7. *Настанова* з улаштування контейнерних майданчиків: ДСТУ-Н Б Б.2.2-7:2013. – [Чинний від 2014.04.01]. – К. : Український державний науково-дослідний інститут проблем водопостачання, водовідведення та охорони навколишнього природного середовища УкрВОДГЕО, 2013. – (Національний стандарт України).

8. *Про затвердження* Методики роздільного збирання побутових відходів [Електронний ресурс] : Наказ Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України від 01.08.2011 № 133. – Режим доступу : http://zakon.rada.gov.ua/laws/show/z1157-11.

УДК 004.7

Д.Б. Мехед, канд. пед. наук
Чернігівський національний технологічний університет, м. Чернігів, Україна

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Д.Б. Мехед, канд. пед. наук
Черниговский национальный технологический университет, г. Чернигов, Украина

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Dmytro Mekhed, PhD in Pedagogical Sciences
Chernihiv National University of Technology, Chernihiv, Ukraine

INFORMATION SECURITY IN COMPUTER NETWORKS

Розглянуто комп'ютерні мережі, типи їх побудови, зроблено аналіз переваг і недоліків різних типів мереж. Проаналізовано основні типи передачі інформації, виділено їхні переваги й недоліки, можливість втрати інформації, а також методи її захисту.

***Ключові слова**: комп'ютерна мережа, передача інформації, захист інформації.*

Рассмотрены компьютерные сети, типы их построения, сделан анализ преимуществ и недостатков различных типов сетей. Проанализированы основные типы передачи информации, выделены их преимущества и недостатки, возможность потери информации, а также методы ее защиты.

***Ключевые слова**: компьютерная сеть, передача информации, защита информации.*

The article deals with computer networks, types of construction, the analysis of the advantages and disadvantages of different types of networks. The basic types of information transmission, highlighted their advantages and disadvantages, losing information and methods of protection.

***Key words**: computer network, communication activity, information security.*

Постановка проблеми. Нині в Україні у зв'язку з входженням у світовий інформаційний простір швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Створюються локальні і регіональні обчислювальні мережі, великі території охоплені мережами сотового зв'язку, факсимільний зв'язок став доступним для широкого кола користувачів. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У зв'язку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації [1]. Аналіз стану захисту інформації – це комплексне вивчення фактів, подій, процесів, явищ, пов'язаних з проблемами захисту інформації, у тому числі даних про стан роботи з виявлення можливих каналів витоку інформації, про причини й обставини, що сприяють витоку і порушенню режиму секретності (конфіденційності) у ході повсякденної діяльності підприємства.

Аналіз останніх досліджень і публікацій. Дослідженню інформаційної безпеки присвячені роботи В.В. Баранника, В.М. Богуна, С.В. Віхорева, І.Д. Горбенко, Ю.І. Грицюк, С.В. Казмирчук, Г.Ф. Конаховича, О.Г. Корченка, М.Г. Луцького, А.І. Марущака, В.П. Мельнікова, В.В. Мохора, О.М. Новікова, О.В. Олійника, О.В. Сосніна, С.В. Толюпи, В.О. Хорошко, О.К. Юдіна та ін.

Дослідження різноманітних аспектів інформаційно-аналітичної діяльності здійснювали Т.В. Абрамова, С.С. Алдишев, В.П. Александрова, А.А. Атаян, С.Ф. Багаундінова, Т.В. Вдовіна, А.В. Горячов, Р.О. Гуревич, М.І. Жалдак, О.П. Значенко, В.Г. Кальченко, Н.В. Кисіль, В.І. Клочко, Н.В. Морзе, С.Ю. Нікіфорова, О.В. Пархоменко, С.А. Раков, М.В. Селіна, Ю.М. Ткач, В.А. Сластьонін та ін.

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на значний обсяг накопичених у цій сфері знань, недостатньо дослідженою залишилась проблема захисту інформації комп'ютерних мереж.

Мета статті. Головною метою цієї роботи є аналіз основних типів передачі інформації за допомогою комп'ютерних мереж. Визначення основних причин можливості втрати інформації та методи її захисту.

