Телекомунікації та захист інформації

УДК 004.056.5 DOI: 10.20535/2523-4455.2018.23.1.113193

Методи і технології захисту комп'ютерних мереж (мережний, транспортний та прикладний рівні)

Кучернюк П. В., к.т.н., доц., ORCID 0000-0001-6381-0156
e-mail kuchernuk@kpi.ua
Кафедра конструювання електронно-обчислювальної апаратури keoa.kpi.ua
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського» 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 другою з циклу статей, присвячених аналізу методів і технологій захисту. Наведено типові загрози комп'ютерним мережам мережевого, транспортного і прикладного 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. Налаштування відповідного функціоналу на мережевому обладнанні дозволить здійснювати контроль відповідності політиці мережевої безпеки та реалізовувати захист максимально близько до можливого джерела порушень.**

Бібл. 16, табл. 1.

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

I. Вступ

Дана робота є другою з циклу статей, присвячених аналізу методів і технологій захисту комп'ютерних мереж. У попередній статті циклу [1] було підкреслено актуальність вирішення 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 та розглянуто технології захисту фізичного і канального рівнів моделі OSI. Метою даної статті є:

1) аналіз особливостей методів і технологій захисту мережевого, транспортного та прикладного 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;
2) визначення можливих варіантів їх застосування при розробці та реалізації комплексних систем захисту корпоративних мереж.

II. Методи захисту на мережному рівні

Більшість атак мережевого рівня пов'язані з використанням протоколу IP: підміна IP-адреси вузла, нав'язування хибного маршруту, перехоплення зловмисником діапазону IP-адрес та отримання інформації про логічну структуру мережі (IP-адреси вузлів, доменні імена), проблеми одноразової ідентифікації за IP-адресою.

Можна виділити такі підходи до захисту від наведених атак:

- створення прив'язок IP – MAC-порт для запобігання підміні IP-адреси та несанкціонованому підключенню до мережі (базові підходи реалізуються на канальному рівні і їх було розглянуто у попередній статті циклу [1]),
- використання технології трансляції мережних адрес (Network Address Translation – NAT [2]) для приховання від зовнішніх зловмисників діапазону IP-адрес організації та логічної структури мережі,
- створення списків контролю доступу (Access Control List– ACL [2]) для обмеження доступу

до вузлів та протоколів/сервісів прикладного рівня.

Протокол NAT використовується для передачі пакетів з IP-адрес, призначених тільки для внутрішнього використання, в зовнішні мережі і для вирішення задачі приховування внутрішньої логічної структури мережі від зовнішніх мереж [2], [3]. NAT транслює тільки той трафік, який проходить між внутрішньою і зовнішньою мережею і визначений для трансляції. Будь-який трафік, який не відповідає критеріям трансляції або той, який проходить між іншими інтерфейсами на маршрутизаторі, ніколи не транслюється і пересилається з використанням маршрутизації. Слід звернути увагу на те, що протокол NAT виконує тільки трансляцію адрес і не виконує функції фільтрації. Для заборони проходження пакетів з зовнішніх мереж у внутрішню необхідно застосовувати відповідні списки доступу.

Існують наступні способи реалізації NAT.

Статичний NAT – відображення конкретної внутрішньої IP-адреси на конкретну зовнішню IP-адресу (можлива також заміна портів протоколів транспортного рівня при трансляції). Зазвичай статичний NAT використовують, коли до вузла внутрішньої мережі необхідно забезпечити доступ з зовнішніх мереж з використанням конкретних протоколів прикладного рівня.

Динамічний NAT – відображає адресу з блоку внутрішніх IP-адрес на одну з вільних адрес блоку зовнішніх адрес. Досить рідко використовується завдяки необхідності використання декількох зовнішніх IP-адрес та пов’язаній з цією ж особливістю низькою масштабованістю.

