УДК 004.056.32

ДОСЛІДЖЕННЯ МОДЕЛІ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ З ПОГЛЯДУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Б. Я. Корнієнко, канд. техн. наук, доц.
Національний авіаційний університет
e-mail: bogdanko@i.ua

Розглянуто модель OSI з погляду інформаційної безпеки, класифікацію вразливостей та заходів убезпечення за рівнями моделі OSI. З метою побудови комплексних систем захисту інформації для інформаційно-комунікаційних систем та мереж запропоновано розширити семирівневу модель до дев'ятирівневої — за рахунок восьмого рівня — рівня політик та дев'ятого — рівня користувачів.

Ключові слова: модель OSI, інформаційна безпека, вразливості, заходи убезпечення.

In this article the OSI model in terms of information security classification of vulnerabilities and security measures at the level of model OSI. In order to build a comprehensive information security systems for information and communication systems and networks offer a model to extend the seven- nine levels — through eight levels — level politician and ninth — level users.

Keywords: OSI model, information security, vulnerabilities, security measures.

Вступ

Інформація сьогодні є важливим елементом промисловості та однією з основ сучасного суспільства. Інформаційно-комунікаційні системи та мережі служать для розширення доступу користувачів до інформаційних ресурсів та надання широкого спектра сервісів. Але крім корисних функцій та надання різноманітних послуг, інформаційно-комунікаційні системи та мережі можуть стати каналом несанкціонованого доступу до комп'ютерів користувачів. Тому комп'ютерні мережі та завдання інформаційної безпеки нерозривно пов'язані між собою та потребують постійного вдосконалення відповідно до зростаючого рівня загроз.

Ключовим елементом для дослідження комп'ютерних мереж є запропонована Міжнародною організацією зі стандартизації (ISO) модель взаємодії відкритих систем (*Open Systems Interconnection*, OSI) [1]. Модель OSI складається із семи рівнів, на кожному з яких існують загрози для інформаційної безпеки. Побудова комплексних систем захисту інформації потребує не тільки протидії загрозам на кожному рівні моделі OSI, а також створення цілісної багатошарової системи захисту інформації із розробкою політики безпеки, інструкцій та рекомендацій для користувачів інформаційно-комунікаційних систем та мереж [2]. Розроблена більше тридцяти років тому модель OSI потребує певного розширення та доповнення, з урахуванням проблем інформаційної безпеки [3].

Постановка завдання

Мета даних досліджень — розгляд семи рівнів моделі OSI з погляду інформаційної безпеки, класифікація вразливостей та заходів убезпечення за рівнями моделі OSI та пропозиції щодо розширення та доповнення моделі OSI.

Виклад основного матеріалу дослідження

У рамках моделі OSI взаємодія двох систем відбувається фактично у вигляді двох моделей — горизонтальної та вертикальної:

— у рамках горизонтальної моделі розглядається пряма взаємодія (обмін даними) однакових рівнів у двох кінцевих точках (хостах); для організації такої взаємодії в кожній з кінцевих точок повинні підтримуватися однакові протоколи для даного рівня;

— у вертикальній моделі розглядається обмін інформацією (взаємодія) між сусідніми рівнями однієї системи з використанням інтерфейсів; у цій моделі кожен рівень може надавати свої послуги вищому рівню, і користуватися послугами нижчого рівня (крайні рівні моделі в цьому сенсі є винятком — прикладний рівень надає свої послуги користувачу, а фізичний рівень не користується сервісом інших рівнів) (рис. 1).

Спираючись на структуру моделі OSI, реалізована класифікація протоколів обміну даними та апаратного забезпечення комп`ютерних мереж. Задачі інформаційної безпеки слід розглядати згідно з рівнями моделі взаємодії відкритих систем. Наприклад, можна одразу викремити визначну роль фізичного рівня для передачі даних. За будь-якого вимкнення пристрою від мережі передача даних припиняється.

При одержанні фізичного доступу до мережі стороннім комп'ютером важко уникнути втрат даних. За наявності помилок на фізичному рівні вищі рівні не можуть коректно функціонувати, вони повністю залежать від цілісності фізичного рівня.

