

# Телекомунікації та захист інформації

УДК 004.056.5

DOI: [10.20535/2523-4455.2017.22.6.113191](https://doi.org/10.20535/2523-4455.2017.22.6.113191)

## Методи і технології захисту комп'ютерних мереж (фізичний та каналний рівні)

Кучернюк П. В., к.т.н., доц., ORCID [0000-0001-6381-0156](https://orcid.org/0000-0001-6381-0156)e-mail [kuchernuk@kpi.ua](mailto:kuchernuk@kpi.ua)Кафедра конструювання електронно-обчислювальної апаратури [keoa.kpi.ua](http://keoa.kpi.ua)

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського» [kpi.ua](http://kpi.ua)

Київ, Україна

**Реферат**—Розглянуто найбільш поширені рішення, які підтримуються виробниками обладнання для комп'ютерних мереж (комутатори 2-го та 3-го рівнів, маршрутизатори), реалізовані у операційних системах та протоколах і можуть бути використані при розробці та реалізації комплексних систем захисту корпоративних мереж. Стаття є першою з циклу статей, присвячених аналізу методів і технологій захисту. Наведено типові загрози комп'ютерним мережам фізичного та каналного рівнів моделі OSI та проведено аналіз особливостей методів і технологій захисту. Результати аналізу можуть бути використані для прийняття обґрунтованих рішень щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації.

Бібл. 17, табл. 1.

**Ключові слова** — безпека; загрози; захист; комп'ютерні мережі; міжмережні екрани.

### I. ВСТУП

Питання захисту комп'ютерних мереж від можливих атак, направлених на порушення функціонування мереж та окремих вузлів, несанкціонованого доступу до інформації та несанкціонованого використання сервісів мережі є одним з актуальніших, особливо для корпоративних мереж, до яких відносяться і мережі вищих навчальних закладів. Для захисту мереж розробляються і реалізуються комплексні системи захисту інформації (КСЗІ) [1], які складаються з набору організаційно-технічних заходів – від правил роботи користувачів у корпоративній мережі та розмежування прав доступу до інформаційних ресурсів та сервісів до встановлення та налаштування високофункціональних апаратно-програмних комплексів – міжмережних екранів (ММЕ) для захисту корпоративної мережі від зовнішніх атак.

Найчастіше у якості основної технічної складової КСЗІ використовують апаратні міжмережні екрани (ММЕ), які поділяються на ряд категорій за своїм функціоналом [2] та пропонуються різними виробниками телекомунікаційного обладнання [3]. Тим не менш, можна виділити ряд недоліків використання ММЕ: ММЕ не вирішують усіх задач захисту (перш за все захисту від внутрішніх атак, які виконуються з середини корпоративної мережі, розподілених (DDos) атак на зовнішні канали тощо), вартість таких апаратно-програмних комплексів досить висока.

Сучасне телекомунікаційне обладнання для комп'ютерних мереж усіх провідних світових виробників підтримує цілий ряд функціоналу, який може бути успішно використаний для вирішення питань захисту комп'ютерних мереж без додаткових фінансових вкладень. Стаття є першою з циклу статей, її метою є розгляд методів і технологій захисту фізичного та каналного рівнів моделі OSI, які підтримуються виробниками обладнання для комп'ютерних мереж (комутатори 2-го та 3-го рівнів, маршрутизатори), реалізовані у операційних системах та протоколах і можуть бути використані при розробці та реалізації комплексних систем захисту корпоративних мереж.

