, Procera, Sandvine). До них можна додати світових лідерів в області мережевих технологій, які також мають рішення для глибокого аналізу трафіку (Cisco, Huawei). Кожна з цих компаній вже більше 15 років займається розробкою рішень для контролю і управлінням трафіком з гнучким налаштуванням продуктивності і багатим функціоналом.

Платформа складається з продуктивного обладнання і добре оптимізованого програмного забезпечення.

Обладнання серії Allot NetEnforcer (рис 2.5) є апаратними комплексами аналізу мережевого трафіку і управління ним для окремих застосувань і абонентів. Дозволяють оптимізувати послугу надання широкосмугового доступу в Інтернет корпоративним користувачам і інтернет-провайдерам. Обладнання відмінно справляється з визначенням типу трафіку (p2p, video, skype) і його розподілом. У лінійці представлене обладнання різної продуктивності, але має однакову функціональність.

Allot NetEnforcer	AC-500	AC-1400 / AC-3000	AC-6000
			
Смуга пропускання	From 20 to 400 Mbps	From 100 Mbps to 8 Gbps	From 2 Gbps to 16 Gbps
Кількість мережевих портів	2 or 4 x 10/100/1000BASE-T	8 x 10/100/1GE SX/LX/ ZX Copper	8 x 1GE SX/LX/ ZX, Copper and 8 x 10GE/1GE SR, LR, ER
Макс. число потоків і підключень	200,000 / 400,000	2M / 4M	5M / 10M
Кількість абонентів	32,000	160,000	400,000
Інтегровані засоби безпеки VAS	URL - фільтрація	URL - фільтрація, батьківський контроль, захист від шкідливого ПЗ і DDoS, анти-бот сервіс	
Перенаправлення трафіка	4 порти 10/100/1GE для перенаправлення трафіка на внутрішні сервіси		Будь-який порт може використовуватися для резервування чи перенаправлення

Рисунок 2.5 – Обладнання для систем DPI серії Allot NetEnforcer

Allot Service Gateway (рис. 2.6) – модульне масштабоване рішення для операторів зв'язку, призначене для фіксованих, мобільних і змішаних мереж широкосмугового доступу, а також для центрів обробки даних. Шлюз дозволяє ідентифікувати трафік на швидкостях до 160 Гбіт/с (масштабується в кластер до 1 Тбіт/с), проводити його аналіз і візуалізацію, застосовувати задані політики для оптимізації смуги пропускання і поліпшення якості надання сервісу абонентам. Характеристики даного рішення наведені у таблиці 2.1.

Рисунок 2.6 – Обладнання для систем DPI серії Allot Service Gateway

Таблиця 2.1 – Порівняння характеристик обладнання

Allot Service Gateway	Sigma E6	Sigma E14
Шасі	6 слотів	14 слотів
Смуга пропускання на платформу	до 64 Гбіт/с	до 160 Гбіт/с
Смуга пропускання на кластер	до 360 Гбіт/с	до 1 Тбіт/с
Кількість мережевих портів	до 8 портів 10GE або 32 по 1GE	до 16 портів 10GE або 32 по 1GE
Кількість абонентів	до 3 200 000	50M/100M
Макс. число з’єднань і потоків	20/40 млн	50/100 млн
Перенаправлення трафіка	Перенаправлення трафіка в сервіси, які працюють на блейд-модулях в платформі з підтримкою «гарячої» заміни, в реальному часі або розгортання на зовнішніх системах	
Збір даних	Збір і експорт даних, сесій і звітів використання мережі в системи аналізу і біллінгу	
Детектування спільного доступу до мобільного Інтернету	Виявлення тетеринга і застосування політик оператора по відношенню тетеринга в реальному часі	
Платформа рівня оператора	Шасі і блейд-модулі ATCA; висока доступність за рахунок автоматичного аварійного переключення; резервування блейд-модулів	
Захист інвестицій	Модернізація з можливістю використання існуючих шасі і блейд-модулів	

Компанія Procera робить акцент на своїй програмній платформі PacketLogic, ядром якої є DRDL (Datastream Recognition Definition Language), що розробляється інженерами компанії упродовж 15 років.

Молодша платформа PacketLogic 1600 використовується для серверів статистики і трендів (агрегація даних). Вона складається з двох компонентів: вузла управління і вузла зберігання. До одного вузла управління можна підключити до 4 вузлів зберігання, що дозволяє масштабувати систему під об'єми статистичної інформації, що зберігається та збільшуються.

Компанія має 5 основних фізичних рішень (рис. 2.7) різних конфігурацій і новинку PacketLogic/V Platform – віртуальна платформа, яка дозволяє розгорнути весь функціонал PacketLogic на будь-якому сумісному обладнанні.

						
	PacketLogic/ V Platform	**PacketLogic 7000 Platform**	**PacketLogic 8000 Platforms**	**PacketLogic 9000 Platform**	**PacketLogic 15000 Platform**	**PacketLogic 20000 Platform**
Розмір	-	1U	2U	2U	4U	14U
Смуга пропускання	до 155 Гбіт/с	від 1 до 5 Гбіт/с	від 32 до 70 Гбіт/с	120 Гбіт/с	до 600 Гбіт/с	до 600 Гбіт/с
Кількість мережевих портів	Залежить від апаратної платформи	від 2 до 11xGE	від 16 до 24xGE або від8 до 12x10GE	24xGE або 16x10GE	24x10GE або 3x100GE	36x10GE і 4x40GE або 8x10GE
Максимальна кількість підключень	-	від 400 тис. до 2 млн.	від 15 до 20 млн.	30 млн.	240 млн.	240 млн.
Кількість абонентів	-	від20 до 100 тис.	від 2 до 3 млн.	3 млн.	10 млн.	10 млн.

Рисунок 2.7 – Апаратні платформи DPI PacketLogic компанії Procera

На всіх платформах використовується однакове програмне забезпечення, що дозволяє використовувати в одній мережі декілька пристроїв різної продуктивності в певних сегментах. Усі пристрої підтримують роботу з асиметричним трафіком завдяки функції Flow Sync і режим Bypass.

Компанія Sandvine має скромніший асортимент систем для глибокої фільтрації трафіку (DPI) – це 3 пристрої Policy Traffic Switch різної

продуктивності і віртуальна платформа PTS Virtual Series, побудована на Sandvine Policy Engine.

Віртуальна платформа PTS Virtual Series має ті ж функції, що і апаратне рішення PTS, але відрізняється більшою гнучкістю за рахунок того, що може бути встановлена на будь-яке апаратне рішення і споживати ту кількість ресурсів, яка потрібна при поточному навантаженні (рис. 2.8). Також вона легко інтегрується з віртуальною інфраструктурою оператора, у тому числі з віртуальною мережею.

Основними перевагами апаратної платформи PTS є:

- Функція розподілу навантаження на апаратному рівні – продуктивність PTS не зменшується при включенні додаткових портів, оскільки модуль масштабування лінійний.
- Управління і обробка даних гарантують захист PTS від мережевих атак (DDoS, флуд) і не знижують її продуктивності.
- Програмний bypass не навантажує додатково процесор при обробці дубльованого трафіку.
- Гнучка конфігурація модулів – додаткові модулі можуть бути використані для збільшення числа портів або забезпечення bypass.

