15. Филаретов, В. Ф. Устройства и системы управления подводных роботов [Текст] / В. Ф. Филаретов, А. В. Лебедев, Д. А. Юхимец // [отв. ред. Ю.И. Кульчин] ; Инс-т автоматики и процессов управления ДВО РАН. – М.: Наука, 2005. – 270 с.
16. Блінцов, С. В. Автоматичне керування автономними підводними апаратами в умовах невизначеності : Монографія [Текст] / С. В. Блінцов // – Миколаїв : ТОВ "Фірма "Іліон", 2008. – 204 с.
17. Moore, S. Underwater Robotics: Science, Design & Fabrication [Text] / Steven W. Moore, Harry Bohm, Vickie Jensen // - Publisher: Marine Advanced Technology Education (MATE) Center, 2010. – 770 p.
18. Бабак, Л. Н., Об одном алгоритме поиска источника подводного шлейфа, основанном на использовании группы АНПА [Текст] / Л. Н. Бабак, А. Ф. Щербатюк // Управление большими системами : Сборник трудов. - 2010. – Специальный выпуск №30.1 «Сетевые модели в управлении». – С. 536-548.
19. Иванов, А. И. Сетецентрические аспекты группового поведения автономных подводных аппаратов [Текст] / А. И. Иванов, Н. А. Лазутина, И. У. Сахабетдинов // Технические и программные средства систем управления, контроля и измерения : Труды 3-й Всероссийской конференции с международным участием. – М.: Институт проблем управления РАН, 2010. – С. 548-551.
20. Toshiyuki, Yasuda Multi-robot systems, trends and development [Text] / Toshiyuki Yasuda, Kazuhiro Ohkura // - InTech, India, 2011. – 596 p.
21. Ильюшко, В. М. Беспилотные летательные аппараты : Методики приближенных расчетов основных параметров и характеристик [Текст] / В. М. Ильюшко, М. М. Митрахович, А. В. Самков, В. И. Силков, О. В. Соловьев, В. И. Стрельников // [под общ. Ред. В. И. Силкова] – К.: ЦНИИ ВВТ ВС Украины, 2009. 302 с.
22. Городецкий, В. И. Прикладные многоагентные системы группового управления [Текст] / В. И. Городецкий, О. В. Карсаев, В. В. Самойлов, С. В. Серебряков // «Искусственный интеллект и принятие решений» - 2009. –№2. – С. 3-24.

Проводиться аналіз підходів до вирішення задачі моніторингу мережевого трафіку та обробки його результатів. Розглядаються сучасні мережеві системи та проблеми, які виникають при дослідженні їх стану. В результаті аналізу існуючих методів дослідження мережевих систем запропоновано використання методу прослуховування мережевого інтерфейсу як способу дослідження мережевих систем для подальшого адміністрування системи

Ключові слова: сніфер, мережеві системи, адміністрування

Проводится анализ подходов к решению задачи мониторинга сетевого трафика и обработки его результатов. Рассматриваются современные сетевые системы и проблемы, возникающие при исследовании их состояния. В результате анализа существующих методов исследования сетевых систем предложено использование метода прослушивания сетевого интерфейса как способа исследования сетевых систем для дальнейшего администрирования системы

Ключевые слова: снифер, сетевые системы, администрирование

УДК 004.457

АНАЛІЗ ПІДХОДІВ ДО ВИРІШЕННЯ ЗАДАЧІ МОНІТОРИНГУ ТРАФІКУ МЕРЕЖЕВИХ КОМУНІКАЦІЙ ТА ОБРОБКА ЙОГО РЕЗУЛЬТАТІВ

Р. Б. Скрип'юк
Кандидат технічних наук, доцент
Кафедра комп'ютерних технологій
в системах управління і автоматики
Івано-Франківський національний
технічний університет нафти і газу
вул. Карпатська 15, м. Івано-Франківськ,
Україна, 76000
E-mail: rostyslav.skrypyuk@gmail.com

1. Вступ

Важко переоцінити роль комп'ютерних мереж для сучасного світу. Розвиток цієї області IT індустрії розвивається надзвичайно швидко, намагаючись вгамувати постійно зростаючий попит на швидкий та якісний зв'язок з глобальною мережею Internet. Саме тому існує потреба у розробці спеціалізованого програмного забезпечення (сніферів), яке б спростило роботу системним адміністраторам у відлагодженні

мереж та дозволило б менш компетентним у цій сфері спеціалістам почати виконувати такого роду роботу.