Виклад основного матеріалу. Комп'ютерна мережа – система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа – це система зв'язку через кабельне чи повітряне середовище, власне комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, переважно. різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання інформації у комп'ютерних мережах можуть бути телефонні та спеціальні мережеві кабелі: коаксіальні, виті пари, волоконно-оптичні, а також радіохвилі та світлові сигнали [2]. Мережа дає можливість окремим співробітникам організації взаємодіяти один з одним і звертатися до спільно використовуваних ресурсів; дозволяє їм одержувати доступ до даних, що зберігаються на персональних комп'ютерах у видалених офісах, і встановлювати зв'язок з постачальниками [1]. Мережеві операції регулюються набором правил і угод (званих мережевим протоколом), який визначає: типи роз'ємів і кабелів, види сигналів, формати даних, алгоритми роботи мережевих інтерфейсів, способи контролю та виправлення помилок, взаємодію прикладних процесів та ін.

До теперішнього часу розроблено значну кількість різновидів організаційної та архітектурної побудови комп'ютерних мереж. Системну їх класифікацію можна здійснити за такими критеріями [4]:

1) за масштабом – локальні та глобальні;

2) за способом організації – централізовані і децентралізовані;

3) за топологією (конфігурацією) – зіркоподібні, кільцеві, шинні, змішані.

Різновиди комп'ютерних мереж за виділеними значеннями перерахованих критеріїв характеризуються таким чином [4]:

– локальні обчислювальні мережі – мережі, вузли яких розташовуються на невеликих відстанях один від одного (у різних приміщеннях тієї самої будівлі, в різних будівлях, розташованих на одній території);

– глобальні обчислювальні мережі – вузли мережі розташовані на значних відстанях один від одного (у різних частинах великого міста, у віддалених один від одного населених пунктах (які включають у себе цегляні, панельні і дерев'яні будинки), у різних регіонах країни і навіть у різних країнах).

Централізовані локальні обчислювальні мережі – мережі, в яких передбачено головний вузол, через який здійснюються всі обміни інформацією і який здійснює управління всіма процесами взаємодії вузлів.

Децентралізовані обчислювальні мережі – мережі з відносно рівноправними вузлами, управління доступом до каналів передачі даних у цих мережах розподілено між вузлами.

На основі навіть такого швидкого розгляду можливих структур обчислювальних мереж неважко зробити висновок, що для тих об'єктів (підприємств, установ, інших організацій), в яких регулярно обробляються значні обсяги інформації, найбільш доцільною буде комбінована структура комп'ютерних обчислювальних мереж.

Мережева взаємодія. Це питання розглянемо на прикладі найбільш поширеної і визнаної еталонної моделі взаємодії відкритих систем OSI [2].

В основу еталонної моделі покладена ідея декомпозиції процесу функціонування відкритих систем на рівні, причому розбиття на рівні проводиться таким чином, щоб згрупувати в межах кожного з них функціонально найбільш близькі компоненти. Крім того,

потрібно, щоб взаємодія між суміжними рівнями була мінімальною, кількість рівнів порівняно невеликим, а зміни, вироблені в межах одного рівня, не вимагали б перебудови суміжних.

Окремий рівень, таким чином, являє собою логічно і функціонально замкнену підсистему, що сполучається з іншими рівнями за допомогою спеціально визначеного інтерфейсу. В межах моделі OSI кожен конкретний рівень може взаємодіяти тільки із сусідніми. Сукупність правил (процедур) взаємодії об'єктів однойменних рівнів називається протоколом.

Еталонна модель містить сім рівнів (знизу вгору): фізичний; канальний (або передачі даних); мережевий; транспортний; сеансовий; представницький; рівень додатків.

Кожен рівень передавальної станції в цій ієрархічній структурі взаємодіє з відповідним рівнем приймаючої станції за допомогою нижчих рівнів. При цьому кожна пара рівнів за допомогою службової інформації повідомлень встановлює між собою логічне з'єднання, забезпечуючи тим самим логічний канал зв'язку відповідного рівня. За допомогою такого логічного каналу кожна пара верхніх рівнів може забезпечувати між собою взаємодію, абстрагуючись від особливостей нижніх [4]. Іншими словами, кожен рівень реалізує строго визначений набір функцій, який може використовуватися верхніми рівнями незалежно від деталей реалізації цих функцій (табл.).

