Сергій ПАХАРЧУК
здобувач вищої освіти 1 курсу ОС «Бакалавр»
спеціальності 203 «Садівництво та виноградарство»
Ірина МУШЕНИК
канд. екон. наук, доцент кафедри математики,
інформатики та академічного письма
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Життя сучасного суспільства неможливо уявити без використання сучасних інформаційних технологій. Активне впровадження сучасної комп'ютерної техніки та мережевих технологій в будь-яку сферу життя майже кожної людини призвело до того, що величезні обсяги різноманітної інформації в цифровій формі зберігаються в комп'ютерних системах та передаються з використанням комп'ютерних мереж. Серед всього обсягу інформаційних ресурсів є інформація, що має статус конфіденційної і потребує обмеження в доступі. Це може бути інформація, що містить державну таємницю, комерційну таємниці, особисті данні і таке інше. Природно, виникає потреба захистити таку інформацію від несанкціонованого доступу, крадіжки, знищення і інших злочинних дій. Концентрація інформації в цифровій формі в комп'ютерних системах примушує все більше приділяти увагу задачі її захисту [4, с. 216].

Питання безпеки і захисту інформації в комп'ютерних системах та мережах від несанкціонованого доступу є важливими та актуальними на сьогоднішній день. В останні роки проблеми, пов'язані із захистом інформації турбують як фахівців в галузі комп'ютерної безпеки, так і численних звичайних користувачів персональних комп'ютерів. Дослідження в цьому напрямку призвели до виникнення окремої галузі – інформаційної безпеки. Інформаційна безпека має декілька аспектів: правовий, програмно-технічний, організаційний, морально-етичний [5, с.96].

Програмні засоби захисту інформації – системні та прикладні програми, призначені для захисту інформації, що передається по телекомунікаційним каналам, зберігається в базах даних і на інформаційних носіях. Найчастіше

програмні засоби захисту інформації застосовують для виконання таких процесів як ідентифікація й автентифікація користувачів, розмежування доступу користувачів до інформаційної мережі, парольний захист і перевірка повноважень, шифрування інформації, а також її захист від несанкціонованих змін, зчитування, копіювання[3].

Судячи по зростаючій кількості публікацій і компаній, які професійно займаються захистом інформації в комп'ютерних системах, вирішенню цієї задачі надається велике значення. Однією із найбільш очевидних причин порушення системи захисту є навмисний несанкціонований доступ (НСД) до конфіденційної інформації з боку нелегальних користувачів і наступні небажані маніпуляції із цією інформацією [2].

Існує несанкціонований доступ до інформації, яка знаходиться в комп'ютерних мережах. Він буває: непрямим – без фізичного доступу до елементів локальних мереж; прямим – з фізичним доступом до елементів локальних мереж. В даний час існують наступні шляхи несанкціонованого отримання інформації (канали витоку інформації): застосування підслуховуючих пристроїв; дистанційне фотографування; перехоплення електромагнітних випромінювань; розкрадання носіїв інформації і виробничих відходів; зчитування даних у масивах інших користувачів; копіювання носіїв інформації; несанкціоноване використання терміналів; маскування під зареєстрованого користувача за допомогою розкрадання паролів та інших реквізитів розмежування доступу; використання програмних пасток; отримання даних, що захищаються за допомогою серії дозволених запитів; використання недоліків мов програмування і операційних систем; умисне включення в бібліотеки програм спеціальних блоків типу «троянських коней»; незаконне підключення до апаратури або ліній зв'язку обчислювальної системи; зловмисним виведення з ладу механізмів захисту [3].

Основні проблеми, що виникають з безпекою передачі інформації в комп'ютерних мережах, можна поділити на такі :

- перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушена;

- модифікація інформації – вихідне повідомлення змінюється або повністю підміняється іншим і надсилається адресату;

- підміна авторства інформації. Дана проблема може мати серйозні наслідки. Наприклад, хтось може надіслати листа від чужого імені (цей вид обману прийнято називати спуфінгом) або Web-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів [1, с. 79].

Існує багато механізмів безпеки інформації в комп'ютерних мережах, що поділяються на два класи, а саме: спеціальні механізми забезпечення безпеки, які використовуються для реалізації специфічних послуг і різняться для різних послуг, та загальні механізми, які не належать до конкретних послуг безпеки. До спеціальних механізмів забезпечення безпеки належать такі: шифрування; механізми цифрового підписи; механізми управління доступом; механізми забезпечення захисту цілісності даних, які включають криптографічні контрольні функції; механізми автентифікації; механізми заповнення трафіку; механізми керування маршрутизацією [5, с. 35].

Сьогодні в області безпеки інформаційних комп'ютерних систем застосовуються різноманітні технології захисту конфіденційної інформації в цифровій формі за рахунок обмеження доступу до неї на основі систем ідентифікації користувачів. В таких системах доступ користувачів до різних класів інформації визначається ідентифікацією, тобто процесом розпізнавання параметрів, що однозначно визначають особу користувача.

Список використаних джерел:

1. Бакін Д. Проблеми захисту інформації в комп'ютерних мережах. *Актуальні задачі і досягнення у галузі кібербезпеки:* Матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листопада 2016 р. Кропивницький, 2016. С. 79-80.

2. Семенов С.Г. Захист інформації в комп'ютерних системах та мережах : навч. посіб. та ін. Харків : НТУ «ХПІ», 2014. 251 с.

3. Захист інформації в локальних мережах. Вікіпедія: *вільна енциклопедія*. URL: https://uk.wikipedia.org/wiki/Захист_інформації_в_локальних_мережах (дата звернення:16.10.2021).

4. Кошева Н. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів. *Системи обробки інформації*. Вип. 6. Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2013. С. 215-223.

5. Мазниченко Н. Про деякі засоби захисту конфіденційної інформації комп'ютерних систем від несанкціонованого доступу. *Актуальні питання сьогодення:* матеріали Міжнар. наук.-практ. конф. 20 березня 2018 року у м. Вінниця. Обухів: Друкарня «Друкарик» (ФОП Гуляєва В.М.), 2018. Т.9. с. 124.

6. Мушеник І.М. Технології дослідницького навчання і проективної освіти. Освітній простір XXI ст.: виклики та перспективи: збірник наукових праць Всеукр. наук.-практ. інтернет-конф. молодих вчених і здобувачів вищої освіти (22 квітня 2021р., м. Кам'янець-Подільський). Кам'янець-Подільський : Подільський державний аграрно-технічний університет, 2021. С.109-114.