### II. ОСНОВНА ЧАСТИНА

Існує досить велика кількість підходів до класифікації загроз та можливих атак на комп'ютерні мережі. Враховуючи, що апаратні та програмні засоби комп'ютерних мереж працюють на відповідних рівнях моделі взаємодії відкритих систем (модель OSI), для аналізу методів і технологій захисту використаємо класифікації, які також орієнтовані на модель OSI [4], [5]. Найбільша кількість атак найчастіше реалізується на п'яти рівнях (фізичний, каналний, мережний, транспортний, прикладний). Загрози на сеансовому та представницькому рівнях пов'язані, в першу чергу, з процедурами ідентифікації, автентифікації та шифрування, алгоритми і протоколи яких



реалізовані в операційних системах і вплив на роботу яких з боку адміністраторів мереж мінімальний. У даній статті зупинимось на розгляді технологій захисту фізичного та каналного рівнів. Технології мережного, транспортного та прикладного рівнів будуть розглянуті у наступній статті циклу.

### III. МЕТОДИ ЗАХИСТУ НА ФІЗИЧНОМУ РІВНІ

Найбільш розповсюдженими атаками фізичного рівня на такі об'єкти, як канали передачі даних, є [5]:

- фізичне пошкодження;
- несанкціоновані зміни у функціональному середовищі;
- вимкнення фізичних каналів передачі даних;
- постановка шумів по всій полосі пропускання каналу.

Для реалізації каналів передачі у сучасних мережах використовуються обмежені середовища [6] (відповідно до діючих стандартів на структуровані кабельні системи використовуються оптичні кабелі та мідні кабелі «звита пара» у незахищеному та захищеному виконанні) та необмежені середовища передачі (відкритий ефір). Вибір середовища передачі для побудови каналів передачі даних здійснюється виходячи з таких основних вимог: призначення каналу (магістральні, лінії зв'язку мереж доступу) та його довжина, безпека передачі інформації, швидкість передачі даних, електромагнітна сумісність, вартість створення і експлуатації.

З точки зору захисту від наведених вище атак найбільш захищеним рішенням є використання оптичного кабелю. Оптичний канал за своєю фізичною природою [6] унеможливує прослуховування, зняття інформації та постановку шумів. Пропускна здатність оптичних каналів з використанням сучасних технологій щільного та розрідженого мультиплексування за довжинами хвиль може досягати декількох сотень Гб/с, а мінімальна протяжність без використання проміжного підсилення від 10 до 40 км (залежить від потужності лазерного випромінювача) [7]. Як альтернативу для коротких відстаней (до 100 м), яка дозволяє захиститися від атак, пов'язаних з електромагнітним впливом на канал, можна використати екрановану звиту пару. Враховуючи обмеження такого каналу по довжині та пропускній здатності (найбільш поширені технології набору стандартів IEEE 802 визначають швидкості передачі 100 і 1000 Мб/с, а технологія стандарту IEEE Std 802.3-2008 підтримує максимальну пропускну здатність на звитій парі 10 Гб/с [7]), такі лінії зв'язку можуть успішно використовуватись у локальних мережах з відповідними вимогами до захисту інформації.

Тим не менш, для побудови мереж доступу найбільш розповсюдженим рішенням є використання незахищеної звитої пари та безпроводових технологій (Wi-Fi). Такі рішення найменш захищені від згаданих вище атак. Єдиною можливістю захисту від несанкціонованого доступу до інформації при використанні таких ліній зв'язку є шифрування даних

(розгляд методів криптографічного захисту інформації виходить за рамки даної статті; з ними можна ознайомитись, наприклад, в [8], [9]).

Для запобігання можливим атакам, направленим на несанкціоновані зміни у функціональному середовищі, необхідно, перш за все, забезпечити обмеження фізичного доступу до кабельних каналів, комутаційних вузлів та дата-центрів, розробити та реалізувати політику віддаленого доступу до мережного обладнання, розгорнути допоміжні системи відеоспостереження та контролю доступу. Важливим фактором при забезпеченні надійності роботи інформаційно-комунікаційних систем можна вважати резервування найбільш критичних каналів, мережних пристроїв та серверів.