Сніфери - це програми, які перехоплюють весь мережевий трафік. Сніфери корисні при проведенні діагностики мережі. Сніфери переводять мережеву карту в режим прослуховування (PROMISC), тобто вони отримують всі пакети, що проходять через неї [1]. Сніфери можуть перехоплювати всі пакети, крім того, в налаштуваннях багатьох сніферів можна задавати фільтрацію окремих пакетів.

Логічно стверджувати, що снiфінг - це сукупність заходів з перехоплення мережевого трафіку. У рамках конкретного продукту може бути реалізована функція по захопленню пакетів (packet capturing).

2. Аналіз літературних даних та існуючого досвіду

Основним принципом роботи будь-якої мережі є семирівнева модель OSI.

Еталонна модель OSI, яку деколи називають стеком OSI, являє собою 7-рівневу мережеву ієрархію, розроблену Міжнародною Організацією по Стандартах (International Standardization Organization - ISO). Ця модель містить у собі по суті 2 різних моделі:

1. Горизонтальну модель на базі протоколів, що забезпечує механізм взаємодії програм і процесів на різних машинах.

2. Вертикальну модель на основі послуг, забезпечуваних сусідніми рівнями один одному на одній машині.

У горизонтальній моделі двом програмам потрібен загальний протокол для обміну даними. У вертикальній - сусідні рівні обмінюються даними з використанням інтерфейсів API [2]. На рис. 1 зображена загальна схема роботи моделі.

Фізичний рівень (Physical layer) - нижній рівень моделі, призначений безпосередньо для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів в кабель або в радіоефір і, відповідно до цього, їх прийом і перетворення в біти даних методами кодування цифрових сигналів.

Канальний рівень (Data Link layer) - рівень мережевої моделі OSI, призначений для передачі даних вузлам, що знаходяться в тому ж сегменті локальної мережі.

Протокол мережевого рівня (Network layer) - протокол 3-го рівня мережевої моделі OSI, і його призначення - це визначення шляху передачі даних. Відповідає за трансляцію логічних адрес та імен у фізичні, визначення найкоротших маршрутів, комутацію і маршрутизацію, відстеження неполадок і заторів у мережі.

Транспортний рівень (Transport layer) - 4-й рівень мережевої моделі OSI призначений для доставки даних. При цьому не важливо, які дані передаються, звідки й куди, тобто він надає сам механізм передачі.

Сеансовий рівень (Session layer) - 5-й рівень мережевої моделі OSI, відповідає за підтримання сеансу зв'язку, дозволяючи додаткам взаємодіяти між собою тривалий час. Рівень управляє створенням та завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди не активності додатків.

Представницький рівень (Presentation layer) - шостий рівень мережевої моделі OSI. Цей рівень відповідає за перетворення протоколів і кодування/декодування даних. Запити додатків, отримані з рівня додатків, він перетворить у формат для передачі по мережі, а отримані з мережі дані перетворить у формат, зрозумілий додаткам.