Metric	PTS 22000	PTS 24000	PTS 32000
Розмір	2 RU	4 RU	2 RU
Смуга пропускання	40 Gbps	160 Gbps	400 Gbps
Смуга пропускання в кластері	280 Gbps	720 Gbps	8 Tbps
Число абонентів	2 M	5 M	30 M
Кількість підключень	16 M	72 M	90 M
100GE порти	N/A	N/A	2
40GE порти	N/A	N/A	2
10GE порти	11	4	16

Рисунок 2.8 – Апаратні платформи DPI компанії Sandvine

Пристрої можуть об'єднуватися в кластери для збільшення числа портів і продуктивності.

У компанії Cisco за функції DPI відповідає серія пристроїв Service Control Engine (SCE), характеристики яких приведені на рисунку 2.9. Вони відносяться до операторського класу, можуть аналізувати трафік, розпізнавати додатки і динамічно застосовувати задані політики. Комплекс SCE об'єднує апаратну платформу і додаткові програмні пакети Subscriber Manager (SM), Collection Manager (CM) і SCA BB Console для налаштування, управління і моніторингу.

КАТЕГОРІЯ	SCE1000 	SCE2000 	SCE8000 
Інтерфейси	2-GBE (Fiber SX/LX)	4-GBE (Fiber SX/LX)	2-10G 4-10G (Fiber SX/LX/ZX)
Інтерфейси управління	2 x 10/100/1000 Eth	2 x 10/100/1000 Eth	2 x 10/100/1000 Eth
Макс. кількість однонаправлених потоків	2M	2M	16M (зі збільшенням до 32M)
Макс. кількість абонентів	40,000	200,000	1,000,000
Підключення до мережі	Out of Line Inline	Out of Line Inline Clustering	Out of Line Inline Clustering

Рисунок 2.9 – Апаратні платформи DPI компанії Cisco

Молодша лінійка систем DPI SCE1000 і SCE2000 перенесена в EOL, їх більше не випускають і не продають. Старша все ще активно продається, але у зв'язку з новою стратегією Cisco про перенесення функцій DPI на пристрої ASR скоро зникне і вона.

Cisco ASR1000 з підтримкою функції Application Visibility and Control (AVC) дозволяє ASR1000 збирати статистику мережевого трафіку, робити

розбиття по додатках і абонентах (NBAR2) і вивантажувати її в Net Flow колектори (FNF+), наприклад в Cisco Insight Report. Такий підхід дозволяє поєднувати на одному пристрої максимальну кількість функцій і масштабувати мережу у рамках однієї лінійки продуктів.

Компанія Huawei останніми роками активно збільшує свою долю на мережевому ринку. У напрямі аналізу трафіку Huawei представляє платформу SIG9800-X – сервісний шлюз операторського класу, побудований на продуктивній платформі маршрутизації, яка дозволяє виконувати повний перелік функцій DPI: аналіз і управління трафіком, візуалізація статистики по використанню смуги пропускання додатками і користувачами, QoS і захист від мережевих атак (рис. 2.10).

	Характеристики		
Модель	**SIG9800-X3** 	**SIG9800-X8** 	**SIG9800-X16** 
Сервісні (SPU/LPU) слоти	3 *слоти*	8 *слотів*	*16 слотів*
Інтерфейси (LPUK)	1*10GE LAN/WAN карта 1*10G POS карта 12*GE (Optical) карта 12*10M/100M/1000M(RJ-45 electrical) карта		
Інтерфейси (LPUN)	2*10GE LAN/WAN карта 20*GE (Optical) карта		
Смуга пропускання	20 Гбіт/с	60 Гбіт/с	120 Гбіт/с
Кількість підключень	16M	48M	96M
Кількість нових підключень в секунду	0.8M	2.4M	4.8M
Затримка	<200us		

Рисунок 2.10 – Апаратні платформи DPI компанії Huawei

Виробник заявляє, що SIG9800 здатна ідентифікувати більше 850 протоколів в 20 категоріях для більш ніж тисячі додатків.

З пристроїв молодшої серії можна виділити Cisco SCE1000 і Huawei SIG9800-X3 як занадто дорогі для цього сегменту. Вартість Huawei пояснюється його високою продуктивністю, що перевищує всі інші платформи, а Cisco користується своїм ім'ям і досвідом на ринку мережевих пристроїв.

Якщо порівнювати пристрої середнього сегменту, видно практично повний паритет по продуктивності і технічному оснащенню.

2.3 Варіанти використання DPI

Основні сценарії, які реалізуються на практиці за допомогою технології DPI:

- Аналіз і класифікація трафіку, моніторинг і тренди.
- Пріоритезація трафіку.
- Оптимізація аплінків.
- Розподіл каналу між абонентами.
- Кешування.
- Поведінкова оцінка абонентів.
- Повідомлення абонентам.
- Заборона ресурсів (білий і чорний списки).
- Захист, перехоплення трафіку, предфільтр.

Завдання системи глибокого аналізу трафіку – використовуючи набори сигнатур і поведінкові методи, проводити класифікацію і створювати в реальному часі звіти про споживання трафіку додатком або абонентом.

Отримання сумарної інформації за класами трафіку кожного абонента дозволяє окремо тарифікувати SIP, Skype, Viber, BitTorrent. Також можна заздалегідь виявити додаток або користувача з найбільшим навантаженням на

смугу пропускання, проаналізувати тренди і захистити мережу від перевантаження, обмеживши швидкість.

Пріоритезація трафіку – незамінна функція управління трафіком для оптимізації пріоритету між протоколами і забезпечення високої швидкості роботи абонента в Інтернеті.

Найпопулярнішим прикладом необхідності розподілу пріоритетів трафіку є p2p протокол (Torrent). Вирішення цієї проблеми просте: робиться пріоритет трафіку p2p нижче за інших, і обмежується смуга пропускання, інші застосування починають працювати стабільно, як потрібно.

Система DPI дозволяє змінювати поле пріоритету в пакетах, що проходять через неї, залежно від детектованого протоколу, що дозволяє маршрутизаторам і шейперам використовувати цю розмітку для забезпечення потрібного рівня QoS.

Аплінк – це канал, який складає основну частину трафіку оператора і є обмеженням для надання абонентові вищих швидкостей. Забезпечити високу якість послуг можна двома шляхами: збільшенням ширини каналу або оптимізацією трафіку.

Зростання трафіку зазвичай відбуваються в певні години і дні тижня (вечір, вихідні, не більше декількох годин), так що збільшувати ширину каналу для таких короткочасних моментів фінансово недоцільно. Проте, якщо не робити ніяких дій, абоненти стикатимуться з повільним завантаженням.

Важливою особливістю DPI системи є те, що правила поведінки трафіку можна задати не лише для додатка, але і для конкретного користувача (per – subscriber).

Тарифний план абонента може обмежувати його загальну смугу пропускання, задавати пріоритети за класами трафіку для підвищення QoS (обмежувати Torrent або, навпаки, давати більше швидкості на відео), призначати єдині правила для корпоративних абонентів, що мають загальну групу IP адрес.

Користувачі можуть бути розділені на групи (золота, срібна, бронзова) по кількості споживаного трафіку. Для кожної групи задається та швидкість, яка задовольняє користувачів. Якщо користувач починає споживати більше трафіку, він переноситься у іншу групу. Оператор економить ресурси, а користувачі задоволені швидкістю, що надається.

Інтернет – це безмежне сховище інформації, і кожен користувач знаходить тут те, що йому цікаве. Але існує найбільш популярна інформація, яку викачують більшість користувачів. Це можуть бути відеоролики, фільми, оновлення програм і операційних систем, фотографії і картинки.