### IV. МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ НА КАНАЛЬНОМУ РІВНІ

Найбільш розповсюдженими атаками каналного рівня є генерація ширококомовних кадрів з метою переваження каналів передачі даних і комутаційного обладнання (до таких же наслідків приводять і так звані «широкомовні шторми» у великих комутуваних мережах [10]), підміна MAC-адрес вузлів, атаки на ARP і Spanning-Tree протоколи [10]. Технології захисту каналного рівня передбачають, перш за все, роботу з MAC-адресами вузлів, хоча ряд захисних функцій комутаторів аналізує і використовує й IP-адреси вузлів, що розширює область їх дії і на мережний рівень.

Можна виділити такі підходи до захисту на каналному рівні:

- застосування MAC-фільтрації та прив'язок MAC-адрес до портів комутаторів (функція Portsecurity комутатора [11]);
- застосування додаткових захисних функцій комутаторів, таких, як DHCP Snooping, DynamicARP Inspection, IP SourceGuard [11];
- сегментація мережі на окремі зони (домени ширококомовлення) з використанням технології віртуальних локальних мереж (Virtual Local Area Network – VLAN);
- автентифікація та авторизація на каналному рівні.

### V. ФУНКЦІЇ БЕЗПЕКИ НА КОМУТАТОРАХ

Portsecurity — функція комутатора, що дозволяє адміністративно вказати MAC-адреси вузлів, підключених до конкретного порту (прив'язка MAC-адреси до порту) або обмежити кількість MAC-адрес на порту, яким дозволено передавати дані через порт [11]. Використовується для запобігання:

- несанкціонованій зміні MAC-адреси мережного пристрою,
- несанкціонованому підключенню вузла до мережі,
- атакам, спрямованим на переповнення таблиці комутації.

Функція відстеження DHCP (DHCP Snooping) — функція комутатора, яка призначена для захисту від атак з використанням протоколу DHCP (наприклад, підміна або додавання несанкціонованого DHCP-сервера в мережі або атака DHCP starvation, яка змушує DHCP-сервер видати усі існуючі на сервері адреси зловмисникові).

Функція DHCP Snooping передбачає наступні дії [11]:

- визначення DHCP-повідомлень від ненадійних (несанкціонованих) джерел (DHCP-серверів) і відфільтрування таких повідомлень,
- розмежування DHCP-повідомлень від надійних та ненадійних джерел з подальшим відкиданням повідомлень або перенаправленням їх на відповідні порти,
- побудова та підтримка бази даних прив'язок, яка містить інформацію про ненадійні вузли з орендованими IP-адресами (вузли, які отримали IP-адреси від несанкціонованих DHCP-серверів),
- використання бази даних прив'язок для визначення та фільтрації кадрів від ненадійних вузлів.

При налаштуванні даної функції комутатор відстежує процес отримання IP-адрес вузлами з DHCP-серверів, аналізує DHCP-повідомлення, на підставі чого створює запис IP-MAC з прив'язкою до порту підключення вузла з даною MAC-адресою. В подальшому трафік від вузлів, які отримали IP-адреси з ненадійних DHCP-серверів або вузлів зі статичними IP-адресами (вузли не відповідають правилу прив'язки), не буде пропускатися через комутатор.

База даних прив'язок, отримана в процесі роботи функції DHCP Snooping, використовується також для подальшої роботи і інших захисних функцій комутаторів, таких, як:

- Dynamic ARP Inspection (Protection) [11] — перевірка ARP-пакетів, спрямована на боротьбу з атакою ARP-spoofing;
- IP SourceGuard [11] — перевірка IP-адреси відправника в IP-пакетах, спрямована на боротьбу з атакою IP-spoofing.

Dynamic ARP Inspection (Protection) (DAI) — функція комутатора, призначена для захисту від атак з використанням протоколу ARP. Такі атаки направлені на підміну законної MAC-адреси в ARP-записі на вузлах на фальшиву (атака ARP-spoofing), що дозволяє зловмиснику або перехопити кадри від вузлів і отримати доступ до конфіденційної інформації, або розірвати зв'язок між вузлами, що атакуються, порушивши нормальну роботу мережі. Щоб протидіяти таким атакам, комутатор повинен мати механізм для перевірки та пересилання між портами тільки законних ARP-повідомлень.