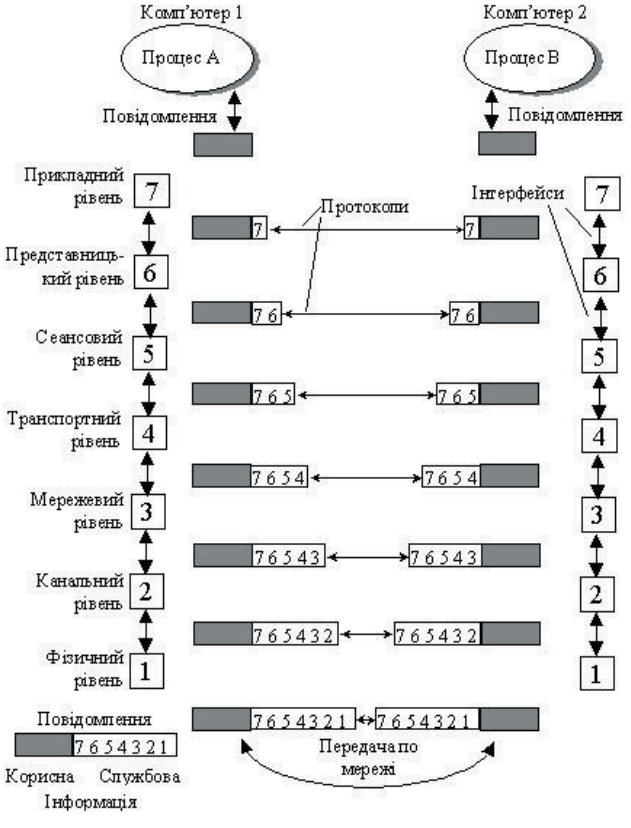

Рис. 1. Загальна схема роботи 7-ми рівневої моделі OSI

Протокол прикладного рівня (Application layer) - протокол верхнього (7-го) рівня мережевої моделі OSI, забезпечує взаємодію мережі й користувача. Рівень дозволяє додаткам користувача мати доступ до мережевих служб, таких як обробник запитів до баз даних, доступ до файлів, пересиланню електронної пошти. Також відповідає за передачу службової інформації, надає додаткам інформацію про помилки і формує запити до рівня подання.

Питаннями досліджень трафіку мережевих комунікацій займаються багато науковців та спектр напрямів досліджень дуже широкий: це й дослідження кореляцій між сигналами [4, 5], й заходи щодо вибору параметрів при побудові профілів захисту інформаційних ресурсів [6 – 8], й питання захисту інформаційних ресурсів при передачі даних по мережах [9 – 13]. Але в усіх цих питаннях залишається актуальною проблема аналізу трафіку мережевих комунікацій з можливістю аналізу статистичних даних, що отримує система в процесі моніторингу.

3. Мета дослідження, постановка задачі

Об'єктом дослідження є система автоматизації обліку та аналізу трафіку мережевих комунікацій, тобто

мережевий сніфер з можливістю аналізу отриманих статистичних даних. Суть роботи системи полягає в тому, що вона перехоплює пакети, що надсилаються в мережу через один з мережевих пристроїв, вибирає з них необхідну інформацію і робить записи про їх проходження.

4. Підхід до моніторингу трафіку мережевих комунікацій

Після створення запису системою, вона пересилає пакет далі в мережу. Запис про проходження пакету повинен включати в себе наступну інформацію [14]:

1. Час створення запису відносно початку прослуховування.
2. IP-адреса відправника пакета.
3. Номер порту відправника пакета.
4. IP-адреса отримувача пакета.
5. Номер порту отримувача пакета.
6. Кількість байт інформації що передана.
7. Тип транспортного протоколу.

Система також повинна надати можливість користувачу вибору одного з існуючих мережевих інтерфейсів в разі наявності декількох мережевих адаптерів.

До кожного з них повинен виводитись опис. Також користувач повинен бути в змозі призупинити, продовжити процес обліку пакетів з мережі.

Необхідно розробити механізм, який дозволить робити побудову графіків з аналітичною інформацією про стан мережі в час, коли прослуховування мережі призупинено чи зупинено зовсім. Розроблена система не повинна відчутно впливати на швидкодію мережевого адаптера, а також забирати багато процесорного часу.