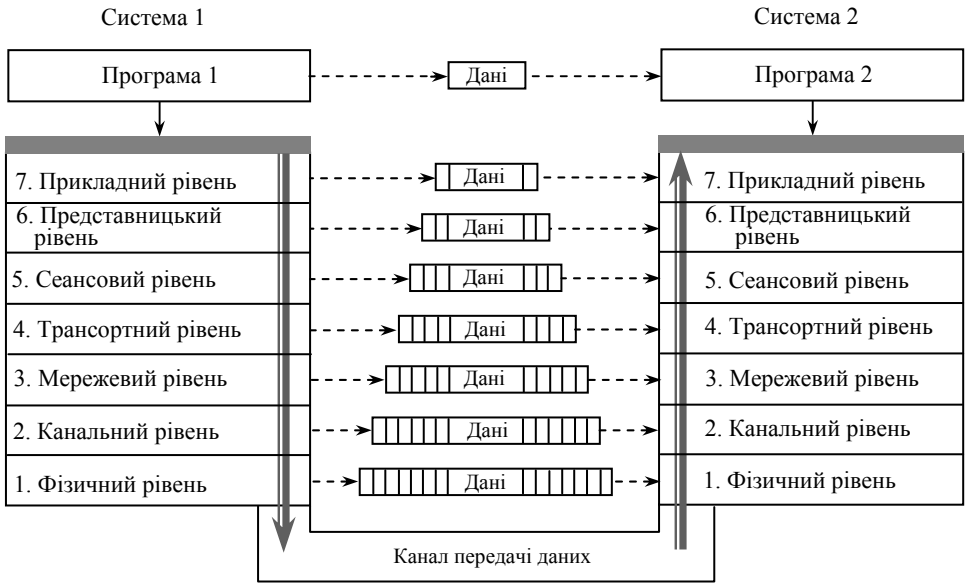

Рис. 1. Модель взаємодії відкритих систем:
--------- — логічне з'єднання між рівнями; ═══ — реалізація передачі даних

Іншим прикладом можуть бути загрози інформаційної безпеки на прикладному рівні. Нехай усі шість нижчих рівнів мають ефективні налаштування з погляду захисту інформації — якісна фізична ізоляція, використання VLAN, міжмережеві екрани з жорсткою фільтрацією пакетів. Але проблеми можуть виникнути через застаріле програмне забезпечення на сервері, погано написані коди програм та сценаріїв. Оскільки ці проблеми належать до прикладного рівня, захист протоколів нижчих рівнів їх не в змозі вирішити. Так міжмережевий екран і демілітаризована зона не захистять мережу від зловмисників, якщо є можливість підключитися до портів вразливих служб (WWW, SMTP, Netbios, SQL). Отже, безпека повинна реалізовуватись на рівні сервісів.

Тому використовуючи модель OSI як об'єктивну міру розглянемо, задачі інформаційної безпеки на кожному рівні, їх взаємодію та запропонуємо комплексний підхід для побудови систем захисту інформаційно-комунікаційних систем та мереж.

Фізичний рівень моделі OSI

Для захисту інформації необхідно забезпечити фізичну цілісність інформаційних ресурсів. Фізичний рівень відповідає за фізичний зв'язок між кінцевими робочими станціями. Це пов'язане із кодуванням, довжиною хвилі та передачею даних. Також необхідно враховувати фізичні носії інформації, пристрої вводу-виводу, блоки живлення та ін. Звичайна втрата живлення та обрив мережевого кабелю можуть призвести до хаосу в комп'ютерній мережі.

Значну загрозу являє собою й електромагнітне підслуховування. Соціальна інженерія є значною загрозою для інформаційних ресурсів. Радіочастотні та електромагнітні перешкоди, вплив бруду, вологи та температури можна віднести до загроз фізичного рівня.

Для протидії загрозам на фізичному рівні слід застосовувати відеоспостереження, реєстрацію та блокування входу та виходу, PIN-паролі, біометрична перевірка даних особи. Необхідно обмежити фізичний доступ до інформації. Для протидії соціальній інженерії необхідно здійснювати підготовку користувачів комп'ютерних мереж. Слід подбати також про резервне копіювання та аварійне відновлення критично важливих інформаційних ресурсів.