При налаштуванні функції DAI комутатор переходить, фіксує (заносить до журналу) та відкидає кадри з ARP-повідомленнями, які не відповідають раніш

створеним адресним прив'язкам IP-MAC (база даних прив'язок DHCP Snooping) [11]. Враховуючи, що для проведення атаки ARP-spoofing використовується ширококомвне розсилання повідомлень (повідомлення передаються в межах одного домену ширококомвнення/віртуальної локальної мережі), функція DAI використовується для захисту від внутрішніх атак.

Функція захисту від підміни IP-адрес (IP SourceGuard або Dynamic IP Lockdown) — функція комутатора, яка виконує фільтрацію трафіку на інтерфейсах 2-го (канального) рівня на підставі аналізу бази даних прив'язок DHCP Snooping або статичних прив'язок IP-MAC. Функція використовується для боротьби з такою атакою, як IP-spoofing. На першій стадії комутатор блокує передачу всього трафіку через захищений порт, окрім DHCP-повідомлень. Після отримання вузлом IP-адреси та створення запису в базі даних прив'язок DHCP Snooping або створення адміністратором статичної прив'язки IP-MAC весь трафік з цього вузла буде пересилатися через порт. Пересилання трафіку з інших вузлів заборонено. Таким чином, IP SourceGuard є порторієнтованою функцією, яка автоматично створює неявний список управління доступом до порту.

## VI. ТЕХНОЛОГІЯ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ (VIRTUAL LOCAL AREA NETWORK – VLAN)

Сегментація мережі на окремі зони (домени ширококомвнення) з використанням технології віртуальних локальних мереж дозволяє реалізувати такий функціонал:

- контроль за ширококомвним трафіком та його обмеження в рамках окремих сегментів;
- можливість створення функціональних робочих груп;
- підвищення інформаційної безпеки.

VLAN — віртуальна локальна мережа, яка являє собою групу вузлів мережі, трафік якої, в тому числі і ширококомвний, на каналному рівні повністю ізолюваний від інших вузлів мережі [10], [12]. Це означає, що передача кадрів між різними віртуальними мережами на підставі MAC-адреси неможлива, незалежно від типу адреси — унікальної, групової або ширококомвної. У той же час всередині віртуальної мережі кадри передаються за технологією комутації. Програмне забезпечення комутаторів дозволяє переносити вузли з однієї віртуальної мережі в іншу без фізичного переключення ліній зв'язку на інші порти або комутатори.

З точки зору забезпечення інформаційної безпеки найбільш цікавими функціями технології VLAN є контроль за ширококомвним трафіком та підвищення інформаційної безпеки.

### A. Контроль за ширококомвним трафіком

На відміну від традиційних LAN, побудованих за допомогою маршрутизаторів/комутаторів, VLAN можна розглядати як ширококомвний домен з логічно-налаштованими границями. VLAN дозволяє будувати

широкомовні домени незалежно від фізичного розміщення, середовища мережного доступу, типу носія та швидкості передачі. Вузли можуть розташовуватися там, де необхідно, а не там, де є спеціальне з'єднання з конкретним сегментом. VLAN збільшують продуктивність мережі, обмежуючи розповсюдження широкомовного трафіку рамками окремих VLAN.