Кеш-сервер дозволяє викачаний з Інтернету користувачем популярний контент поширювати іншим користувачам вже локально, з внутрішнього сховища. Мало того що оператор економить на інтернет-трафіку, так і швидкість доступу до керованого контенту дорівнює швидкості локальної мережі, а не швидкості доступу до мережі Інтернет.

Кожен користувач мережі унікальний. Система DPI може зібрати різну інформацію, не порушуючи особистих прав абонента, і показати її в наочному виді операторові.

Використовувати отриману інформацію можна різними способами, в першу чергу для поліпшення якості послуг, що надаються.

Якщо знати контент, якому віддається перевага користувачем, можна налаштувати відповідний пріоритет трафіку. Залежно від того, в який час абонент користується Інтернетом, можна збільшити або зменшити смугу пропускання для інших.

Повідомлення абонентам – це функція, яка дозволяє операторові оповіщати абонента під час роботи в Інтернеті. Користувач вводить адресу сайту, який хоче відвідати, а бачить в браузері повідомлення від оператора, що змінюється через декілька секунд сторінкою, яку планував відвідати.

Повідомлення може містити як інформацію від оператора (зміна в тарифі, регламентні або технічні роботи, спеціальні пропозиції), так і екстрені повідомлення від державних структур.

Такий спосіб сповіщення охоплює дуже широку аудиторію, оскільки майже 60 % людей принаймні раз на день виходять в мережу Інтернет, а також знижує витрати на інші способи сповіщення (SMS, телефонний дзвінок).

Всім операторам зв'язку на території України з 2017 року необхідно виконувати вимоги санкцій і блокувати заборонені веб-ресурси. Щоб виконувати ці вимоги, оператор повинен постійно перевіряти актуальні записи в реєстрі і фільтрувати трафік заборонених сайтів.

Фільтрація по IP-адресах – не ефективний спосіб, оскільки вимагає навантаження на персонал із-за ручних операцій і допускає велике число помилок у зв'язку зі зміною доменного імені забороненого сайту або його IP. Використання DPI-технології з фільтрацією по URL в автоматичному режимі (завантаження списків) дає найкращий результат, оскільки вона розбирає усі пакети, що проходять через неї, і визначає їх приналежність і заголовки до заборонених ресурсів.

При негативному балансі рахунку абонента його можна переадресувати в особистий кабінет для оплати, надавши доступ до сторінок платіжних систем і обмеживши до усіх інших сайтів. Також в білий список можуть входити внутрішні мережеві ресурси і інші, на які оператор надає доступ.

Оскільки DPI пропускає через себе і фільтрує весь трафік, захист абонентів і обчислювальних систем в хмарі стає для неї однієї з безпосередніх завдань. Основними напрямами захисту є:

- Спам-боти (виявляються на основі аналізу SMTP трафіку).
- DoS і DDoS-атаки (виявляються по аномаліях трафіку).
- Зараження вірусами (виявляється за сигнатурами).

Захист від спаму реалізується шляхом блокування відправника, коли з однієї адреси генерується надмірно велике число SMTP -запитів.

Система DPI дозволяє захиститися від TCP SYN Flood і Fragmented UDP Flood.

Атака SYN flood викликає підвищену витрату ресурсів системи, оскільки на кожний SYN-пакет, що входить, система повинна зарезервувати певні ресурси в пам'яті або згенерувати велику кількість пакетів в секунду, що призводить до її відмови.

DPI виявляє перевищення порогу SYN-запитів, та замість сайту відповідає на них.

Fragmented UDP Flood атака здійснюється фрагментованими udp-пакетами, зазвичай невеликого розміру, на обробку і аналіз яких витрачається багато ресурсів.

DPI відкидає неактуальні для сайту протоколи або обмежує їх по смузі пропускання (для веб-сайту залишаються тільки протоколи HTTP і HTTPS).

При захисті від DDoS-атак часто застосовуються різні поведінкові стратегії (behavioral DDoS protection), які дозволяють визначити відхилення в нормальній поведінці. Але за допомогою системи глибокого аналізу трафіку можна використовувати простіший і ефективніший підхід – використання тесту Тюрінга (сторінки з CAPTCHA від англ. Completely Automated Public Turing test to tell Computers and Humans Apart), який дозволяє визначити, людина або комп'ютер здійснює запит до ресурсу.

Якщо кількість запитів до сайту перевищує порогове значення, користувачеві пропонується ввести слово з картинки. Якщо тест пройдений, користувач заноситься в білий список і може далі працювати з сайтом. Якщо тест провалений, то бот не може просунутися далі і зробити атаку на сайт.

Ще однією додатковою функцією DPI може стати допомога системі технічних засобів для Кіберполіції. Можливість проводити запис мережевого трафіку в реальному часі може використовуватися для моніторингу трафіку в цілях діагностики і аналізу загроз безпеки. Перехоплений за допомогою певних протоколів трафік записується на дисковий накопичувач.

Можливість використання DPI як предфільтр знижує навантаження на обладнання за рахунок того, що відсікає усі протоколи (torrent, youtube, mpeg, flash), що не представляють інтересу. В результаті трафік скорочується більш ніж на 50 %.

2.4 Глибокий аналіз пакетів і даних для SCADA-систем

Світова промисловість, об'єкти транспортної галузі і енергетики нині зазнають труднощі із забезпеченням належного рівня IT-безпеки. Ця сфера, в основному, використовує типові SCADA-системи і промислові АСУ із стандартизованими протоколами обміну даними. Багато з цих систем проектувалися десятки років назад, коли поняття IT-безпеки не існувало взагалі.

Сучасні мережеві технології вже щільно увійшли до промислової інфраструктури, дозволяючи отримати доступ до інформації в мережі на всіх рівнях. З одного боку, легкий доступ до інформації підвищує ефективність системи, а з іншого боку, зростає її вразливість з боку різних мережевих загроз (несанкціонований доступ, віруси, хакерські атаки). Ця проблема вимагає негайного рішення, але, враховуючи велику тривалість життєвого циклу промислових систем розраховувати на швидку появу і поширення захищених SCADA-систем, промислових систем управління і відповідних протоколів не доводиться.

Між тим рішення усунення загроз в безпеці промислових систем існують. Одним з них є застосування спеціальних брандмауерів для SCADA –систем, які використовують технологію глибокого аналізу пакетів даних (Deep Packet Inspection – DPI) і здатних забезпечити контроль над трафіком системи управління.

За останні 10 років промислові системи використовують такі мережеві технології, як Ethernet і TCP/IP. Ці технології широко використовуються в

АСУ і SCADA-системах, створюючи умови для ефективнішої роботи підприємств і роблячи системи контролю доступнішими для користувачів. Але разом з перевагами вони принесли і проблему: об'єднання інформаційних мереж на різних рівнях підприємства в єдиний наскрізний інформаційний простір значно підвищує вразливість системи з боку зовнішніх атак, вірусів і хакерів. Проблему посилює те, що мережеві протоколи, які використовуються промисловими АСУ і SCADA-системами, розроблялися без урахування вимог по забезпеченню безпеки. Якщо вони і пропонують деякі заходи по обмеженню негативної поведінки в мережі, то ці заходи вкрай примітивні і легко обходяться. А якщо кому-небудь дозволено читати дані з контролера, то можна вимкнути або перепрограмувати його.