Канальний рівень моделі OSI

З погляду інформаційної безпеки канальний рівень є достатньо дослідженим і відповідає за формування та доставку кадру без помилок. На цьому рівні використовується апаратна MAC-адресація та здійснюється обчислення контрольної суми.

Широко застосовуються зловмисниками атаки на підміну MAC-адреси, атаки на ARP і Spanning-Tree протоколи, кінцевою метою яких є перехоплення трафіку та одержання доступу до більш важливої конфіденційної інформації.

Можливості побудови віртуальних мереж VLAN, які реалізовані на базі комутаторів, створюють загрозу захоплення зловмисником усіх портів VLAN. Активне впровадження бездротових мереж IEEE 802.11 створило загрозу безконтрольного підключення зловмисників до них.

Протидіяти наведеним загрозам на канальному рівні можна шляхом застосування MAC-фільтрації, використання брандмауерів для ізоляції різних зон у мережі та відмови від VLAN, а для бездротових мереж необхідно застосовувати шифрування, автентифікацію та фільтрацію MAC-адрес.

Мережевий рівень моделі OSI

Основним завданням протоколів мережевого рівня є ідентифікація ресурсів мережі, адресація та обчислення маршруту між відправником та одержувачем інформації. Сучасні комутатори, маршрутизатори та брандмауери працюють саме на мережевому рівні та створюють таблиці маршрутизації, правила фільтрації і забезпечують різноманітні сервіси — NAT, DNS, DHCP.

Більшість загроз мережевого рівня пов'язані з використанням протоколу IP — підміна IP-адреси, підміна маршруту, перехоплення зловмисником діапазону IP-адреси та проблеми одноразової ідентифікації за IP-адресою.

Відповідно до широкого застосування та великої кількості загроз мережевого рівня реалізується протидія їм за допомогою цілої низки додаткових механізмів.

Так, NAT — трансляція мережевих адрес розширюється функцією *Port Address Translations* (PAT), що дозволяє одній публічній IP-адресі бути пов'язаною з декількома віртуальними портами і забезпечувати в Інтернеті більшу анонімність. Побудова на базі протоколу IPSec віртуальних приватних мереж — VPN із застосуванням технологій брандмауерів значно підвищують рівень інформаційної безпеки у мережі. Проблеми, пов'язані із DHCP, можна вирішити шляхом скорочення часу оренди адрес. Отже, реалізація жорсткої політики управління маршрутами у поєднанні із застосуванням брандмауерів та моніторингом програмного забезпечення утворюють надійний комплекс заходів протидії загрозам на мережевому рівні.

Транспортний рівень моделі OSI

Транспортний рівень моделі OSI є першим суто логічним рівнем цієї моделі. Протоколи транспортного рівня, такі як TCP та UDP, здійснюють доставку пакетів та дейтаграм від відправника до одержувача та орієнтовані на підвищення продуктивності передачі інформації. Широке використання та відсутність перевірки джерел інформації утворюють ряд загроз, що властивих для протоколів транспортного рівня.

Поширеність призвела до активного підключення прикладних програм та інших протоколів саме до портів протоколів транспортного рівня. Програми-трояни та шпигунське програмне забезпечення також часто орієнтовані на відкриті порти протоколів транспортного рівня.

Перехоплення даних може реалізовуватись на основі протоколу UDP, через відсутність у нього контролю за цілісністю інформації. Більш складні атаки, такі як перехоплення та підміна сеансів, реалізуються на основі протоколу TCP.

Врешті-решт атаки на протоколи транспортного рівня можуть призвести до захоплення контролю над мережею.

Протидія загрозам транспортного рівня здійснюється шляхом активного використання брандмауерів із динамічною фільтрацією вмісту пакетів, обмеження доступу прикладних програм до портів протоколів TCP, UDP та посилення механізмів ідентифікації.

Сеансовий рівень моделі OSI

Завданням протоколів сеансового рівня є сприяння в обміні інформацією шляхом встановлення, підтримки, синхронізації, управління та завершення з'єднання з можливою ідентифікацією та автентифікацією сторін. Типовими протоколами є SSL та Kerberos, що використовують сервери автентифікації та криптографічні алгоритми.