Перевантаження (Overload) – форма динамічного NAT, який відображає адресу з блоку внутрішніх IP-адрес в єдину зовнішню IP-адресу, використовуючи різні порти (відома також як PAT —Port Address Translation). Найбільш поширений варіант для організації виходу в Інтернет з внутрішніх вузлів корпоративної мережі.

Списки контролю доступу(Access Control List – ACL [2], [3]) містять набір правил, де визначено дію над пакетами і параметри пакетів для фільтрації (адреси відправників та отримувачів, номера портів протоколів транспортного рівня тощо). Перевірка пакетів проводиться точно в тому порядку, в якому задані правила в списку. Коли пакет потрапляє на інтерфейс, він перевіряється по першому правилу. Якщо параметри пакету відповідають першому правилу, подальша перевірка припиняється. Пакет або буде передано далі, або знищено. Якщо параметри пакету не відповідають першому правилу, проводиться його аналіз на відповідність наступному правилу і так далі, поки не буде перевірено усі правила (якщо пакет не відповідав вимогам якогось з правил вище). Якщо параметри пакету не відповідають жодному з правил списку, пакет просто знищується (в кінці кожного списку стоїть неявне правило, яке забороняє проходження усіх пакетів).

ACL можуть бути застосовані до:

- фізичних або логічних інтерфейсів (в тому числі на інтерфейси VLAN-комутаторів 3-го рівня);
- термінальних ліній для обмеження доступу до пристрою по протоколам Telnet або SSH;
- VPN-тунелів (які пакети потрібно шифрувати);
- механізмів QoS (визначення пріоритетів для різних типів трафіку);
- шейперів для обмеження швидкості трафіку користувачів;
- протоколу NAT (визначають, які IP-адреси необхідно транслювати).

За допомогою списків доступу вирішується і задача захисту від нав'язування хибного маршруту. Така атака базується на властивості ICMP-протоколу «на льоту» змінювати маршрут просування пакетів (повідомлення "Перенаправлення маршруту" (Redirect) ICMP протоколу). В результаті зв'язок вузла з мережею буде розірваний. Відповідним правилом ACL необхідно заборонити прийом ICMP повідомлень «Redirect» на зовнішніх інтерфейсах маршрутизатора.

Одним з різновидів ACL є динамічні списки доступу (Dynamic (Lock-and-Key) ACL) [2], [3]), використання яких дозволяє організувати доступ до вузлів внутрішньої мережі, попередньо ініціювавши з'єднання з прикордонним маршрутизатором за допомогою якого-небудь протоколу (наприклад, telnet або ssh). Зазвичай ці ACL використовуються для віддалених підключень до мережі організації, але можливе їх застосування і для підключення до різних корпоративних ресурсів з попередньої авторизацією.

Процедура роботи динамічних ACL наступна:

- користувач підключається до зовнішнього інтерфейсу прикордонного маршрутизатора з будь-якої зовнішньої мережі;
- • користувач проходить автентифікацію (вводить логін/пароль);
- • у випадку успішної автентифікації на інтерфейсі активуються спеціальні правила динамічного ACL, які дозволяють проходження пакетів з IP-адреси користувача до вузлів внутрішньої мережі. Правила залишаються активними впродовж налаштованого періоду часу (тайм-ауту). Слід відзначити, що таке рішення дозволяє тільки ідентифікувати та авторизувати користувача і не захищає дані, які будуть передаватися між вузлом користувача та корпоративною мережею. Більш захищеним рішенням є використання технології віртуальних приватних мереж [4], [5].

Використання розглянутих вище ACL не вирішує задачу атак на вузли корпоративної мережі по відкритим портам TCP та UDP-протоколів, які завжди наявні. Для вирішення цієї задачі використовують механізм контролю сесій (Statefull Inspection, також знана

як динамічна фільтрація пакетів [6]). Цей механізм передбачає моніторинг стану активних сеансів та використовує цю інформацію для прийняття рішення щодо фільтрації пакетів, які надходять на інтерфейси маршрутизатора чи MME. При використанні такого підходу перевіряються усі вхідні та вихідні пакети (аж до прикладного рівня; зазвичай ідентифікується номер порту прикладного протоколу або сервісу) і через прикордонний пристрій (маршрутизатор або MME) будуть пропущені тільки ті вхідні пакети, які є правильною відповіддю на вихідні запити. Підхід може бути використаний і для фільтрації даних прикладних протоколів для забезпечення захисту на прикладному рівні [7].