Промислові системи контролю і управління рідко замінюються і модернізуються. Їх термін експлуатації складає від 10 до 20 і більше років. Функціонал таких систем визначається заздалегідь і не міняється, і вразливість промислових АСУ і SCADA-систем, раніше введених в експлуатацію, не може бути усунена відповідними патчами, як це робиться в ОС Windows. Тому пройде багато років, перш ніж нові, безпечніші системи контролю і управління потримають поширення. Протягом цих років безліч промислових систем контролю і управління будуть беззахисні перед шкідливими діями навіть непрофесійних хакерів. А якщо зловмисник або шкідливе програмне забезпечення (ПЗ) може отримати доступ до промислової системи, то може бути виведено з ладу більшість контролерів, порушений технологічний процес, завдана шкода дорогому устаткуванню, можливе створення умов для виникнення аварій і так далі.

Вирішенням цієї проблеми є технологія глибокою аналізу пакетів DPI, що дозволяє контролювати всю інформацію, яка передається в системі з високою точністю. Це відносно просте рішення. Воно не вимагає повної заміни дорогих вже існуючих SCADA-систем і устаткування.

Для розумінні того, як працює технологія DPI, важливо розуміти принцип работи звичайного брандмауера. Він перехоплює трафік і аналізує його відповідно до списку наборів правил (Access Control List – ACL). Усі повідомлення, які не задовольняють спискам ACL не пропускаються брандмауером.

Традиційний брандмауер використовує списки ACL для перевірки трьох перших полів повідомлення Ethernet:

1) адресу відправника повідомлення (IP-адресу джерела);

2) адресу одержувача повідомлення (IP-адресу приймача);

3) протокол рівня додатка, що міститься в IP-повідомленні, за номером віртуального порту (порт одержувача).

Наприклад, протокол Modbus TCP використовує порт 502, а протокол HTTP використовує порт 80. Номери портів зареєстровані в департаменті Internet Assigned Numbers Authority (IANA) міжнародній організації Internet Corporation for Assigned Names and Numbers (ICANN) і ніколи не змінюються.

Якщо треба дозволити тільки Web -трафік (протокол HTTP) від клієнта з IP -адресою 192.168.1.10 до Web – серверу з адресою 192.168.1.20, то слід в список ACL додати такий рядок: Allow Src=192.168.1.10 Dst=192.168. 1.20 Port=HTTP.

Після завантаження списку ACL з цим правилом пропускатимуться тільки повідомлення, що задовольняють усім трьом вказаним критеріям.

Якщо вимагається заблокувати весь трафік Modbus TCP, що проходить через брандмауер, то треба визначити правило, що забороняє усі пакети, що містять номер 502 в полі заголовка пакету, як порту одержувача.

Проблема принципу роботи традиційних брандмауерів полягає в тому, що вони абсолютно однозначні. Використовуючи такий принцип, можна або дозволити певний протокол, або заборонити його. Детальніше управління в середині протоколу неможливе.

Причина цього в тому, що протоколи, які використовуються в АСУ і SCADA-системах, не піддаються деталізації. З точки зору номера порту одержувача, сполучення з читанням даних виглядає як оновлення ПО. Таким чином дозволяючи проходження сполучень з читанням даних з пристрою операторського інтерфейсу для ПЛК через стандартний брандмауер, автоматично дає дозвіл на програмування контролерів. А це серйозне упущення з точки зору безпеки.

На жаль, брандмауери, представлені на ринку, не здатні розрізняти команди від SCADA-системи. Оскільки трафік SCADA -системи вважається критично важливим, більшість інженерів просто повністю дозволяють його, незважаючи на можливі проблеми з безпекою.

Очевидно, що слід глибше розбиратися в протоколах для того, щоб точно визначати, який протокол для чого використовується. І це якраз те, що дозволяє робити технологія DPI. Після того, як традиційні правила брандмауера застосовані, брандмауер з підтримкою DPI досліджує контент у середині TCP/IP повідомлення і застосовує більш детальні правила. Він спроектований так, щоб розуміти специфічні протоколи SCADA-систем і застосовувати фільтри до полів і їх значень, що і дозволяє детально контролювати систему. Залежно від протоколу ці поля можуть включати команди (такі як читання або запис регістра), об'єкти, сервіси (отримати/записати значення) і діапазони адрес ПЛК (рис. 2.12).

Рисунок 2.12 – Порівняння можливостей фільтрації трафіку брандмауерами

Наприклад, брандмауер з можливістю глибокого дослідження протоколу Modbus (Hirschmann EAGLE Tofino, Honeywell Modbus Read – only Firewall, Schneider CoiweXium Tofino Firewall) здатний визначати, якого типу повідомлення (читання, запис) і відфільтрувати з'єднання із записом інформації .

Хороший DPI-брандмауер також здатний провести інспекцію повідомлень на предмет їх нестандартного формату або нетипічної поведінки (наприклад, 10 000 повідомлень у відповідь на єдиний запит). Такий трафік характерний для мережевих атак і шкідливого ПЗ і має бути заблокований.

Ще років 5 тому технологія DPI розглядалася як цікаве доповнення до системи. Зараз завдяки поточному поколінню вірусів типу Stuxnet, Duqu, Conficker вона є необхідністю для захищених АСУ і SCADA-систем.

Розробники шкідливого ПЗ знають, що брандмауери і другі засоби мережевої безпеки здатні відфільтрувати недозволений протокол відразу. Якщо в мережі використовуються звичайні протоколи типу HTTP, Modbus і MS-

SQL, то поява нового протоколу відразу зверне на себе увагу системного адміністратора або міжмережевого екрану. Тому розробники шкідливого ПЗ намагаються піти іншим шляхом, використовуючи трафік тих протоколів, які вже використовуються в мережі, що атакується. Наприклад, багато сучасних вірусів ховають свій зовнішній трафік у середині протоколу HTTP так, що зовні його повідомлення виглядають абсолютно звичайно.

Вірус Stuxnet – це відмінний приклад маскування небезпечного ПЗ усередині звичайного протоколу. Він спроектований для функціонування у середині протоколу RPC (Remote Procedure Call) і призначений як для зараження нових жертв, так і для комунікацій в режимі точка-точка між зараженими машинами (рис. 2.13).

RPC – це ідеальний протокол для атаки на АСУ і SCADA-системи, оскільки він широко застосовується в сучасних системах контролю і управління. Для прикладу, технологія OPC (OLE for Process Control), що являється самою використовуваною в промисловій інтеграції об'єктів, базується на технології DCOM (Distributed Component Object Model), яка також базується на протоколі RPC.

Більше того сервери управління і робочі станції зазвичай конфігуруються для спільного використання файлів і принтерів за допомогою протоколу Microsoft SMB, який також передається поверх протоколу RPC. І, можливо, самий показовий приклад – усі контролери Siemens SIMATIC PC S7 і системи на їх основі, які використовують власні протоколи обміну, також передаються поверх протоколу RPC.