Таблиця

Семирівнева модель протоколів мережевого обміну OSI

№ рівня	Найменування рівня	Зміст
7	Рівень додатків	Надання послуг на рівні кінцевого користувача
6	Рівень представлення даних	Інтерпретація та стиск даних
5	Рівень сеансів	Аутентифікація та перевірка повноважень
4	Транспортний рівень	Забезпечення коректної передачі даних
3	Мережевий рівень	Маршрутизація та ведення обліку
2	Канальний рівень	Передача та прийом пакетів, визначення апаратних адрес
1	Фізичний рівень	Кабель або фізичний носій інформації

Розглянемо докладніше функціональне призначення кожного рівня.

Фізичний рівень. Фізичний рівень забезпечує електричні, функціональні та процедурні засоби встановлення, підтримки і роз'єднання фізичного з'єднання. Реально він представлений апаратурою генерації та управління електричними сигналами і каналом передачі даних. На цьому рівні дані представлено у вигляді послідовності бітів або аналогового електричного сигналу. Завданням фізичного рівня є передача послідовності бітів з буфера відправника в буфер одержувача.

Канальний рівень. Протоколи канального рівня (або протоколи управління ланкою передачі даних) посідають особливе місце в ієрархії рівнів: вони є сполучною ланкою між реальним каналом, що забезпечує безпомилкову передачу даних. Цей рівень використовується для організації зв'язку між двома станціями за допомогою наявного (зазвичай ненадійного) каналу зв'язку. При цьому станції можуть бути пов'язані декількома каналами.

Протокол канального рівня повинен забезпечити:

– незалежність протоколів вищих рівнів від використовуваного середовища передачі даних;

– кодонезалежність переданих даних;

– вибір якості обслуговування під час передачі даних.

На цьому рівні дані представлено кадром, який містить інформаційне поле, а також заголовок і кінцевик (трейлер), що привласнюються протоколом. Заголовок містить службову інформацію, використовувану протоколом канального рівня приймаючої станції і служить для ідентифікації повідомлення, правильного прийому кадрів, віднов-

лення і повторної передачі у разі помилок і т. ін. Кінцевик містить перевірочне поле, що служить для корекції та виправлення помилок, внесених каналом. Завдання протоколу канального рівня – складання кадрів, правильна передача і прийом послідовності кадрів, контроль послідовності кадрів, виявлення та виправлення помилок в інформаційному полі (якщо це необхідно).

Мережевий рівень. Мережевий рівень надає транспортному рівню набір послуг, головними з яких є наскрізна передача блоків даних між передавальною і приймальною станціями (тобто виконання функцій маршрутизації та ретрансляції) і глобальне адресування користувачів. Іншими словами, знаходження одержувача за вказаною адресою, вибір оптимального (в умовах цієї мережі) маршруту та доставка блока повідомлення за вказаною адресою.

Таким чином, на межі мережевого і транспортного рівнів забезпечується незалежність процесу передачі даних від використовуваних середовищ за винятком якості обслуговування. Під якістю обслуговування розуміється набір параметрів, що забезпечують функціонування мережевої служби, що відображає робочі (транзитна затримка, коефіцієнт невиявлених помилок та ін.) та інші характеристики (захист від несанкціонованого доступу, вартість, пріоритет та ін.). Система адрес, використовувана на мережевому рівні, повинна мати ієрархічну структуру і забезпечувати такі властивості: глобальну однозначність, маршрутну незалежність і незалежність від рівня послуг.

На мережевому рівні дані представлено у вигляді пакета, який містить інформаційне поле і заголовок, який присвоюється протоколом. Заголовок пакета містить керуючу інформацію, яка вказує адресу відправника, можливо, маршрут і параметри передачі пакета (пріоритет, номер пакета в повідомленні, параметри безпеки, максимум ретрансляції та ін.). Розрізняють такі види мережевої взаємодії:

– зі встановленням з’єднання – між відправником та одержувачем спочатку за допомогою службових пакетів організовується логічний канал (відправник – відправляє пакет, одержувач – чекає отримання пакунків плюс взаємне повідомлення про помилки), який роз’єднується після закінчення повідомлення або у разі невиправної помилки. Такий спосіб використовується протоколом X.25;

– без встановлення з’єднання (дейтаграмний режим) – обмін інформацією здійснюється за допомогою дейтаграм (різновид пакетів), незалежних один від одного, які приймаються також незалежно один від одного і збираються в повідомлення на приймальній станції. Такий спосіб використовується в архітектурі протоколів DARPA.