### В. Підвищена інформаційна безпека

VLAN також пропонує додаткові переваги для інформаційної безпеки. Користувачі однієї робочої групи не можуть отримати доступ до даних іншої групи, тому що кожна VLAN — це закрита група вузлів (обмеження реалізовано на 2-му – каналному рівні моделі OSI). Для забезпечення передачі даних між вузлами різних VLAN необхідно задіяти 3-й – мережний рівень (налаштувати маршрутизацію між IP-мережами, кожній з яких відповідає окрема VLAN). При цьому за допомогою додаткових фільтрів, налаштованих на маршрутизаторі або комутаторі (зазвичай 3-го рівня), можна реалізувати політику взаємодії користувачів з різних віртуальних мереж. Зокрема, на деяких комутаторах можливе направлення пакетів в різні VLAN в залежності від адрес одержувача/відправника, портів і загальної завантаженості каналу (так звані Policy-Based VLANs). Таким чином, VLAN може бути частиною загальної стратегії мережної безпеки.

## VII. АВТЕНТИКАЦІЯ ТА АВТОРИЗАЦІЯ НА КАНАЛЬНОМУ РІВНІ

Для вирішення задач автентифікації та авторизації кінцевих пристроїв та користувачів безпосередньо в точках їх підключення (наприклад, на портах комутаторів локальних мереж або на точках доступу Wi-Fi) та реалізації задач централізованого контролю доступу до мережі використовується протокол IEEE 802.1x [13]. Протокол 802.1x функціонує на каналному рівні, сумісний з протоколом PPP (Point-to-Point Protocol) та протоколами каналного рівня 802 набору стандартів та забезпечує так звану порт-орієнтовану (port-based) авторизацію.

Для розгортання системи контролю доступу з використанням протоколу 802.1x необхідні три складові [14]:

- пристрій, що авторизується (так званий суплікант (supplicant) з програмним клієнтом 802.1x,
- пристрій доступу або автентифікатор (наприклад, комутатори локальної мережі або точки доступу Wi-Fi з підтримкою протоколу 802.1x),
- сервер авторизації — RADIUS сервер з базою даних користувачів (у якості облікових записів можуть виступати і MAC-адреси вузлів), який виконує безпосередню авторизацію або виступає посередником для авторизації, наприклад, в ActiveDirectory Microsoft.

При відсутності програмного клієнту 802.1x на пристрої користувача (наприклад, мережні принтери, IP-відеокамери тощо) можна провести авторизацію за MAC-адресою (режим MAC Authentication Bypass – MAB), або авторизуватися після проходження веб-автентифікації ( режим Web-Auth) [15].

Реалізуючи таку систему контролю доступу, можна надавати користувачам права доступу до корпоративної мережі незалежно від місця фізичного підключення до мережі та технології (проводової чи безпроводової). При успішному проходженні авторизації пристрій користувача буде автоматично підключено до відповідної VLAN, яка визначена політикою безпеки, та автоматично отримає IP-адресу з блоку адрес даної VLAN, до якої будуть застосовані відповідні списки доступу (більш детально списки доступу будуть розглянуті у наступній статті циклу). Протокол 802.1x може використовуватись для управління доступом до мережі не тільки на основі ідентифікаційних даних пристроїв та користувачів, а і спільно з протоколами верхніх рівнів, реалізуючи таким чином відповідні політики мережної безпеки.

Таблиця 1 МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ КАНАЛЬНОГО РІВНЯ

Метод захисту	Загрози, яким протидіє	Результат дії методу
Функція Portsecurity	Внутрішні загрози несанкціонованого підключення до мережі або зміни MAC-адреси	При несанкціонованому підключенні вузла порт блокується або відкидаються кадри з недозволеною MAC-адресою відправника
Функція DHCP Snooping	Внутрішні загрози додавання несанкціонованого DHCP-серверу, DoS-атаки на DHCP-сервер.	Автоматичне створення прив'язок IP-MAC-порт з подальшим відкиданням кадрів від вузлів, які не відповідають прив'язкам
Функція Dynamic ARP Inspection	Внутрішні загрози, пов'язані з підміною MAC-адрес в ARP-записах (атака ARP-spoofing)	Відкидання кадрів з незаконними ARP-повідомленнями
Функція IP SourceGuard	Внутрішні загрози, пов'язані з підміною IP-адрес	Відкидання кадрів від вузлів, які не відповідають прив'язці IP-MAC-порт
Сегментація на VLAN	Внутрішні загрози широкомовних штормів та несанкціонованого доступу до вузлів та інформації	Передача кадрів з будь-якими MAC-адресами отримувача тільки між вузлами окремих VLAN
Авторизація по протоколу 802.1x	Внутрішні загрози несанкціонованого підключення вузлів до мережі та доступу до сервісів та інформації	Передача кадрів від вузла тільки після проходження автентифікації та авторизації кінцевого пристрою або користувача