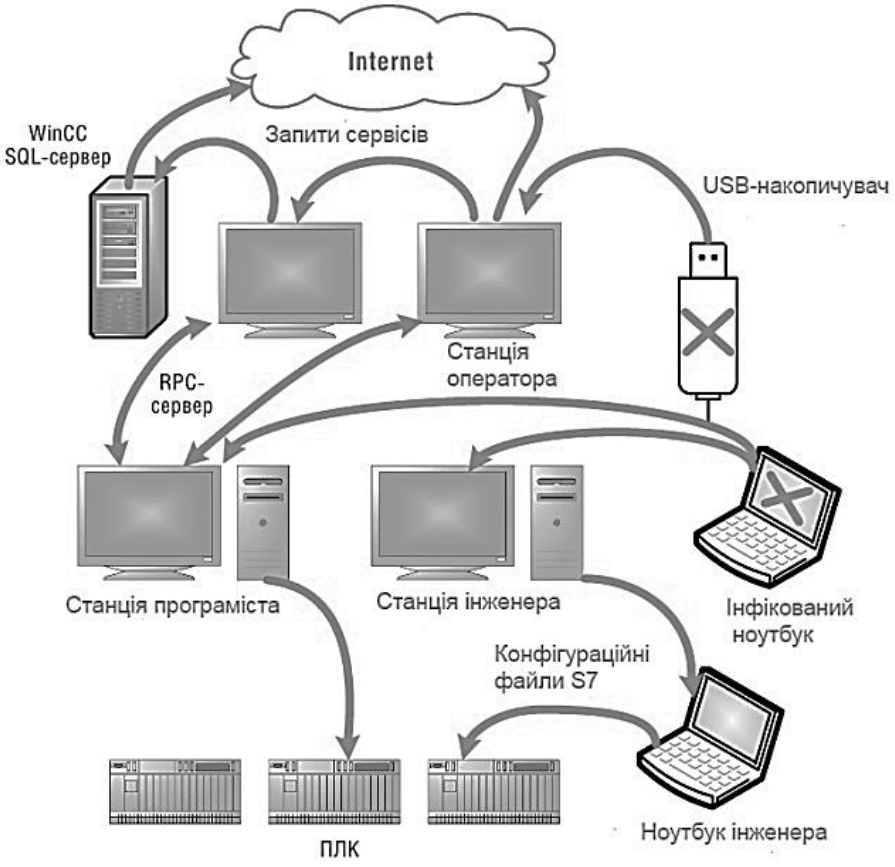

Рисунок 2.13 – Принцип поширення вірусу Stuxnet

Аналізуючи мережі, зараженої вірусом Stuxnet, єдине, що можливо помітити, це – невелике збільшення трафіку RPC, що навряд чи послужило б приводом для тривоги. Навіть якщо б щось і запідозрили, то навряд чи щось виявили, маючи в арсеналі лише стандартний брандмауер. Просте блокування усього RPC-трафіка приведе до зупинки усіх пов'язаних з цим протоколом сервісів на підприємстві. Без засобів аналізу складу трафіку протоколу RPC і блокування паразитного трафіку не вдасться зупинити дію шкідливого ПЗ.

Висновки до розділу 2

Технологія DPI – потужний інструмент в асортименті засобів забезпечення IT-безпеки, який дозволяє виявляти і блокувати шкідливий трафік в системах управління і SCADA-системах. Ця технологія не абстрактна, вона має

цілком конкретну робочу реалізацію у вигляді модульного ПЗ Tofino від Byres Security, що входить в апаратно-програмний комплекс захисту Hirschmann EAGLE Tofino. EAGLE Tofino здатний проводити глибокий аналіз більш ніж 50 промислових протоколів (PROFINET, МЭК 61850, DNP та ін.), аналізувати трафік Modbus TCP і OPC-сервера/клієнта, будувати VPN-тунелі. Програмне забезпечення Tofino включає більше 25 заздалегідь налагоджених профілів безпеки для ПЛК Siemens, VIPA, WAGO і так далі, дозволяючи забезпечити контролери від несанкціонованого втручання в їх програми.

3 АНАЛІТИЧНА І МАТЕМАТИЧНА МОДЕЛІ ТЕХНОЛОГІЇ DPI

3.1 Розробка аналітичної моделі технології DPI

Велику частку інтернет-трафіку займає трафік мереж P2P (Peer - to -Peer) і потокового відео OTT (Over the Top), наприклад, YouTube. Неконтрольованість деяких мережевих сервісів знижує якість обслуговування інших і створює небезпеку перевантаження мережі. Система DPI дозволяє виявити трафік таких сервісів, а потім блокувати або обмежити швидкість передачі даних. Такий підхід дозволяє зменшити темпи постійного розширення мереж і зробити кожне розширення більше передбачуваним [15]. Застосування DPI – перший і необхідний крок для підтримки стабільних мережевих послуг і ефективного управління мережевими ресурсами [16].

Основний метод DPI – перевірка сигнатур протоколів і додатків. Під сигнатурою розуміється шаблон опису даних, який однозначно відповідає додатку/протоколу. Наприклад, це може бути пошук таких ключових слів в даних пакету, як BitTorrent, або запитів GET/POST протоколу HTTP. Прості сигнатури засновані на URL-адресах в заголовку HTTP, а сам файл сигнатур вендора періодично оновлюється. Частина методів DPI заснована на статистичних і поведінкових критеріях аналізу потоку даних. Саме поведінковий аналіз дозволяє виявити сканування портів з одного джерела [17]. У складніших випадках сигнатура заснована на аналізі параметрів пов'язаних потоків одного застосування [18]. Усі ці сигнатури використовуються для виявлення використовуваних потоком додатка IP -адрес і транспортних портів для подальшого контролю над потоком даних: статистики, тарифікації, прослуховування або блокування.

DPI застосовується для відстеження або блокування переговорів з використанням Skype в Китаї і країнах Близького Сходу. Компанія Skype не завжди розкриває дані клієнтів, а DPI дозволяє здійснювати контроль потоків даних і

статистики трафіку в мережі. Серед систем аналізу трафіку на основі вільного програмного забезпечення (open source) можна згадати OpenDPI, Tstat і SPID [19].

Окрім "важкого" трафіку важливим чинником впровадження DPI систем став указ президента України №133/2017 про рішення ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)". Для контролю доступу до вмісту сайтів і блокування трафіку застосовують DPI системи. Аналізуючи трафік на рівні додатків, технологія DPI дозволяє вибірково заблокувати заборонений ресурс по URL адресі без повного блокування сервера компанії хостингу. Такий підхід задовольняє вимозі блокування трафіку на основі доменного імені або поєднанню IP-адреса і адреса, що веде до забороненого контенту. Це вирішує проблему популярного методу блокування забороненого ресурсу за його IP-адресом, коли виявляються недоступними і інші ресурси, що використовують сервер компанії хостингу з тим же IP-адресом. Причому інший метод блокування доменних адрес в службі DNS (Domain Name System) досить просто можна обійти [10].

Для опису системи DPI необхідно заглибиться в питання її архітектури, але воно досить складне і заслуговує окремого розгляду. У рамках даної роботи представимо DPI у вигляді етапів роботи з пакетами, показаними на (рис. 4.1): прийом мережевою картою і фільтрація пакетів, виділення потоків трафіку, вилучення даних пакету (0,3% часу роботи процесора) і завантаження сигнатур з БД (7,6% часу роботи процесора), обробка даних алгоритмами (8,7% часу роботи процесора) і порівняння з сигнатурами (83% часу роботи процесора) під управлінням комбінатора рішень про приналежність потоку до певного класу.

Комбінатор рішень дає алгоритмам початкові дані і вибирає найбільш достовірне рішення [11]. Далі відбувається співвідношення пакету з певним потоком трафіку. У [12] була проведена оцінка відсоткового відношення

необхідного часу роботи процесора для виконання цих етапів, яка показала, що 83% займає етап порівняння даних пакету з сигнатурами.

Якщо на етапі виділення потоків пакет належить існуючому потоку даних, то він передається на апаратний фільтр.

Рисунок 3.1 – Аналіз пакетів DPI з використанням комбінатора рішень

Зазвичай на етапі аналізу даних пакету алгоритмами обробки спочатку проводиться аналіз 2-4-го рівнів і заголовків тунелів, далі відбувається порівняння інформації 5-7-го рівнів з базою сигнатур додатків (що містить більше 1000 прикладів).