Основними загрозами для протоколів сеансового рівня можуть бути слабкі або відсутні механізми автентифікації, перехоплення імені та паролю користувача при передачі їх у відкритому вигляді, перехоплення сеансів та одержання несанкціонованого доступу до даних шляхом необмеженої кількості спроб на встановлення сеансу. Уникнути загроз сеансового рівня можна за допомогою використання криптографічних алгоритмів, передачі даних та паролів у зашифрованому вигляді, обмеження часу дії паролів та кількості спроб на встановлення з'єднання.

Представницький рівень моделі OSI

Протоколи представницького рівня здійснюють організацію даних, що передаються від прикладного рівня у мережу, та забезпечують уніфікацію даних, при їх обміні між платформами із різними схемами кодування. Крім того, протоколи представницького рівня реалізують контроль за стисненням та шифруванням даних.

Для протоколів представницького рівня властиві загрози, пов'язані із неправильною обробкою даних, через недоліки у програмному забезпеченні та криптографічних алгоритмах та помилками при введені інформації та її випадковому витоку.

Заходи захисту інформації проти загроз представницького рівня спрямовані на ретельний контроль даних, що вводяться до програм, та моніторинг їх обробки, а також на постійну

модернізацію та моніторинг криптографічних алгоритмів.

Прикладний рівень моделі OSI

Протоколи прикладного рівня забезпечують сервісами кінцевого користувача мережі і всі функції, що безпосередньо не стосуються мережевих операцій, реалізовані саме на цьому рівні.

Протоколи верхнього рівня охоплюють увесь спектр сучасних послуг мережі — HTTP, FTP SMTP, SNMP, DNS, Telnet та багато інших.

Відкритий характер протоколів прикладного рівня зумовлює велику кількість загроз, найпоширенішою з яких є передача конфіденційної інформації у відкритому вигляді. Ідентифікація та автентифікація користувачів із подальшою авторизацією утворює загрозу перехоплення або підбору логіну та паролю.

Надлишковий або невиправдано обмежений доступ користувачів до ресурсів мережі створюють загрозу складності конфігурування системи захисту інформації.

Значну загрозу становлять віруси та шпигунське програмне забезпечення, які діють саме на прикладному рівні.

Організувати протидію загрозам прикладного рівня можна шляхом реалізації комплексних систем захисту інформації із чіткою та однозначною політикою безпеки, залучення потужних механізмів розмежування доступу користувачів до ресурсів мережі і застосування технологій криптографічного та антивірусного захисту.

Узагальнені вразливості та заходи убезпечення на різних рівнях моделі взаємодії відкритих систем наведено в табл. 1.

Таблиця 1

Класифікація вразливостей та заходів убезпечення за рівнями моделі OSI

Рівень моделі OSI	Вразливості	Заходи убезпечення
Фізичний рівень	Втрата потужності Фізичні крадіжки даних і устаткування Фізичне пошкодження або знищення даних і устаткування Несанкціоновані зміни у функціональному середовищі (передачі даних, змінних носіїв, додавання / видалення ресурсів) Вимкнення фізичних каналів передачі даних Приховане перехоплення даних з клавіатури та інших засобів введення інформації	Закриття периметру і корпусів мережі Електронний механізм блокування для реєстрації та авторизації Відео та аудіо спостереження Застосування PIN-кодів і паролів Біометричні системи аутентифікації Електромагнітне екранування
Канальний рівень	Підміна MAC-адреси Обхід технологій VLAN Використання помилок алгоритму Spanning Tree для передачі пакетів у нескінченний цикл У бездротових мережах безкоштовне несанкціоноване підключення до мережі Затоплення комутаторами всіх портів VLAN	Фільтрація MAC-адрес Не використовувати мережі VLAN для захисту інформації Фізична ізоляція різних зон мережі за допомогою як брандмауерів Бездротові мережі необхідно захищати з використанням вбудованого шифрування, автентифікації та фільтрації MAC-адрес
Мережевий рівень	Підміна маршруту — поширення неправдивої топології мережі Підміна IP-адреси — джерело помилкового рішення після дії шкідливих пакетів Проблеми одноразової ідентифікації	Застосування політики управління маршрутами — жорсткі фільтри маршрутів і антиспуфінг Використання міжмережевих екранів із потужною політикою фільтрації Моніторинг програмного забезпечення, для мінімізації можливих зловживань

