інформації, а також вони оснащені системами реєстрації всіх «зовнішніх» дій. Так як звичайний користувач не має доступу в ці системи, то будь-яке проникнення сприймається як атака або спроба до нелегального отримання даних. Інформація, накопичена системами, застосовується для аналізу дій, скоєних зловмисником, а також для поліпшення і вдосконалення захисних функцій системи. Ці системи мають високу вартість і важкі в експлуатації, тому їх зазвичай використовують великі підприємства або організації, які зайняті в сфері інформаційної безпеки.

ВИСНОВКИ

У сучасному світі більшість компаній зберігає важливу інформацію, дані про співробітників, клієнтів, а також мають online доступ до банківських рахунків в мережах і на комп'ютерах. Кожна компанія прагне убезпечити себе від викрадення зловмисником важливої інформації, який може скористатися їй для корисливих цілей. Підприємство має визначити і знайти для себе максимально ефективний спосіб захисту, оцінити її вартість, взяти до уваги те, що вартість захисту інформації не повинна перевищувати вартість від її втрати.

ЛІТЕРАТУРА

1. Корченко О. Г. Системи захисту інформації [Текст] : Монографія / О.Г. Корченко. – К. : НАУ, 2004. – 264 с.

Павлов І. І.
ДВНЗ «Криворізький національний університет»
Музика І. О.
к. т. н., доцент, ДВНЗ «Криворізький національний університет»

МЕТОДИ ПІДВИЩЕННЯ НАДІЙНОСТІ ТА ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

У даній роботі були розглянуті сучасні методи та засоби захисту інформації в корпоративній мережі, наведені їх переваги та недоліки.

Хід розвитку сучасного суспільства тісно пов'язаний з розвитком інформаційної складової та інформаційної безпеки. Пи-

тання безпеки в інформаційних системах на сучасному етапі розглядаються як пріоритетне в наукових установах, державних структурах і в комерційних фірмах. Інформаційна безпека – одна з головних проблем, з якою стикається сучасне суспільство. Причиною загострення цієї проблеми є широкомасштабне використання автоматизованих засобів накопичення, зберігання, обробки і передачі інформації.

Метою роботи є огляд сучасних засобів захисту інформації та проведення заходів для забезпечення доступності, цілісності та конфіденційності інформації в окремо взятому підприємстві.

Засоби захисту інформації – це сукупність інженерно-технічних, електричних, електронних, оптичних і інших пристроїв які використовуються для вирішення різних завдань із захисту інформації, в тому числі забезпечення безпеки та попередження витоку захищеної інформації. На рисунку 1 наведена класифікація існуючих методів та засобів захисту інформації.

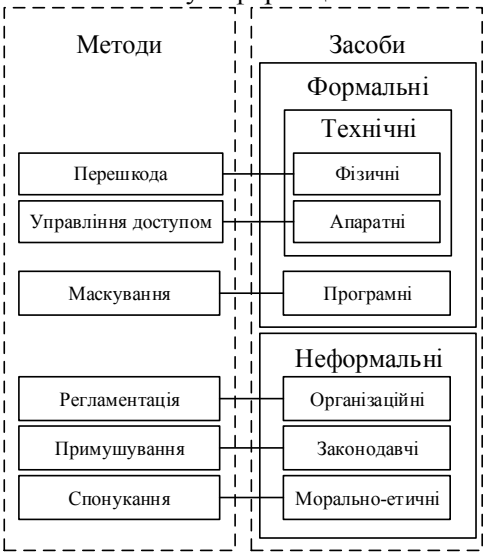

Рис. 1 – Методи та засоби захисту інформації

Загалом данні засоби поділяють на такі групи:

Технічні – це різні за типом пристрою (механічні, електромеханічні, електронні) засоби які апаратно вирішують завдання захи-

сту. Вони перешкоджають доступ до інформації, в тому числі за допомогою її маскування. До апаратних засобів відносяться: генератори шуму, мережеві фільтри, спеціальні регістри для зберігання реквізитів захисту, пристрої вимірювання індивідуальних характеристик людини (голосу, відбитків) з метою його ідентифікації, і безліч інших пристроїв. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високу стійкість до модифікації. Слабкі сторони – недостатня гнучкість, відносно великий обсяг та маса, висока вартість.

Змішані – апаратно-програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

Програмні – ідентифікаційні програми користувачів, програмне забезпечення для контролю доступу, шифрування інформації, видалення тимчасових файлів. Приклади програмних засобів: антивірусна програма (антивірус), firewall, VPN [1]. Переваги програмних засобів: надійність, універсальність, гнучкість. Недоліки: обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, можлива залежність від апаратного та програмного забезпечення комп'ютерів.

Організаційні – складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). Для захисту периметра інформаційної системи створюються: системи охоронної та пожежної сигналізації, системи цифрового відео спостереження, системи контролю та управління доступом (СКУД). Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами та заходами: використанням екранованого кабелю і прокладання проводів і кабелів в екранованих конструкціях, установкою на лініях зв'язку високочастотних фільтрів, побудовою екранованих приміщень («капсул»). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості

модифікації і розвитку. Недоліки: висока залежність від суб'єктивних чинників, в тому числі від загальної організації роботи в конкретному підрозділі.

За ступенем поширення і доступності виділяються програмні засоби. Інші засоби застосовуються в тих випадках, коли потрібно забезпечити додатковий рівень захисту інформації.

ВИСНОВКИ

Слід пам'ятати, що не існує стандартних рішень, однаково добре працюючих у різних умовах. Завжди можливі і необхідні доповнення до розглянутого загального плану захисту корпоративної мережі, що враховують особливі умови тієї чи іншої організації.

ЛІТЕРАТУРА

1. Лысенко Е. И., Барабошин А. С., Черненко С. С. Принципы обеспечения безопасности корпоративной сети // Современные проблемы науки и образования. – 2014. – № 4.; URL: http://www.science-education.ru/ru/article/ view?id=14218 (дата обращения: 01.03.2019).

Кумченко Ю. О.
канд. техн. наук, ст. викладач,
Криворізький національний університет
Шевченко О. В.,
Криворізький національний університет

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Розглянуто основні алгоритми та типи криптографічного захисту. Наведено їх переваги та недоліки. Запропоновано використання симетричного алгоритму блочного шифрування AES та комбінації з ним. Сформовано рекомендації запобігання витоку конфіденційної інформації на підприємствах.

Актуальність теми захисту конфіденційної інформації криптографічними методами обумовлена активним збільшенням інформаційних потоків на підприємствах. Аналіз систем захисту інформації свідчить про очевидний рух у бік комбінованих методів шифрування завдяки їх надійності та стійкості.