Прикладом реалізації підходу на основі механізму контролю сесій є рефлексивні або дзеркальні списки доступу (Reflexive ACL) [2], [3]. Вони дозволяють відслідковувати стан сесій, ініційованих з внутрішньої мережі, і створювати відповідні зворотні правила.

Рефлексивні ACL працюють наступним чином. Створюються два списки доступу. Перший список дозволяє доступ з локальної мережі в Інтернет (можливі стандартні обмеження за IP-адресами, протоколами, портами). В правилах цього списку задається команда відображення (reflect) у динамічне правило іншого списку, яке дозволить проходження пакетів з зовнішніх мереж тільки на запити з внутрішньої мережі. Другий список містить динамічні правила, які дозволяють проходження пакетів. Проходження будь-яких інших пакетів з зовнішніх мереж у внутрішню заборонено. Таким чином реалізується проходження пакетів з зовнішніх мереж на вузли внутрішньої мережі тільки за ініціативою внутрішніх вузлів.

Розглянуті вище методи захисту мережевого рівня досить ефективно дозволяють захистити вузли корпоративної мережі, але не вирішують задачу захисту від DDoS-атак на зовнішні канали, які призводять до того, що небажаний трафік на IP-адреси вузлів, що атакуються, з автономної системи корпоративної мережі чи провайдера утилізує усю пропускну спроможність зовнішніх каналів (прикладом таких атак є атака DNS Amplification). Можливим рішенням для захисту є ідентифікація IP-адрес, що атакуються, та блокування маршрутів на ці адреси з використанням відповідного функціоналу протоколів зовнішньої маршрутизації (наприклад, функції Blackhole протоколу BGP [8]). Налаштування та використання функції Blackhole BGP дозволяє керувати трафіком на рівні магістральних маршрутизаторів різних операторів/провайдерів, до попадання цього трафіку на інтерфейси маршрутизаторів, які обслуговують автономну систему з IP-адресами вузлів, що атакуються.

Для налаштування Blackhole використовують розширені можливості по управлінню маршрутами - BGP community. Для цього створюються спеціальні групи (community) для маршрутів, трафік по яким необхідно направити у «чорну діру». В момент проведення атаки адміністратор визначає IP-адресу, що атакується, та створює маршрут з маскою /32 з визначеним для Blackhole community, який анонсується маршрутизаторами своїм сусідам. В результаті сусідні маршрутизатори повинні відкидати пакети, які надходять на цей маршрут. Фільтрація пакетів на сусідніх маршрутизаторах може виконуватись з використанням спеціально налаштованих ACL або шляхом направлення їх на віртуальний (Null) інтерфейс. Більш ефективним рішенням, яке дозволяє не допустити небажаний трафік і в магістральні канали сусідів, є використання рекурсивного blackhole [9]. У цій процедурі, отримавши маршрут з Blackhole community, маршрутизатори виконують фільтрацію небажаного трафіку та анонсують маршрут далі своїм сусідам (при цьому значення Blackhole community буде змінюватись на оговорене між сусідами). В результаті анонси про маршрути досягають маршрутизаторів, до яких підключені IP-мережі, з яких виконуються атаки, і подальша фільтрація буде виконуватись саме на цих маршрутизаторах. Це дозволяє звільнити від небажаного трафіку магістральні канали усіх проміжних операторів. Такий підхід дозволяє повністю припинити потік трафіку на вузол, що атакується, та зняти паразитне навантаження з магістральних каналів та зовнішніх каналів корпоративної мережі. Звичайно ж, використовувати його можна тільки постфактум – після початку атаки. В результаті реакція на атаку завжди є запізнілою (а у нічний час не завжди є черговий адміністратор, який може зробити необхідний аналіз трафіку та внести зміни в налаштування протоколу BGP). Недоліком такого рішення є також те, що повністю блокується весь трафік до вузлів, IP-адреси яких визначені в Blackhole маршрутах.