Основною задачею програмного продукту повинен бути аналіз результатів прослуховування мережевого адаптера та виведення їх в графічному вигляді. Основні види графіків, що будуть будуватися:

1. Кількість пакетів, переданих від даної IP адреси в різні проміжки часу.
2. Кількість пакетів, переданих до даної IP адреси в різні проміжки часу.
3. Кількість TCP пакетів, переданих від даної IP адреси в різні періоди.
4. Кількість UDP пакетів, переданих від даної IP адреси в різні періоди.
5. Кількість TCP пакетів, переданих до даної IP адреси в різні періоди.
6. Кількість UDP пакетів, переданих до даної IP адреси в різні періоди.

Очевидним є те, що система матиме графічний інтерфейс користувача, основною ціллю якого є інтуїтивність та доступність. Для старту, зупинки чи призупинення повинні бути наявні графічні елементи інтерфейсу. Також потрібні елементи, такі як edit box, в яких можна вказати опції фільтрації трафіку. Необхідною є можливість збереження результатів роботи системи.

Метою функціонування системи є ведення обліку мережевого трафіку, який проходить через певний мережевий інтерфейс. Облік трафіку буде проводитись за певними критеріями, встановленими користувачем. Підсистема фільтрації мережевого трафіку займатиметься власне відкиданням мережевих пакетів (фреймів), які не цікавлять користувача. Подальше управління буде передано підсистемі збереження результатів, яка зберігатиме пакети, які підходять під критерії, встановлені користувачем перед початком ведення моніторингу мережевого трафіку. За потреби ця підсистема може передати збережені дані підсистемі обробки результатів, яка саме займатиметься аналізом результатів моніторингу і виведенням графічного зображення його аналізу. Зв'язок між цими підсистемами відбуватиметься за допомогою інтерфейсу, що визначатиме функціонал, достатній для виконання завдань, поставлених на даний модуль (підсистему).

Є декілька аспектів функціонування даної підсистеми:

1. Середовище виконання. Середовищем виконання, де буде працювати система, повинні бути стаціонарні комп'ютери, здатні до мережевих комунікацій.

2. Аспект аналізу:

a) Відбір параметрів фільтрації. Для збільшення зручності системи у її використанні користувачу буде надано можливість вказати додаткові параметри фільтрації.

b) Генерування аналітичних графіків. Система генеруватиме графіки, що показуватимуть завантаженість мережі, а також окрему частку навантаження, яке отримує мережа від окремої мережевої точки.

На рис. 2 зображено схему перетворення даних в системі.

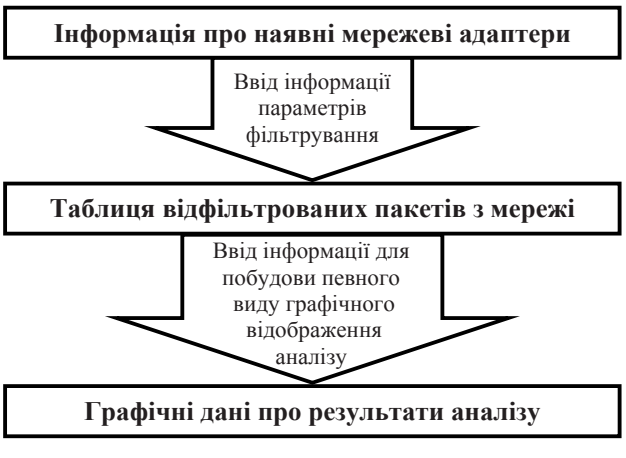

Рис. 2. Схема перетворення даних в системі

Вхідними даними для нашої системи є всі доступні на даний момент часу мережеві інтерфейси, які будуть показані користувачеві для вибору одного з них та налаштування користувачем відповідного фільтру для прослуховування мережевих пакетів певного типу.