Для нового виявленого потоку призначена політика виконується на апаратному фільтрі, в якому (режим розвантаження) не ведеться аналіз 5-7-го рівнів, але робиться підрахунок трафіку для заданого застосування [4].

Окрім режиму аналізу пакетів, що надходять в даний момент, DPI -системи можуть працювати в режимі навчання, в якому аналізуються приклади різнорідних помічених потоків трафіку. Режим навчання має наступні етапи: захоплення пакетів, зчитування міток істинних значень потоків трафіку, отримання сигнатур і запис в базу даних (БД).

Для систем DPI важливо забезпечити задану тривалість обробки пакетів і її стабільність. Також складним завданням виступає підтримка стабільності імовірнісно-тимчасових характеристик в умовах роботи на граничній продуктивності [4].

Зазвичай аналіз і вилучення необхідної інформації вимагають значних обчислювальних ресурсів. Чим вони вищі, тим менше буде тривалість обробки пакетів, а значить, менше буде величина затримки проходження нового потоку даних через систему DPI. Крім того, робота апаратного фільтру також вносить певну затримку при проходженні пакетів. Якщо навантаження на систему DPI почне перевищувати певний поріг, то це приведе до збільшення затримки, втрати пакетів і в крайньому випадку – до пропуску трафіку без його аналізу.

Щоб оцінити доцільність застосування технології DPI для забезпечення QoS, необхідно розробити її математичну модель. Це дозволить з'ясувати, наскільки впровадження DPI дозволить підвищити параметри QoS за рахунок точного визначення типів трафіку для диференційованого обслуговування і обмеження потоків "важкого" трафіку, а також дізнатися, яку ціну, у величині виникаючої затримки і втратах пакетів, доводиться платити при використанні DPI.

В якості першої системи масового обслуговування ($СМО_1$) позначимо багатопроцесорний сервер аналізу трафіку з чотирма опрацьовувачами. За класифікацією Кендалла M/M/V означає систему з пуасонівським вхідним потоком заявок, експоненціальним законом розподілу часу обслуговування і V – опрацьовувачами. Припущення, що сумарний вхідний потік на сервер аналізу трафіку пуассонівський, засноване на його великому числі незалежних стаціонарних потоків [12]. Наступна $СМО_2$ – це сервер ухвалення рішень про застосування політики з одним опрацьовувачем (M/M/1). Аналогічно, використовуючи теорему Берка, можна зробити висновок, що потік, який поступає на сервер ухвалення рішень теж пуасонівський, але відрізняється від початкового з

ймовірністю настання випадку звернення до цього сервера. Позначимо інтенсивність простого потоку, що входить, через λ.

Отримаємо модель, показану на (рис. 3.2).

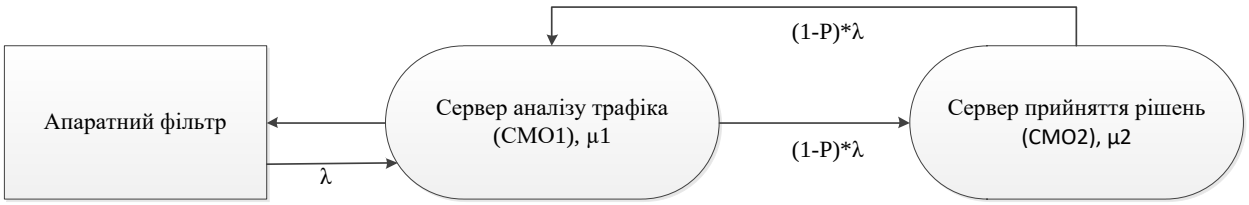

Рисунок 2.2 – Спрощена аналітична модель системи DPI

3.2 Розробка математичної моделі технології DPI

Для побудови простої математичної моделі, що представляє систему масового обслуговування (СМО), треба ще раз спростити етапи обробки трафіку системою DPI. Допустимо, що сервер аналізу трафіку використовує тільки перший пакет потоку, що поступає з апаратного фільтру, і по ньому визначає необхідну політику і передає далі на апаратний фільтр. Позначимо середню затримку пакету при аналізі як T_1. Проте в деяких випадках сервер аналізу трафіку посилає запит на необхідну політику у сервера ухвалення рішень про застосування політики. У такому разі середня затримка (T_2) буде сумою затримок в чергах і затримок обробки на сервері ухвалення рішень і двічі сервера аналізу трафіка.

Відповідно до теореми Берке, що виходить із $СМО_2$ (що працює в стаціонарному режимі) потік буде простим з тим же параметром λ. Інтенсивність вхідного потоку на $СМО_2$ дорівнюватиме:

$$\lambda_{вх2} = (1-P)\lambda \ , \qquad (3.1)$$

де P - ймовірність самостійної класифікації нового потоку сервером аналізу трафіку ($СМО_1$). Аналогічно для $СМО_2$. При цьому необхідно враховувати, що вимоги, які надійшли після обробки із $СМО_2$, також потраплятимуть в чергу $СМО_1$.

Таким чином, інтенсивність вхідного потоку на $СМО_1$ після обробки $СМО_2$ дорівнюватиме:

$$\lambda_{вх12} = (1-P)\lambda \ , \tag{3.2}$$

В результаті загальна інтенсивність надходження пакетів на сервер аналізу трафіку ($СМО_1$) визначається виразом:

$$\lambda_{вх1} = \lambda + (1-P)\lambda \ , \tag{3.3}$$

Продуктивність $СМО_1$ визначається як:

$$p_1 = \frac{\lambda + (1-P)\lambda}{\mu 1} , \tag{3.4}$$

де p_1 – інтенсивність обслуговування пакетів. Ймовірність того, що система вільна (P_0), може бути отримана за формулою:

$$P_0 = \frac{1}{\frac{{p_1}^{n+1}}{n! \cdot (n - p_1)} + \sum_{n=0}^{n} \frac{{p_1}^{n}}{n!}} , \tag{3.5}$$

де n=4 – число опрацьовувачів.

Середню затримку сервера аналізу трафіку (T_1) можна отримати на основі числа заявок в системі (N_1), залежного від середнього числа заявок в черзі (NS):

$$NS = \frac{p_1^{n+1} p_0}{nn!(1-\frac{p_1}{n})^2}, \tag{3.6}$$

$$N_1 = NS + p_1, \tag{3.7}$$

$$T_1 = \frac{N_1}{\lambda + (1-P)\lambda} \tag{3.8}$$

Знаючи інтенсивність надходження пакетів на сервер ухвалення рішень ($СМО_2$) – $\lambda_{вх2}$, можна отримати наступні характеристики для $СМО_2$: продуктивність (p_2) середнє число заявок в системі (N_2), середню затримку сервера ухвалення рішень (T_2), розрахунок яких проводиться за формулами:

$$p_2 = \frac{(1-P)\lambda}{\mu_2}, \tag{3.9}$$

$$N_2 = \frac{p_2}{1-p_2}, \tag{3.10}$$

$$T_2 = \frac{N_2}{(1-P)\lambda} = \frac{1}{\mu_2(1-p_2)} \tag{3.11}$$

Загальний час, необхідний системі DPI на визначення потоку і політики (T), складає:

$$T = T_1 + P(T_1 + T_2) \tag{3.12}$$

На підставі наведених вище формул визначена залежність затримки в такій системі від інтенсивності навантаження (рис. 3.3), при вибраній

ймовірності звернення до сервера ухвалення рішень $P = 0{,}8$ і інтенсивностями обслуговування заявок $\mu_1 = 5000$, $\mu_2 = 1000$ на СМО 1 і 2 відповідно.