Розглянуті вище методи захисту мережевого рівня зведені у таблицю 1.

ТАБЛИЦЯ 1. МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ МЕРЕЖЕВОГО РІВНЯ

Методи захисту	Загрози, яким протидіє	Результат дії методу
Створення прив'язок IP – MAC – порт	Внутрішні загрози, пов'язані з підміною IP-адрес	Розглянуто у попередній статті циклу в методах канального рівня
Технологія трансляції мережних адрес (NAT)	Зовнішні загрози, пов'язані з визначенням логічної структури мережі та подальшими атаками на вузли	За рахунок заміни IP-адреси відправника пакету від зовнішніх мереж повністю приховується логічна структура мережі
Створення списків контролю доступу (ACL)	Зовнішні та внутрішні загрози несанкціонованого підключення до вузлів та сервісів мережі, DoS-атаки	Відкидання пакетів, які не відповідають правилам списку
Створення списків заборонених маршрутів до вузлів мережі	Зовнішні загрози, пов'язані з DDoS-атаками на зовнішні канали мережі	Відкидання пакетів, які відповідають маршруту з «чорного» списку, на маршрутизаторах магістральної мережі

III. Протоколи захисту на транспортному рівні

Для протоколів транспортного рівня характерна відсутність перевірки джерел інформації, що сприяє таким загрозам, як перехоплення та підключення до відкритих портів протоколів транспортного рівня.

Якщо для запобігання несанкціонованим підключенням до портів протоколів транспортного рівня можна використовувати розглянуті вище списки доступу мережевого рівня, то захист від перехоплення потребує застосування додаткових протоколів, які підтримують шифрування даних та автентифікацію суб'єктів обміну даними.

Для вирішення цієї задачі використовується протокол SSL/TLS (Secure Socket Layer / Transport Layer Security) [10], який реалізує шифрування і автентифікацію між транспортними рівнями приймача і передавача.

Процедура роботи протоколу SSL/TLS включає в себе три основних фази:

1) діалог між сторонами, метою якого є вибір алгоритму шифрування;
2) обмін ключами на основі криптосистем з відкритим ключем або автентифікація на основі сертифікатів;
3) передача даних, які шифруються за допомогою симетричних алгоритмів шифрування.

Таким чином протокол SSL/TLS виконує функції автентифікації, шифрування даних і забезпечення цілісності даних. Автентифікація здійснюється шляхом обміну цифровими сертифікатами при встановленні з'єднання (сесії) [10]. В силу того, що SSL/TLS реалізується на транспортному рівні, захищене з'єднання встановлюється «з кінця в кінець» (захищений віртуальний тунель транспортного рівня). Протокол SSL/TLS зазвичай використовується протоколами прикладного рівня (найбільш поширеним використанням SSL є шифрування HTTP трафіку — режим HTTPS), тому таке рішення часто відносять до прикладного рівня.

IV. Методи та технології захисту на прикладному рівні

Відкритий характер протоколів прикладного рівня зумовлює велику кількість загроз, пов'язаних з основною проблемою цих протоколів —передача інформації у нешифрованому вигляді. Використання на прикладному рівні процедур ідентифікації та автентифікації користувачів із подальшою авторизацією утворює також загрозу перехоплення або підбору облікових записів та паролів. Значну загрозу також становлять віруси та шпигунське програмне забезпечення, які діють саме на прикладному рівні, DoS та DDoS-атаки на інформаційні системи.