Закінчення табл. 1

Рівень моделі OSI	Вразливості	Заходи убезпечення
Трансортний рівень	Неправильна передача пакетів Відмінності в реалізації транспортного протоколу дозволяють здійснити несанкціонований доступ Перевантаження транспортного рівня за рахунок великої кількості звернень до номерів портів обмежує можливості для ефективної фільтрації трафіку Механізми передачі пакетів можуть бути предметом підміни і атаки на основі сформованих пакетів і призводити до руйнування або захоплення контролю над мережею	Жорсткі правила брандмауера обмежують доступ до певних протоколів передачі інформації, таких як номер портів TCP/UDP або тип ICMP Перевірка брандмауером пакетів з урахуванням аналізу вмісту та з'єднання дозволяє закрити доступ до мережі шкідливим пакетам Посилення механізмів ідентифікації з'єднання, щоб уникнути нападу і захоплення контролю над мережею
Сеансовий рівень	Слабкі або відсутні механізми автентифікації Передача під час сеансу інформації, такої як ім'я користувача і пароль у відкритому вигляді, дозволяє її перехоплення та несанкціоноване використання Ідентифікація сеансу може бути предметом підміни і викрадення Витік інформації на основі невдалих спроб автентифікації Здійснення атаки на облікові дані для доступу в разі необмеженої кількості спроб на встановлення сеансу	Зашифрований обмін і зберігання паролів Обмежений термін дії для паролів та повноважень користувачів Захист інформації про ідентифікацію сеансу за допомогою криптографічних засобів Обмеження невдалих спроб встановлення сеансу за допомогою механізму синхронізації, а не блокування.
Представницький рівень	Погана обробка даних може призвести до збою програми Ненавмисне або необачне використання зовнішніх даних, що вводяться в контексті управління може призвести до віддаленої маніпуляції або витоку інформації Криптографічні недоліки можуть бути використані для обходу захисту конфіденційності	Ретельна перевірка даних, що вводяться до програми Контроль дій користувачів та функцій управління Ретельний і безперервний огляд рішень криптографії для забезпечення поточних завдань безпеки до загрози, що постійно оновлюються
Прикладний рівень	Використання безкоштовних ресурсів та програм невідомого походження Недоліки програмного забезпечення, наявність *backdoors* і можливостей обійти стандартні засоби управління безпекою Недостатній контроль засобів захисту за принципом «все або нічого», в результаті чого або надмірний або недостатній доступ до мережі Надмірно ускладнений механізм контролю безпеки, можна обійти або важко застосувати Збої програмного забезпечення при великих навантаженнях	Контроль на рівні програм визначає і забезпечує доступ до ресурсів. Простий та прозорий механізм забезпечення безпеки, з метою уникнення складностей у конфігуруванні. Реалізація криптографічного та антивірусного захисту даних

Потужний функціональний комплекс сучасних інформаційно-комунікаційних систем та мереж надає велику кількість сервісів користувачам та має значну кількість вразливостей, протидія яким здійснюється на різних рівнях моделі OSI. Але застосування лише окремих механізмів та заходів захисту інформації не дає можливості побудувати повноцінну захищену комп'ютерну систему та описати її. Так активне впровадження бездротових технологій за стандартом

IEEE 802.11 потребує нових рішень інформаційної безпеки, що поєднують функції захисту інформації із доступністю для користувачів.

Розширена дев'ятирівнева модель

Семирівнева модель OSI достатньо повно і ефективно описує взаємодію при передачі інформації в комп'ютерних мережах. Разом з тим, питання інформаційної безпеки часто виходять за межі семи рівнів і відповідно модель потребує розширення, з урахуванням сучасних особливостей захисту інформації (рис. 2).

Пропонується доповнити модель двома рівнями — користувачів та політик та перетворення моделі у дев'ятирівневу.