Основним недоліком і, відповідно, вразливістю протоколу 802.1x є відсутність шифрування даних, що може призвести до перехоплення даних та реалізації DoS атак. Більш захищеним рішенням є використання комбінації протоколів IPSec та 802.1x або нових протоколів IEEE 802.1AE [16] (набір протоколів MACsec, які вирішують задачі забезпечення конфіденційності та цілісності даних) та стандарту IEEE 802.1AR [17], який визначає унікальний захищений ідентифікатор пристроїв (SecureDeviceIdentity / DevID) для їх авторизації.

У табл. 1 наведено розглянуті вище методи захисту каналного рівня.

#### ВИСНОВКИ

Задача створення ефективних комплексних систем захисту комп'ютерних мереж може бути вирішена з використанням сукупності методів та технологій, які реалізовані в сучасному телекомунікаційному обладнанні для комп'ютерних мереж, як основи технічної складової таких систем. Виходячи з найбільш поширених загроз фізичного (фізичне пошкодження, несанкціоновані зміни у функціональному середовищі, вимкнення фізичних каналів передачі даних, постановка шумів по всій полосі пропускання каналу) та каналного (генерація широкомовних кадрів з метою перевантаження каналів передачі даних і комутаційного обладнання, підміна MAC-адрес вузлів, атаки на ARP і Spanning-Tree протоколи) рівнів моделі OSI проаналізовано особливості методів і технологій захисту та визначено, для вирішення яких задач захисту вони можуть бути застосовані. Розглянуті у роботі підходи до захисту на каналному рівні (застосування MAC-фільтрації та прив'язок MAC-адрес до портів комутаторів, застосування додаткових захисних функцій комутаторів, таких, як DHCP Snooping, Dynamic ARP Inspection, IP SourceGuard, сегментація мережі на окремі зони (домени широкомовлення) з використанням технології віртуальних локальних мереж, автентифікація та авторизація на каналному рівні) дозволяють ефективно протидіяти внутрішнім порушенням інформаційної безпеки. Проведений в роботі аналіз методів та технологій захисту дозволяє прийняти обґрунтовані рішення щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації. Стаття є першою з циклу статей, присвячених методам та технологіям захисту. У наступній статті буде розглянуто методи і технології мережного, транспортного та прикладного рівнів, які, у першу чергу, направлені на захист від зовнішніх атак на комп'ютерні мережі.

#### ПЕРЕЛІК ПОСИЛАНЬ

- [1] M. V. Graivoronsky and O. M. Novikov, *Bezpeka informatsionno-komunikatsinikh sistem [Safety of the information and*

Надійшла до редакції 27 жовтня 2017 року.

*communication systems*]. Kyiv, Ukraine: Vydavnicha hrupa BHV, 2009.