Саме ці дані є необхідні для системи, щоб повернути таблицю відфільтрованих пакетів, яка, в свою чергу, може служити вхідними даними для побудови різного виду графіків. Після отримання сигналу до побудови графіків, та при потребі – додаткових уточнюючих даних від користувача, система будує графік, який відображає результати аналізу відфільтрованого трафіку.

Для зручного супроводу, а також для гнучкості програми, доцільно забезпечити слабку зв'язність між компонентами, максимально розмежувавши їх. З даних міркувань систему можна розділити на підсистеми [15]:

1. Підсистема перехоплення мережевих пакетів – забезпечує прослуховування мережевого інтерфейсу, і передає дані наступним підсистемам для обробки.

2. Підсистема фільтрації пакетів передає пакет підсистемі зберігання відфільтрованого трафіку, в залежності від того, чи підходить він під встановлені користувачем критерії.

3. Підсистема зберігання відфільтрованого трафіку займається збереженням даних, які користувач отримав внаслідок фільтрації трафіку.

4. Підсистема обробки інформації, поділена на дві компоненти:

a) компонента аналізу отриманих результатів робить висновки відповідно до результатів, які ми отримали після фільтрування;

b) компонента графічного відображення займається побудовою графіків для унаочнення отриманих висновків про функціонування мережі.

5. Також необхідно врахувати підсистеми модулів, такі як WinPcap та Qt. Вони надають базові можливості для взаємодії системи з мережевим інтерфейсом, чи пристроями вводу-виводу, операційною системою.

На рис. 3 зображена загальна структура системи. Прямокутники зображають окремі підсистеми. Деякі з них можуть містити в собі компоненти.

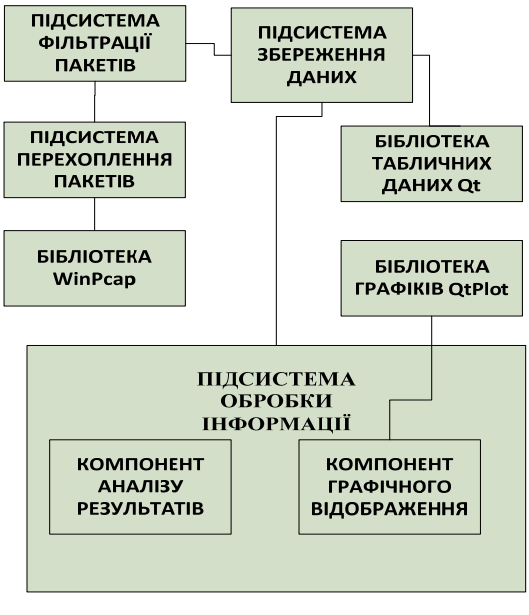

Рис. 3. Структура системи

На рис. 4 зображена діаграма, що ілюструє варіанти використання системи.

З огляду на проведений аналіз проекту, було вирішено для розв'язання поставлених задач обрати найбільш ефективні, швидкі алгоритми, оскільки розроблена програма має підвищені вимоги до точності виконання, можливості перехоплення всіх без винятку пакетів в мережі.