Транспортний рівень. Транспортний рівень призначений для наскрізної передачі даних через мережу між кінцевими користувачами – абонентами мережі. Протоколи транспортного рівня функціонують тільки між кінцевими системами.

Основними функціями протоколів транспортного рівня є розбиття повідомлень або фрагментів повідомлень на пакети, передача пакетів через мережу і збір пакетів. Вони також виконують такі функції: відображення транспортного адреси в мережі, мультиплексування і розщеплення транспортних сполучень, межкінцеве управління потоком і виправлення помилок. Набір процедур протоколу транспортного рівня залежить як від вимог протоколів верхнього рівня, так і від характеристик мережевого рівня.

Найбільш відомим протоколом транспортного рівня є TCP (Transmission Control Protocol), використовуваний в архітектурі протоколів DARPA і прийнятий за стандарт [2]. Він використовується як високонадійний протокол взаємодії між комп’ютерами в мережі з комутацією пакетів.

Протоколи верхніх рівнів. До протоколів верхніх рівнів відносяться протоколи сеансового, представницького і прикладного рівнів. Вони спільно виконують одну задачу – забезпечення сеансу обміну інформацією між двома прикладними процесами, причому

інформація повинна бути представлена в тому вигляді, який зрозумілий обом процесам. Тому зазвичай ці три рівня розглядають спільно. Під прикладним процесом розуміється елемент кінцевої системи, який бере участь у виконанні одного або декількох завдань з оброблення інформації. Зв'язок між ними здійснюється за допомогою прикладних об'єктів – елементів прикладних процесів, що беруть участь в обміні інформацією. При цьому протоколи верхніх рівнів не враховують особливості конфігурації мережі, каналів і засобів передачі інформації.

Протоколи представницького рівня надають послуги за погодженням синтаксису передачі (правил, які задають подання даних при їх передачі) і конкретним уявленням даних у прикладній системі. Іншими словами, на представницькому рівні здійснюється синтаксичне перетворення даних від виду, використовуваного на прикладному рівні, до виду, використовуваному на інших рівнях (і навпаки).

Прикладний рівень, будучи самим верхнім у еталонній моделі, забезпечує доступ прикладних процесів у середовище взаємодії відкритих систем. Основним завданням протоколів прикладного рівня є інтерпретація даних, отриманих з нижніх рівнів, і виконання відповідних дій у кінцевій системі в межах прикладного процесу. Зокрема, ці дії можуть полягати в передачі управління певним службам операційної системи разом з відповідними параметрами.

Крім того, прикладний рівень може надавати послуги з ідентифікації й аутентифікації партнерів, встановлення повноважень для передачі даних, перевірки параметрів безпеки, управління діалогом та ін.

Перелічимо основні загрози, що представляють реальну небезпеку для мереж передачі даних.

1. Прослуховування каналів, тобто запис і подальший аналіз всього потоку повідомлень. Прослуховування здебільшого не помічається легальними учасниками інформаційного обміну.

2. Умисне знищення або спотворення (фальсифікація) повідомлень в мережі, а також включення в потік помилкових повідомлень. Неправдиві повідомлення можуть бути сприйняті одержувачем як справжні.

3. Присвоєння зловмисником своєму вузлу або ретранслятору чужого ідентифікатора, що дає можливість отримувати або відправляти повідомлення від чужого імені.

4. Навмисний розрив лінії зв'язку, що призводить до повного припинення доставки всіх (або тільки обраних зловмисником) повідомлень.

5. Впровадження мережевих вірусів. Передача по мережі тіла віруса з його подальшою активізацією користувачем віддаленого або локального вузла.

Відповідно до цього специфічні завдання захисту в мережах передачі даних полягають у такому:

1. Аутентифікація однорівневих об'єктів, що полягає у підтвердженні справжності одного або декількох взаємодіючих об'єктів під час обміну інформацією між ними.

2. Контроль доступу та захист від несанкціонованого використання ресурсів мережі.