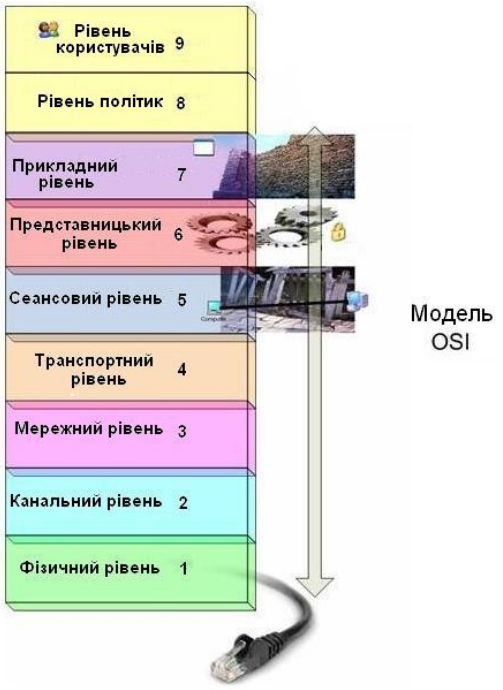

Рис. 2. Розширена модель OSI

Таким чином, взаємодія користувачів із прикладними програмами описується на дев'ятому рівні, а політики управління діями користувачів та безпеки — на восьмому. Політика управління забезпечує контроль за діями користувачів на дев'ятому рівні, а політика безпеки реалізує набір правил та рекомендацій для решти семи рівнів моделі OSI. У рамках восьмого рівня можна сформувати модель об'єкту, модель загроз, модель порушника, модель захисту інформації та політику безпеки.

Йдеться про певний набір стандартів та нормативних документів, які можна адаптувати до задач кожної конкретної мережі [4; 5].

Так, політика якості послуг формується відповідно до вимог міжнародного стандарту ISO 9001:2008 «Системи менеджменту якості. Вимоги», політика безпеки повинна відповідати вимогам міжнародного стандарту ISO/IEC 27001:2005 «Системи менеджменту інформаційної безпеки. Вимоги» (табл. 2).

Таблиця 2

Реалізація 8 та 9 рівнів моделі OSI

Рівень моделі OSI	Назва	Базові функції
9	Рівень користувачів	Нормативні документи для користувачів
		Нормативні документи для адміністраторів та адміністраторів безпеки
		Нормативні документи для сторонніх організацій
8	Рівень політик	Політика управління діями користувачів
		Політика безпеки — стандарт ISO/IEC 27001:2005
		Політики якості послуг — стандарт ISO 9001:2008

На дев'ятому рівні пропонується реалізовувати набір інструкцій та інших нормативних документів для організації роботи користувачів із прикладними програмами у сучасних інформаційно-комунікаційних системах та мережах.

Реалізація всіх інструкцій для різних користувачів відбувається згідно з політикою управління восьмого рівня

Висновки

За результатами досліджень проведена класифікація вразливостей сучасних інформаційно-комунікаційних систем та мереж та заходів захисту інформації відповідно до семирівневої моделі OSI. Встановлено, що семирівнева модель досить повно описує одмін інформацією в мережі, але не охоплює всього переліку проблем інформаційної безпеки. З метою побудови комплексних систем захисту інформації для інформаційно-комунікаційних систем та мереж пропонується розширити семирівневу модель до дев'ятирівневої — за рахунок восьмого рівня — рівня політик та дев'ятого — рівня користувачів.

ЛІТЕРАТУРА

1. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. — 4-е изд. — Питер, 2010. —943 с.

2. *Шаньгин В. Ф.* Защита компьютерной информации / В. Ф. Шаньгин. — М. :ДМК Пресс, 2008. — 544 с.

3. *Kachold Lisa.* Layer 8 Linux Security: OPSEC for Linux Common Users, Developers and Systems Administrators // Linuxgazette.net, July 2009 (# 164).

4. *Системи* менеджменту якості. Вимоги ISO 9001:2008. — 4-те видання 2008.11.15.

5. *Системи* менеджменту інформаційної безпеки. Вимоги ISO/IEC 27001:2005.

Стаття надійшла до редакції 03.09.2012.