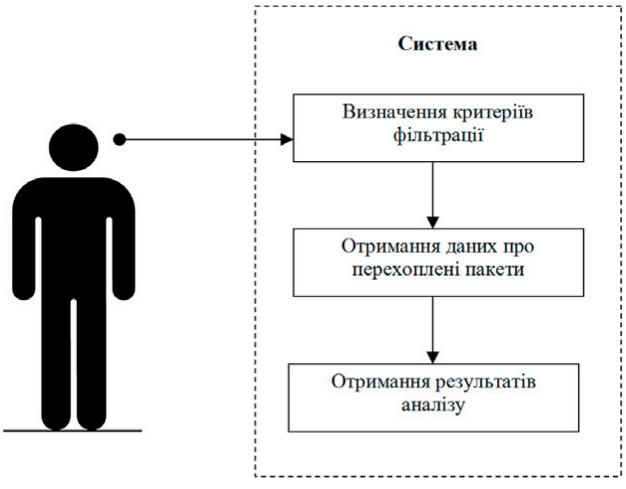

Рис. 4. Діаграма варіантів використання системи

В якості середовища виконання програми вирішено обрати платформу Qt – це програмна технологія, призначена для створення додатків, які виконуються Windows, Unix системах. Включає в себе всі основні класи, які можуть знадобитися при розробці прикладного програмного забезпечення, починаючи від елементів графічного інтерфейсу і закінчуючи класами для роботи з мережею, базами даних і XML. Qt є повністю об'єктно-орієнтованим, легко розширюваним і підтримує техніку компонентного програмування. Для реалізації функцій, що працюють безпосередньо з мережевим адаптером було вирішено обрати бібліотеку WinPcap, яка значно спрощує розробку та впровадження нової системи. На даний момент існує велика кількість спеціалізованого програмного забезпечення для реалізації моніторингу трафіку мережевих комунікацій. Проте кожній системі притаманні певні недоліки, які не здатні забезпечити всі вимоги що розглядаємо. Основними з них є:

Tcpdump – утиліта UNIX, що дозволяє захоплювати і аналізувати мережевий трафік, що проходить через комп'ютер, на якому запущена ця програма. Програма складається з двох основних частин: частини захоплення пакетів (звернення до бібліотеки, libcap (Linux) або pcap (Windows)) і частини відображення захоплених пакетів (яка на рівні вихідного коду є модульною і для підтримки нового протоколу досить додати новий модуль). Основний недолік даної програми – це використання виключно консольного інтерфейсу, що робить її використання незручним для більшості користувачів.

Wireshark (попередня назва Ethereal) – програма для аналізу мережевих пакетів з Ethernet та інших мереж (сніфер). Має графічний інтерфейс користувача. Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, проте Wireshark має графічний інтерфейс користувача і значно більше можливостей із сортування і фільтрації інформації. До недоліків цієї програми можна віднести відсутність детального аналізу отриманої інформації, ця система орієнтована на досвідчених спеціалістів.

ETTERCAP - це сніфер, який працює як під управлінням Linux, так і багатьох інших систем. Об'єднує в собі як функції сніфера, так і деякого мережевого засобу з набором корисних можливостей. Має всі базові

функції сніфера, а також безліч оригінальних, таких як завдання різних режимів роботи для найменшої імовірності виявлення себе в мережі, підтримка плагінів і наявність власного інтерфейсу для їх розробки. Вагомим недоліком є те, що відсутня підтримка інших пристроїв, крім Ethernet інтерфейсів.

Проведений аналіз систем аналогів, які мають ряд недоліків, основними з яких є наявність виключно консольного інтерфейсу, складність у використанні через підвищені вимоги до знань користувача в області мережевих технологій. Деякі з них підтримують виключно Linux системи, що робить їх непридатними для використання на більшості стаціонарних комп'ютерів. Розглянуті системи не мають реалізованої побудови графічних результатів, що могло б стати доволі цінним інструментом при дослідженні мереж.

Саме тому існує потреба у розробці спеціалізованого програмного забезпечення, яке б спростило роботу системним адміністраторам у підлагоджені мереж та дозволило б менш компетентним у цій сфері спеціалістам почати виконувати такого роду роботу.

5. Висновки

Здійснено аналіз об'єкту проектування - системи автоматизації обліку та аналізу трафіку мережевих комунікацій.

Проведено аналіз систем аналогів, в результаті якого було виявлено ряд недоліків. Проведений аналіз вхідних та вихідних даних системи на основі яких побудована відповідна схема та структура системи.

Розглянуто основні середовища виконання програми, на основі чого було здійснено вибір найбільш оптимального програмного середовища для вирішення даної проблематики.

Також зроблено декомпозицію системи на підсистеми, проаналізовано варіанти використання системи.