Зазвичай, коли говорять про засоби захисту на прикладному рівні, розглядають два підходи: використання серверів-посередників (proxy) [6] та використання механізмів контролю сесій (Statefull Inspection), основи якого було розглянуто вище. Обидва ці підходи реалізують контроль за з'єднанням, але не вирішують задачу аналізу вмісту пакетів та фільтрації пакетів з небажаним вмістом, що не дозволяє запобігти розповсюдженню вірусів через електронну пошту, встановленню несанкціонованих програмних додатків через Інтернет на робочі станції, несанкціонованій зміні вмісту веб-сайтів тощо. Для захисту від таких порушень може бути використана контентна фільтрація, яка базується на сигнатурному аналізі пакетів [11]–[13]. Цей механізм передбачає аналіз інформації у пакеті, при чому як заголовка пакета, так і поля даних. Це дозволяє встановити відповідність між інформацією з поля даних та конкретними додатками, контролювати передачу даних між конкретними додатками та проводити фільтрацію небажаної інформації. Враховуючи, що інформація аналізується по пакетно, цей механізм не дозволяє повністю аналізувати трафік мережних додатків.

Окремо слід відзначити забезпечення безпеки в гетерогенних віртуальних обчислювальних середовищах, до яких відносять GRID-системи та «хмарні обчислення» (cloud computing). З кожним роком все більше різних компаній (в тому числі і вищі навчальні заклади) переводять обчислювальні і інформаційні ресурси у віртуальну інфраструктуру. У таких середовищах виникають нові загрози. Перш за все це атаки на засоби управління віртуальними машинами, хмарні контролери, сховища даних, неавторизований доступ до вузлів віртуалізації, використання віртуального середовища для несанкціонованої передачі даних [13], [14].

Можливість проведення наведених атак із віртуальної мережі суттєво обмежує використання традиційних для комп'ютерних мереж методів захисту та потребує розробки спеціалізованих рішень. В основу таких рішень може бути покладено розглянуті вище механізми контролю сесій (Statefull Inspection) та пакетної фільтрації. Так, у роботі [14] пропонується підхід до розмежування доступу на основі контролю віртуальних з'єднань та використання скритої фільтрації. Правила фільтрації можуть бути створені для різних рівнів опису потоків даних на підставі заголовків канальних, мережних, транспортних та прикладних протоколів.

Таким чином, враховуючи велику кількість та різноплановість протоколів та програмних додатків прикладного рівня, організувати ефективну протидію загрозам прикладного рівня можна тільки шляхом розробки та реалізації комплексних систем захисту інформації з використанням спеціалізованих ММЕ, механізмів розмежування та контролю доступу до ресурсів мережі, застосування технологій криптографічного захисту та електронних цифрових підписів. Розгляд останніх технологій виходить за рамки даної статті.

Одним з ефективних рішень комплексного захисту інформаційних систем корпоративних мереж є використання мережі доставки/поширення контенту (*Content Delivery Network* або *Content Distribution Network*, CDN). Системи на базі CDN ефективно вирішують питання захисту від DoS та DDoS-атак не

тільки на прикладному, а і на мережевому і транспортному рівнях [15].

Великі виробники мережевого обладнання пропонують спеціалізовані рішення для вирішення задач комплексного захисту корпоративних мереж. Прикладом таких рішень є технологія NAC (Network Admission Control) компанії Cisco [16]. Дана технологія дозволяє не тільки перевіряти пристрої та користувачів ще на етапі підключення до корпоративної мережі, а і заблокувати доступ комп'ютерів, які не відповідають політиці безпеки (в тому числі заражених вірусами та шкідливими програмами, де не оновлено антивірусні бази, відсутні необхідні оновлення операційної системи тощо). Контроль відповідності політиці безпеки реалізується максимально близько до можливого джерела порушень – на порту комутатора, точки доступу Wi-Fi або маршрутизатора, які підтримують технологію NAC.