- [2] V. Maksimov, "Mezhsetevyie ekrany. Sposoby organizatsii zaschity i [Firewalls. Ways to organize protection]," *Computerpress*, no. 3, pp. 68–69, 2003, **URL**: <http://compress.ru/article.aspx?id=10145>.
- [3] "Apparatnye mezhsetevyie ekrany [Firewalls]," *InfoBezpeka*. [Online]. Available: <http://www.infobezpeka.com/products/apatnye/>.
- [4] B. Y. Korniienko, "Doslidzhennia modeli vzaiemodii vidkrytykh system z pohliadu informatsiinoi bezpeky [Research of open systems interconnection model in terms of information security]," *Sci. Technol.*, vol. 15, no. 3, pp. 83–89, 2012, **DOI**: [10.18372/2310-5461.15.5120](https://doi.org/10.18372/2310-5461.15.5120).
- [5] A. O. Dovhal, "Klasifikatsiia zahroz bezpeky v informatsiinii merezhi [Classification of security threats in the information network]," in *IX International Scientific Conference of Young Scientists "Electronics-2016"*, 2016.
- [6] P. V. Kucherniuk, *Osnovy postroeniia informatsionnykh setey: uchebnoe posobie dlia studentov spetsialnosti «Radioelektronnye apparaty i sredstva» [Fundamentals of information networks: Textbook for students of specialty "Radio-electronic devices and equipment]*. Kyiv, Ukraine: NTUU "KPI," 2014, **URI**: <http://ela.kpi.ua/handle/123456789/8071>.
- [7] P. V. Kucherniuk, *Kompiuterni merezhi: navchalnii posibnyk z distsipliny «Kompiuterni merezhi ta zasoby telekomunikatsii» dlia studentiv spetsialnosti 7.05090201, 8.05090201 «Radioelektronni apparaty ta zasoby» [Computer Networks: Textbook on discipline "Computer networks a. Kyiv, Ukraine: NTUU "KPI," 2014,* **URI**: <http://ela.kpi.ua/handle/123456789/12042>.
- [8] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography engineering: design principles and practical applications*. Indianapolis, USA: Wiley Publishing, 2010, **ISBN**: [978-0470474242](https://doi.org/10.1002/9780470474242).
- [9] A. A. Petrov, *Kompiuternaia bezopasnost. Kriptograficheskie metody zaschity [Computer security. Cryptography protection methods]*. Moscow, Russia: DMK Press, 2008, **ISBN**: [5-89818-064-8](https://doi.org/10.1002/9785898180648).
- [10] R. Seifert and J. Edwards, *The all-new switch book: the complete guide to LAN switching technology*, 2nd ed. Indianapolis, IN, USA: Wiley Publishing, cop., 2008, **ISBN**: [978-0470287156](https://doi.org/10.1002/9780470287156).
- [11] F. H. Y. Bhajji, *Network security technologies and solutions*. Indianapolis, IN, USA: Cisco Press, 2008, **ISBN**: [978-1-58705-246-0](https://doi.org/10.1002/9781587052460).
- [12] V. Olifer and N. Olifer, *Novye tekhnologii i oborudovanie IP-setei [New technologies and equipment of IP-networks]*. St.-Peterburg, Russia: Bhv, 2000, **ISBN**: [5-8206-0053-3](https://doi.org/10.1002/9785820600533).
- [13] "IEEE 802.1: 802.1X-2001 - Port Based Network Access Control," *IEEE 802*, 2001. [Online]. Available: <http://www.ieee802.org/1/pages/802.1x-2001.html>.
- [14] "Obzor i tipy EAP [EAP Overview and types]," 2017. [Online]. Available: <https://www.intel.ru/content/www/ru/ru/support/articles/000006999/network-and-i-o/wireless-networking.html>.
- [15] privilege15, "IEEE 802.1x," *TelecomBook*, 2010. [Online]. Available: <http://telecombook.ru/archive/network/cisco/directory/53-ieee-802-1x-cisco>.
- [16] "802.1AE: MAC Security (MACsec)," *IEEE 802*, 2006. [Online]. Available: <https://1.ieee802.org/security/802-1ae/>.
- [17] "P802.1AR-Rev: Secure Device Identity (Revision) |," *IEEE 802*, 2017. [Online]. Available: <https://1.ieee802.org/security/802-1ar-rev/>.