3. Маскування даних, що циркулюють у мережі.

4. Контроль і відновлення цілісності всіх даних, що знаходяться в мережі.

5. Арбітражне забезпечення або захист від можливих відмов від фактів відправки, прийому або змісту відправлених або прийнятих даних.

Висновки і пропозиції. Враховуючи вищезазначене стосовно різних рівнів семирівневого протоколу передачі даних у мережі, завдання захисту інформації в мережі можуть бути конкретизовані таким чином.

1. Фізичний рівень – контроль електромагнітних випромінювань ліній зв'язку та пристроїв, підтримка комутаційного обладнання в робочому стані. Захист на цьому рі-

вні забезпечується за допомогою екрануючих пристроїв, генераторів перешкод, засобів фізичного захисту передавального середовища.

2. Канальний рівень – збільшення надійності захисту (за необхідності) за допомогою шифрування переданих по каналу даних. У цьому випадку шифруються всі передані дані, включаючи службову інформацію.

3. Мережевий рівень – найбільш вразливий рівень з погляду захисту. На ньому формується вся маршрутизована інформація, відправник і одержувач фігурують явно, здійснюється управління потоком.

Крім того, протоколами мережевого рівня пакети обробляються на всіх маршрутизаторах, шлюзах та інших проміжних вузлах. Майже всі специфічні мережеві порушення здійснюються з використанням протоколів цього рівня (читання, модифікація, знищення, дублювання, переорієнтація окремих повідомлень або потоку в цілому, маскування під інший вузол тощо). Захист від таких загроз здійснюється протоколами мережевого і транспортного рівнів і за допомогою засобів криптографічного захисту. На цьому рівні може бути реалізована вибіркова маршрутизація.

4. Транспортний рівень – здійснює контроль за функціями мережевого рівня на приймальному і передавальному вузлах (на проміжних вузлах протокол транспортного рівня не функціонує). Механізми транспортного рівня перевіряють цілісність окремих пакетів даних, послідовності пакетів, пройдений маршрут, час відправлення і доставки, ідентифікацію та аутентифікацію відправника й одержувача та інші функції. Всі активні загрози стають видимими на цьому рівні.

Гарантом цілісності переданих даних є криптозахист як самих даних, так і службової інформації. Ніхто, крім тих, хто має секретний ключ одержувача і / або відправника, не може прочитати або змінити інформацію таким чином, щоб зміна залишилась непоміченою.

Аналіз трафіку забезпечується передачею повідомлень, що не містять інформацію, але виглядають як реальні повідомлення. Регулюючи інтенсивність цих повідомлень залежно від обсягу переданої інформації, можна постійно домагатися рівномірного трафіку. Проте всі ці заходи не можуть захистити від загрози знищення, переорієнтації або затримки повідомлення. Єдиним захистом від таких порушень може бути паралельна доставка дублікатів повідомлення іншими шляхами.

5. Протоколи верхніх рівнів забезпечують контроль взаємодії прийнятої або переданої інформації з локальною системою. Протоколи сеансового і представницького рівня функцій захисту не виконують. У функції захисту протоколу прикладного рівня входить управління доступом до певних наборів даних, ідентифікація й аутентифікація певних користувачів, а також інші функції, які визначаються конкретним протоколом. Більш складними ці функції є у разі реалізації повноважної політики безпеки в мережі.

Список використаних джерел

1. *Камалян А. К.* Комп’ютернімережі та засоби захисту інформації : навч. посіб. / [А. К. Камалян, С. А. Кульов, К. М. Назаренко та ін.]. – Воронеж : ВДАУ, 2003. – 119 с.

2. *Комп’ютерні* мережі [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/Комп%27ютерна_мережа.

3. *Концепція* технічного захисту інформації в галузі зв’язку України [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua.

4. *Оліфер В. Г.* Комп’ютерні мережі. Принципи, технології, протоколи / В. Г. Оліфер, Н. А. Оліфер. – СПб. : Пітер, 2002. – 672 с.

5. *Тардаскін М. Ф.* Технічний захист комерційної таємниці підприємства зв’язку : навч. посіб. / за ред. М. В. Захарченка, М. Ф. Тардаскін, В. Г. Кононович. – Одеса : ОНАЗ, 2002. – 76 с.