Висновки

Виходячи з найбільш поширених загроз мережевого (підміна IP-адреси вузла, нав'язування хибного маршруту, перехоплення зловмисником діапазону IP-адрес та отримання інформації про логічну структуру мережі, DDoS-атак на зовнішні канали), транспортного (перехоплення інформації та підключення до відкритих портів протоколів транспортного рівня) і прикладного (перехоплення інформації, віруси та шпигунське програмне забезпечення, DoS та DDoS-атаки на інформаційні системи) 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 (технологія трансляції мережевих адрес, створення списків контролю доступу, створення списків заборонених маршрутів до вузлів мережі, шифрування даних та автентифікація суб'єктів обміну даними з використанням протоколу SSL/TLS, використання серверів-посередників та механізмів контролю сесій, контентна фільтрація, системи на базі CDN) дозволяють ефективно протидіяти, у першу чергу, зовнішнім порушенням інформаційної безпеки. Стаття є другою з циклу статей, присвячених методам та технологіям захисту. Проведений в роботі аналіз методів та технологій захисту на різних рівнях моделі OSI дозволяє ухвалювати обґрунтовані рішення щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації. 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. При виборі та реалізації технологій захисту для конкретної мережі необхідно враховувати особливості структури мережі, спеціалізації роботи компанії, вірогідність проведення конкретних атак. Налаштування відповідного функціоналу на мережевому обладнанні дозволяє здійснювати контроль відповідності політиці мережевої безпеки та реалізовувати захист максимально близько до можливого джерела порушень, що, у свою чергу, мінімізує можливі негативні наслідки для корпоративної мережі.

Перелік посилань

[1] P. V. Kucherniuk, "Metody i tekhnolohii zakhystu komp'iuternykh merezh (fizychnyi ta kanalnyirivni) [Methods and technologies for computer networks protection (the physical and data link layers)]," *Microsystems, Electron. Acoust.*, vol. 22, no. 6, pp. 64–70, 2017, **DOI:** 10.20535/2523-4455.2017.22.6.113191.

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

[3] S. Wilkins and T. Smith, *CCNP Security. SECURE 642-637 Official Cert Guide*. Cisco Press, 2011, **ISBN:** 978-1-58714-280-2.

[4] P. V. Kucherniuk, *Kompiuterni merezhi: navchalnii posibnyk z distsipliny «Kompiuterni merezhi ta zasoby telekomunikatsii» dlia studentiv spetsialnosti 7.05090201, 8.05090201 «Radioelektronni aparaty ta zasoby» [Computer Networks [Electronic publications]: a textbook on discipline "Computer networks and telecommunications"]*. Kyiv, Ukraine: NTUU "KPI," 2014, **URL:** http://ela.kpi.ua/handle/123456789/12042.

[5] 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.

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

[7] A. V. Silinenko, "Sistema semanticheskogo upravleniya dostupom k setevyim resursam (na osnove mezhsetevyih ekranov) [Semantic management system access to network resources (based on firewalls)]," *IT doma i na rabote [IT at home and at work]*. [Online]. Available: http://old.ci.ru/inform12_08/p_15.htm. [Accessed: 01-Feb-2017].

[8] T. King *et al.*, "BLACKHOLE Community," *Internet Engineering Task Force (IETF)*, 2016. [Online]. Available: https://tools.ietf.org/html/rfc7999. [Accessed: 01-Feb-2017].

[9] Vadim (AKA velizarx), "Zaschita ot DDOS atak sredstvami BGP [Protection from DDOS attacks means BGP]," *Informatsionnaya bezopasnost [Information security]*. [Online]. Available: https://habrahabr.ru/post/211176/. [Accessed: 01-Feb-2017].

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

[11] A. M. Plaskovsky, A. G. Novopashenny, Y. E. Podgurskiy, and V. S. Zaborowski, *Metodyi i sredstva zaschity i kompyuternoy informatsii. Mezhsetevoe ekranirovanie. Razgranichenie dostupa na prikladnom urovne [Methods and means of protection of computer information. Firewall. Access control at the application level]*. St. Petersburg, Russia: Publishing House of STU, 2012.