УДК 004.056.5

# Методы и технологии защиты компьютерных сетей (физический и канальный уровни)

Кучернюк П. В., к.т.н., доц., ORCID [0000-0001-6381-0156](https://orcid.org/0000-0001-6381-0156)e-mail [kuchernuk@kpi.ua](mailto:kuchernuk@kpi.ua)Кафедра конструирования электронно-вычислительной аппаратуры [keoa.kpi.ua](http://keoa.kpi.ua)

Национальный технический университет Украины

«Киевский политехнический институт имени Игоря Сикорского» [kpi.ua](http://kpi.ua)

Киев, Украина

*Реферат*—Рассмотрены наиболее распространенные решения, которые поддерживаются производителями оборудования для компьютерных сетей (коммутаторы 2-го и 3-го уровней, маршрутизаторы), реализованы в операционных системах и протоколах и могут быть использованы при разработке и реализации комплексных систем защиты корпоративных сетей. Данная статья – первая из цикла статей, посвященных анализу методов и технологий защиты. Приведены типовые угрозы компьютерным сетям физического и канального уровней модели OSI и проанализированы особенности методов и технологий защиты. Результаты анализа могут быть использованы для принятия обоснованных решений при выборе методов защиты для сетей разного назначения и с разными требованиями к защите информации.

Библ. 17, табл. 1.

*Ключевые слова* — безопасность; угрозы; защита; компьютерные сети; межсетевые экраны.

UDC 004.056.5

# Methods and technologies for computer networks protection (the physical and data link layers)

P. V. Kucherniuk, PhD, Assoc.Prof., ORCID [0000-0001-6381-0156](https://orcid.org/0000-0001-6381-0156)e-mail [kuchernuk@kpi.ua](mailto:kuchernuk@kpi.ua)Department of design of electronic digital equipment [keoa.kpi.ua](http://keoa.kpi.ua)National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" [kpi.ua](http://kpi.ua)

Kyiv, Ukraine

*Abstract*—Standard solutions that are supported by manufacturers of equipment for computer networks (switches the 2nd and 3rd levels, routers), implemented in the operating systems and protocols, and can be used for the development and implementation of integrated corporate network protection systems are considered in this article. The article is the first of a series of articles devoted to the analysis of methods and technologies of protection. The typical threats to computer network at the physical (physical damage of the data channels, unauthorized changes in the functional environment, disabling physical data channels, setting noise over the entire bandwidth of the channel) and data link (the generation of broadcasting frames to overload the data channels and switching equipment, the substitution of nodes MAC address, attacks on ARP and Spanning-Tree protocols) layers of OSI model are given and the features of methods and technologies to protect are analyzed. The features of use of limited and unlimited signal transmission media in terms of information security are considered at the physical level and a number of additional measures to prevent unauthorized changes in the functional medium networks are given (such as: the limitation of physical access to cable channels, switching nodes and data centers, the development and implementation of a policy of remote access to network equipment, deployment of auxiliary video surveillance and access control systems, redundancy of the most critical channels, network devices and servers). At the data link layer



are analyzed such functions of switches as Port security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard; segmenting the network into separate zones using the technology of Virtual Local Area Network to broadcast restrictions and improving information security; implementation of network access control system with authentication and authorization at the data link layer. To implement the access control systems of the channel level the features of the 802.1x protocol are considered and its main disadvantage (the lack of data encryption, which may lead to data interception and the implementation of DoS attacks) is determined. To build more secure solutions are proposed to use the combination of IPSec and 802.1x or new IEEE 802.1AE protocols (MACsec protocols that solve privacy and data integrity problems) and the IEEE 802.1AR standard, which defines a unique secure device identifier for their authorization. Analysis of methods and protection technologies at the physical and data link levels of the OSI model, which was conducted in work, allows making informed decisions about choosing methods to protect networks for different purposes and with different requirements regarding data protection.

References 17, Tables 1.

*Keywords* — security; threats; protection; computer networks; firewalls.