В результаті чого було сформульовано технічне завдання для розробки спеціалізованого програмного забезпечення для вирішення проблеми моніторингу трафіку мережевих комунікацій та обробки його результатів.

Література

1. Медведовский, И. Д. Атака на Internet [Текст] / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов // М.: ДМК, 2000. – 476 с.
2. Буров, Є. В. Комп'ютерні мережі [Текст] / Є. В. Буров // Львів: «Магнолія 2006», 2006. – 563 с.
3. Политанский, Р. Л. Исследование зависимости корреляции между несущим и информационным сигналом в системах с динамическим хаосом / Р. Л. Политанский, Л. Ф. Политанский, С. Д. Галюк, Н. Я. Кушнир // Східно-Європейський журнал передових технологій. - 2011 - №2/3(50). – С 58-63.
4. Политанский, Р. Л. Исследование свойств цикличности псевдослучайных последовательностей битов / Р. Л. Политанский, Л. Ф. Политанский, М. Я. Кушнир. // Східно-Європейський журнал передових технологій. - 2009 - №6/2(42). – С 64-66.
5. Скопа, О. О. Вплив функціональної надмірності резервованих систем телекомунікацій на скорочення обсягів їх випробувань на надійність / О. О. Скопа, Н. Ф. Казакова, О. С. Мурін // Наук. праці ДонНТУ. Серія: Обчислювальна техніка та автоматизація. Випуск 58. – Донецьк: РВА ДонНТУ, 2003. - С.115-121.
6. Скопа, О. О. Принципи вибору формальних параметрів при побудові профілей захисту інфоресурсів [Текст] / Ю. В. Щербина, С. Л. Волков, О. О. Скопа // Східно-Європейський журнал передових технологій. – 2012. – Т. 5, № 2(59). – С. 31–33.
7. Мухін, О. М. Планування обсягу випробувань в мережах телекомунікацій / О. М. Мухін, Н. Ф. Казакова, О. О. Скопа // Вісник УБЕНТЗ. – 2002. – №2. – С.104-109.
8. Скопа, О. О. Аналіз моделей первинних датчиків псевдовипадкових чисел [Текст] / Н. М. Білик, О. О. Скопа // Системи обробки інформації. – 2009. – №7 (79). – С. 56-59. – ISSN 1681-7710.
9. Скопа, О. О. Статистичне тестування симетричних криптографічних перетворень [Текст] / О. О. Скопа // Східно-Європейський журнал передових технологій. – 2011. – №4/9 (52). – С. 15-18. – ISSN 1729-4061.
10. Скопа, О. О. Інструментальні засоби статистичного тестування криптографічних перетворень [Текст] / О. О. Скопа // Вісник Національного технічного університету «ХПІ». – 2011. – №33. – С. 77-83. – ISSN 2079-0023.
11. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] : пер. з англ. / Брюс Шнайер. – М. : Триумф, 2002. – 816 с. – ISBN 5-89392-055-4, 0-471-11709-9.
12. Siegenthaler, T. Gorrelation-Immunity of Nonlinear Combining Functions for Cryptographic Applications [Текст] / T. Siegenthaler // IEEE Transactions on Information Theory. – 1984. – V. IT-30, №5. – P. 776-780. – ISSN 0018-9448.
13. Matsumoto, M. Mersenne Twister: a 623-dimensionally equidistributed uniform pseudo-random number generator [Текст] / M. Matsumoto, T. Nishimura // ACM Trans. on Modeling and Computer Simulation. – 1998. – №8. – P. 3-30. – ISSN 1049-3301.
14. Столлингс, В. Современные компьютерные сети. 2-е изд. [Текст] / В. Столлингс // СПб.: Питер, 2003. – 783 с.
15. Олифер, В. Г. Новые технологии и оборудование IP-сетей. 4-е изд. [Текст] / В. Г. Олифер, Н. А. Олифер // СПб.: BHV-Санкт-Петербург, 2010. – 943 с.