В результаті розрахунків на основі зразкової математичної моделі роботи системи DPI можна стверджувати, що при збільшенні інтенсивності вхідних потоків зростає загальний час для визначення політики для кожного потоку пакетів. Отримана середня затримка системи DPI (1,2 мс без пікового завантаження, 22,8 мс з піковим завантаженням) дозволяє застосовувати технологію DPI для чутливого до затримок трафіку, як це можна бачити з вимог рекомендації Y.1541 Міжнародного союзу електрозв'язку (ITU – T) від 0,1 до 1 с. [14].

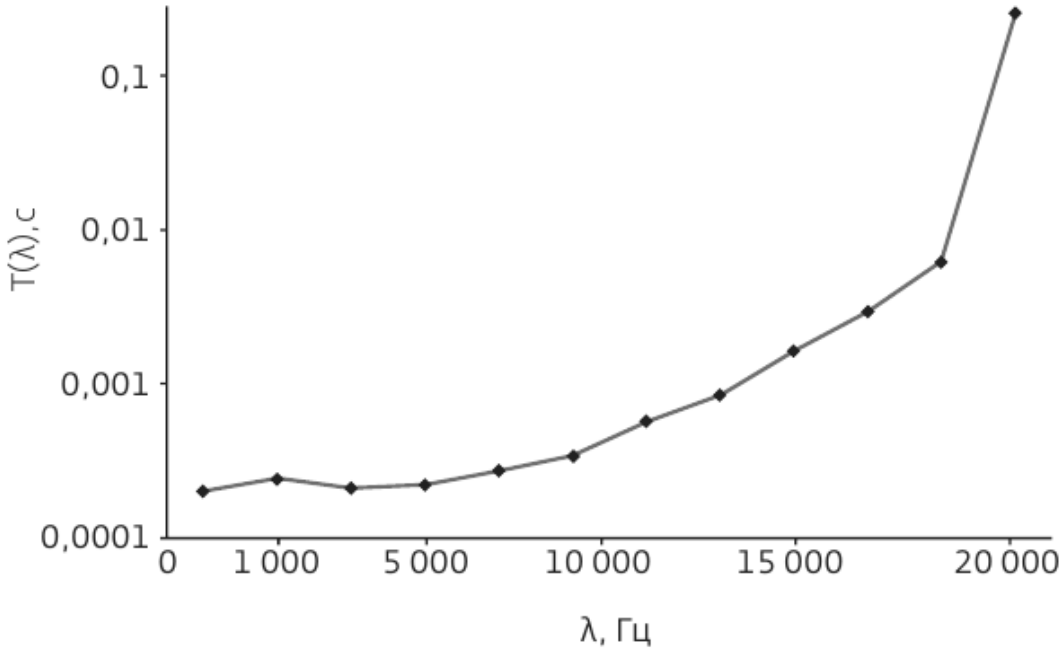

Рисунок 3.3 – Залежність затримки, яка виникає в системі DPI від λ

Проте при піковому завантаженні система показала незадовільну затримку, рівну 260 мс. З урахуванням того, що затримка передачі пакету в мережі складається з часу на подолання відстані, часу на обробку пакетів маршрутизаторами, комутаторами і двох систем DPI (у мережі оператора, який постачає

трафік, і в мережі іншого оператора, який цей трафік приймає). Зрозуміло, що для системи DPI затримки при обробці пакетів мають бути мінімальними. Проте не варто вважати ці результати остаточними, оскільки в цій математичній моделі було зроблено велику кількість допущень.

3.3 Способи обходу технології DPI

На даний момент самим ефективним способом обходу різних блокувань з боку провайдера є VPN, а саме OpenVPN. Але з часом провайдери таки введуть в дію DPI. Найбільш простий спосіб виявлення і блокування OpenVPN трафіка — моніторинг стандартних OpenVPN портів і їх блокування. Найчастіше блокуються 1194-й UDP порт. Боротися з такого роду блокуваннями нескладно. Зазвичай допомагає конфігурація OpenVPN на використання 443-го порту, зашифрований трафік на якому не повинен викликати ні у кого ніяких підозр — на ньому працює HTTPS. Та і крім того, OpenVPN, як і HTTPS, використовує SSL шифрування, тому відрізнити HTTPS і OpenVPN трафік на 443-му порту дуже складно. Але SSL шифрування в OpenVPN трохи відрізняється від того, що використовується в HTTPS, і тому пристрої DPI зможуть виявити цю різницю. У такому разі застосовують утиліту obfsproxy. Хоча і розробляється ця утиліта командою Tor, вона є незалежним продуктом і легко конфігурується для використання разом з OpenVPN. Принцип дії останньої утиліти полягає в обертанні трафіку в новий шар, наприклад в звичайні HTTP пакети. Таким чином, OpenVPN-трафік може спокійно пройти непоміченим повз провайдера (рис. 3.4).

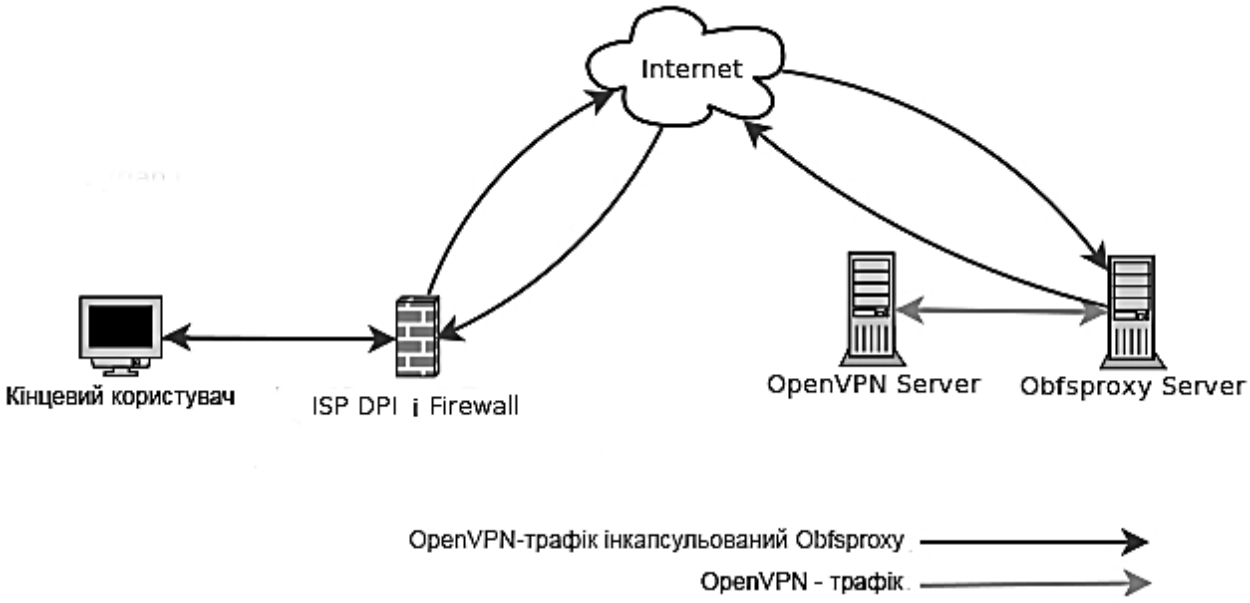

Рисунок 3.4 – Схема проходження інкапсульованого OpenVPN-трафіку

Але бувають пристрої DPI, які можуть виявити і такий трафік. У такому разі OpenVPN-трафік пропускається через SSL-тунель. Додатковий шар шифрування не дозволить ніякому DPI добратися до OpenVPN-трафіку і, відповідно, детектувати його. Для підняття SSL-тунеля використовується утиліта stunnel. Такий спосіб має один мінус — із-за додаткового шару шифрування швидкість передачі знижується.