[12] A. Ott, "Sovremennyie tendentsii v oblasti kontentnoy filtratsii [Modern trends in content filtering]." [Online]. Available: http://alexott.net/ru/writings/cf/. [Accessed: 01-Feb-2017].

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

[14] V. S. Zaborowski, A. A. Lukashin, S. V. Kupreenko, and V. A. Mulyuha, "Arhitektura sistemy i razgranicheniya dostupa k resursam geterogennoy vyichislitelnoy sredyi na osnove kontrolya virtualnyih soedineniy [Delineation system architecture of access to resources of a heterogeneous computing environment based on monitoring virtual connections]," *Vestn. UGATU. Mat. i Program. obespechenie*, vol. 15, no. 5 (45), pp. 170–174, 20111, **URL:** https://elibrary.ru/item.asp?id=18863047.

[15] M. Kozlova (AKA M. Kozlova, "7 luchshikh servisov zashchity ot DDoS-atak dlya povysheniya bezopasnosti [The 7 best services of protecting from DDoS- attacks for the increase of safety]," *HOSTING.cafe*, 2017. [Online]. Available: https://habrahabr.ru/company/hosting-cafe/blog/324848/. [Accessed: 01-Feb-2017].

[16] "Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco." [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html. [Accessed: 01-Feb-2017].

Надійшла до редакції 27 жовтня 2017 р.

УДК 004.056.5

Методы и технологии защиты компьютерных сетей (сетевой, транспортный и прикладной уровни)

Кучернюк П. В., к.т.н., доц., ORCID 0000-0001-6381-0156
e-mail kuchernuk@kpi.ua
Кафедра конструирования электронно-вычислительной аппаратуры keoa.kpi.ua
Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского» 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 – вторая из цикла статей, посвященных анализу методов и технологий защиты. Приведены типовые угрозы компьютерным сетям сетевого, транспортного и прикладного уровней модели OSI и проанализированы особенности методов и технологий защиты. Результаты анализа могут быть использованы для принятия обоснованных решений по выбору методов защиты для сетей разного назначения и с разными требованиями к защите информации. Настройка соответствующего функционала на сетевом оборудовании позволяет осуществлять контроль соответствия политике сетевой безопасности и реализовывать защиту максимально близко к возможному источнику нарушений.**
Библ. 16, табл. 1.

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

UDC 004.056.5

Methods and technologies for computer networks protection (network, transport and application layers)

P. V. Kucherniuk, PhD, Assoc.Prof., ORCID 0000-0001-6381-0156
e-mail kuchernuk@kpi.ua
Department of design of electronic digital equipment keoa.kpi.ua
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute" 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 second**

of a series of articles devoted to the analysis of methods and technologies of protection. The typical threats to computer network at the network (substitution the IP addresses of the nodes, imposing the wrong route, intercepting the IP address range and receiving information about the logical structure of the network, DDoS attacks on external channels), transport (Interception of information and connection to open ports of transport layer protocols) and application (Information interception, viruses and spyware) layers of OSI model are given and the features of methods and technologies to protect at are analyzed. Technology of Network Address Translation and Access Control Lists are analyzed to prevent threats to the network level. Features of using the "Blackhole" BGP function for protection against DDoS attacks on external channels are considered. The features of the protocol Secure Socket Layer / Transport Layer Security to protect against threats to the transport layer are analyzed. Approaches of "Statefull" Inspection and content filtering that allow implementing control of connection, data control between specific applications and performing filtering unwanted information are considered at the application level. Also, features of network security providing in heterogeneous virtual computing environments such as GRID-systems and cloud computing are noted. The approaches to protection which ware considered in work allow to effectively counter acting, first of all, external violation of information security. In the previous article of the cycle the methods and technologies of the physical and channel levels that were aimed at protecting against internal attacks on computer networks were considered. Analysis of methods and protection technologies at various 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. Configuring the proper functionality on the network equipment allows carrying out the monitoring of compliance with network security policies and implement protection as close to possible sources of violations.

Ref. 16, tabl. 1.

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