ВИСНОВКИ

В роботі розглядалося питання ефективності застосування технології Deep Packet Inspection. В першому розділі були проаналізовані механізми анонімності в мережі Інтернет, які актуальні на даний момент, для того щоб розуміти з чим можна буде зіткнутися при впровадженні технології глибокого аналізу пакетів. У кожного із проаналізованих механізмів є свої переваги та недоліки, а проблема анонімності зводиться до вибору між оверлейними (overlay) мережами та децентралізацією із застосуванням криптографії в обох випадках. Застосування децентралізованих механізмів дає змогу повністю ліквідувати серверну частину, а для того, щоб «зламати» мережу й демаскувати дані, потрібно скористатися технологіями аналізу трафіку, зокрема Deep Packet Inspection.

Незважаючи на те, що нині існує достатньо способів залишатися анонімним в Інтернет-мережі, досягнення абсолютної анонімності неможливе – практично у будь-якій ситуації можна дібрати технічні засоби для ідентифікації користувача, бо єдиною перешкодою для цього є матеріальні ресурси і час.

Варіантів використання DPI дуже багато, можливо реалізувати будь-які ідеї і задачі відносно мережевого трафіку, це ще раз підтверджує багатогранність технології DPI і актуальність її впровадження.

Технологія DPI – потужний інструмент в асортименті засобів забезпечення IT-безпеки, який дозволяє виявляти і блокувати шкідливий трафік в системах управління і SCADA-системах. Апаратно-програмний комплекс захисту Hirschmann EAGLE Tofino. EAGLE Tofino здатний проводити глибокий аналіз більш ніж 50 промислових протоколів (PROFINET, МЭК 61850, DNP та ін.), аналізувати трафік Modbus TCP і OPC-сервера/клієнта, будувати VPN-тунелі.

Також, в дипломній роботі предствлена спрощена аналітична та математична моделі систем DPI та результати розрахунків на основі яких можна

стверджувати, що при збільшенні інтенсивності вхідних потоків зростає загальний час для визначення політики для кожного потоку пакетів. Отримана середня затримка системи DPI (1,2 мс без пікового завантаження, 22,8 мс з піковим завантаженням) дозволяє застосовувати технологію DPI для чутливого до затримок трафіку.

Проте при піковому завантаженні система показала незадовільну затримку, рівну 260 мс. З урахуванням того, що затримка передачі пакету в мережі складається з часу на подолання відстані, часу на обробку пакетів маршрутизаторами, комутаторами і двох систем DPI (у мережі оператора, який постачає трафік, і в мережі іншого оператора, який цей трафік приймає). Для високонавантежених систем потрібно проводити або масштабування обладнання або оптимізацію трафіку.

Також, розглянуте питання методів обходу блокувань системою DPI, які ще актуальні на даний час, OpenVPN-трафік проходить обфускацуію та пропускається через SSL-тунель. Додатковий шар шифрування не дозволить DPI добратися до OpenVPN-трафіку і, відповідно, детектувати його. Такий спосіб має один мінус — із-за додаткового шару шифрування швидкість передачі знижується.

Хоча систему DPI можливо обійти, але важливо усвідомити, що анонімність впирається в засоби: матеріальні ресурси і час, які можуть бути затрачені на їх компрометацію, тому краще дану технологію розглядати зі сторони захисту мережевого трафіку і блокуванню заборонених ресурсів, а ніж як її обходити. За технологією DPI майбутнє, так як питання дотримання авторських прав, питання протидії кіберзлочинам набувають значущості в Україні.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. FBI: We need wiretap-ready Web sites – now: (Електронний ресурс) / Product reviews and prices, software downloads, and tech news – CNET. Режим доступу: www/ URL: http://news.cnet.com/8301-1009_3–57428067-83/fbi-we-need-wiretap-ready-web-sites-now/.

2. Why Do People Seek Anonymity on the Internet? Informing Policy and Design: (Електронний ресурс) / Ruogu Kang, Stephanie Brown, Sara Kiesler. Режим доступу: www/ URL: http://www.cs.cmu.edu/~xia/ resources/Documents/kang-chi13.pdf.

3. Anonymity on the Internet Must be Protected: (Електронний ресурс) / Karina Rigby // Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1995. Режим доступу: www/ URL: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/rigby-anonymity.htmI.

4. Anonymity on the Internet: (Електронний ресурс) / Jacob Palme, Mikael Berglund. Режим доступу: www/ URL: http://people.dsv.su.se/~jpalme/society/anonymity.html.

5. Методи анонимности в сети. Часть 1. Просто о сложном: (Електронний ресурс) / Режим доступу: www/ URL: http://habrahabr.ru/post/190396/.

6. Надежние и безопасние сети?! : (Електронний ресурс) / Скрипников Сергей // Спецвипуск Хакер, номер #041. Режим доступу: www/ URL: http://www.xakep.ru/magazine/xs/041/030/Lasp.

7. Secure Shell: (Електронний ресурс) / Wikipedia - the free encyclopedia. Режим доступу: www/ URL: http://en.wikipedia.org/wiki/Secure_Shell.

8. Quang Hieu Vu, Mihai Lupu, Beng Chin Ooi. Peer-to-Peer Computing: Principles and Applications. 2010. 336 Pages.

9. Децентрализация: Какие сервиси уже есть? : (Електронний ресурс) /

Режим доступу: URL: http://habrahabr.ru/post/212653/.

10. Анонимность в сети Интернет : (Електронний ресурс) // Компьютер-Пресс 9/2010. Режим доступу: www/ URL: http://www.compress.ru/article.aspx?id=21613&iid=987.

11. Introducing I2P : (Електронний ресурс). Режим доступу: www/ URL: http://geti2p.net/en/docs/ how/ tech-intro

12. Statistics website for the I2P network : (Електронний ресурс). Режим доступу: URL: http://i2pstats.loria.fr/?sect=historical&subsect_hist=routers.

13. Tor: Overview: (Електронний ресурс) / Режим доступу: URL: https://www.torproject.org/about/overview.html.en.

14. Включаем Tor на всю катушку : (Електронний ресурс) / Антон Жуков. Режим доступу: www/ URL: http://www.xakep.ru/post/50516/.

15. Дубчук Н.В. DPI - хранитель сети ШПД или окончание эры свободного Интернета? // Вестник связи. 2012. № 5. С. 11-12.

16. Сибгатулин М. DPI. Информационно-аналитический портал NAG.ru, (Электрон¬ный ресурс). Код доступа: http://nag.ru/articles/ article/22432/dpi.html/.

17. Сенченко Ю.Х. Некоторые аспекты высокоскоростной обработки трафика // Технологии и средства связи. 2013. № 1. С. 52-53.

18. Dorfinger P., Panholzer G., John W. Entropy Estimation for Real-Time Encrypted Traffic Identification // III international workshop "Traffic Monitoring and Analysis", Berlin: Springer. 2011. PP. 164-171.

19. ITU-T Recommendation Y.1541: Network performance objectives for IP-based services (2006).