УДК 621

# КОНФІДЕНЦІЙНІСТЬ ДАНИХ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ І ЗАСОБИ ЇЇ ЗАБЕЗПЕЧЕННЯ

**Григоренко О.Г., Голуб О.С.**
*Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
*E-mail: olenagri@ukr.net, soupjhoney@gmail.com*

## DATA CONFIDENTIALITY IN INFORMATION COMMUNICATION NETWORKS AND MEANS OF ITS ENSURING

The current issue of data confidentiality in the network is considered and the main means of its provision are analyzed. This contributes to the safe transmission, processing and storage of data in the face of growing potential threats in cyberspace

Розглянуто актуальне питання конфіденційності даних в мережі та проаналізовані основні засоби її забезпечення. Це сприяє безпечній передачі, обробці та зберіганню даних при зростанні потенційних загроз в кіберпросторі

В сьогоднішньому світі, коли загальнодоступна мережа Інтернет використовується для обміну важливими даними, забезпечення конфіденційності даних є актуальною задачею для будь-якої інформаційної системи. У зв'язку з цим, важливим є проаналізувати засоби забезпечення конфіденційності даних в інфокомунікаційних мережах, визначити їх особливості.

Конфіденційність запобігає розкриттю інформації неавторизованим особам, ресурсам або процесам. Тому конфіденційність даних в кіберпросторі потрібно забезпечувати при їх зберіганні, обробці та під час передачі інфокомунікаційною мережею.

Поняття конфіденційної інформації включає дані, захищені від несанкціонованого доступу для гарантування безпеки окремій особі або організації. Конфіденційну інформацію можна розділити на три типи:

- персональна інформація - це особиста інформація, а саме дані, за допомогою яких можна визначити особистість людини. Це такі дані як паспортні дані, медичні записи, номера банківських карток, фінансова інформація;

- ділова інформація - це інформація, яка у разі оприлюднення може створити проблеми для організації. До таких даних відносяться торговельні секрети, плани придбання, фінансові дані, інформація споживача;

- секретна інформація - це інформація, що належить державним органам, засекречена через високий рівень конфіденційності.

Компанії, організації зазвичай обмежують доступ, щоб гарантувати, що тільки уповноважені особи можуть використовувати дані або інші мережні ресурси. Наприклад, програміст не повинен мати доступ до особистої

інформації всіх співробітників. Також в компаніях потрібно навчати співробітників кращим методам захисту конфіденційної інформації, щоб захистити їх та організацію від атак. Основні засоби, які використовуються для забезпечення конфіденційності, включають шифрування даних, аутентифікацію і контроль доступу, політики та процедури щодо кібербезпеки. безпечні протоколи (SSH, SSL/TLS, IPsec) [4], використання VPN (Virtual Private Network) (рис.1).

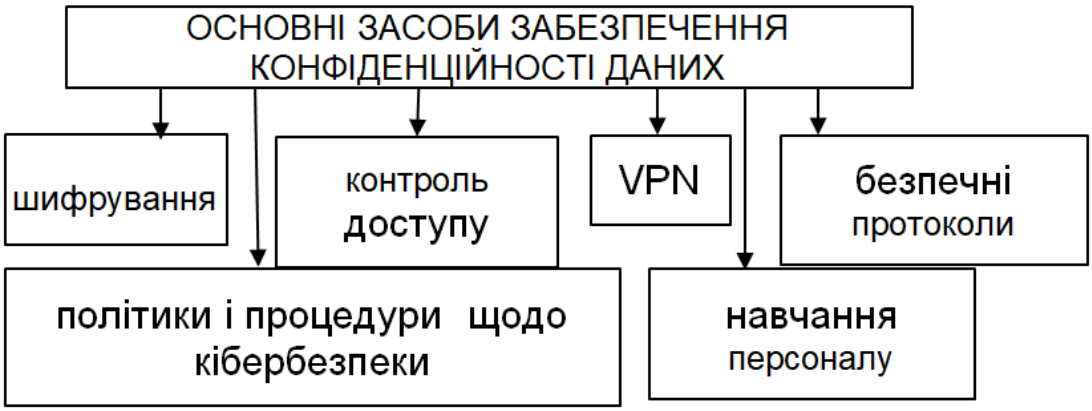


Рис.1 Основні засоби забезпечення конфіденційності

Шифрування перетворює дані таким чином, щоб неавторизована третя сторона не змогла їх прочитати [1]. Для шифрування використовуються математичні алгоритми, надійність яких напряму залежить від надійності ключа. Чим складніший ключ, тим більш безпечний алгоритм. Керування ключами є важливою частиною цього процесу. Всі сучасні криптографічні алгоритми містять обов'язкові процедури керування ключами. На практиці більшість атак на криптографічні системи спрямовані на систему керування ключами, а не на сам криптографічний алгоритм.

Контроль доступу визначає ряд схем захисту, які запобігають несанкціонованому доступу до комп'ютера, мережі, бази даних або інших ресурсів даних. Концепція AAA (Authentication, Authorization, Accounting) включає в себе три служби безпеки: аутентифікація, авторизація та облік. Ці служби забезпечують основну структуру контролю доступу.

Аутентифікація перевіряє особу користувача для запобігання несанкціонованому доступу [2]. Користувачі підтверджують свою особистість за ім'ям користувача або ідентифікатором. Аутентифікація вимагає, щоб користувач надав інформацію, яку він знає (наприклад, пароль), або/та підтвердив наявність чогось (наприклад, картка), або/та надав біометричну інформацію (наприклад, відбитки пальців). Найбільш популярною формою аутентифікації є використання паролів. Поєднання декількох типів аутентифікації відоме як багатофакторна аутентифікація, яка є більш безпечною і надійною завдяки неможливості для кіберзлочинців за короткий час зламати всі види захисту.

Авторизація визначає до яких ресурсів можуть отримати доступ користувачі, а також операції, які вони можуть виконувати. Деякі системи

реалізують це за допомогою списку керування доступом або ACL (Access Control List). ACL визначає, чи має користувач певні привілеї доступу після проходження аутентифікації. Авторизація також може контролювати, коли, тобто в який час, користувач має доступ до певного ресурсу.

VPN - це приватна мережа, яка використовує загальнодоступну мережу, зазвичай Інтернет, для створення безпечного каналу зв'язку [5]. VPN з'єднує за допомогою зашифрованого тунелю дві кінцеві точки, такі як два віддалених офіси, через Інтернет, щоб створити з'єднання.

Мережі VPN використовують IPsec - набір протоколів, розроблених для реалізації безпечних мережних сервісів. Сервіси IPsec забезпечують аутентифікацію, цілісність, контроль доступу та конфіденційність. За допомогою IPsec віддалені вузли можуть обмінюватися зашифрованою і перевіреною інформацією.

Для побудови політики інформаційної безпеки рекомендується окремо розглядати такі напрями захисту інформаційної системи [3] як захист об'єктів інформаційної системи; захист процесів, процедур і програм обробки інформації; захист каналів зв'язку різного виду; придушення побічних електромагнітних випромінювань і наведень; управління системою захисту.

Підсумовуючи, зазначимо, що забезпечення конфіденційності даних є на сьогодні надзвичайно актуальним питанням на тлі зростання потенційних загроз у кіберпросторі. Для цього застосовується комплекс технічних, організаційних, правових заходів. Аналіз особливостей засобів забезпечення конфіденційності показав, що основними є шифрування, використання безпечних протоколів та VPN. Особливу увагу організації приділяють контролю доступу та розробці політик і процедур щодо інформаційної безпеки. Також завжди треба враховувати людський фактор і регулярно проводити навчання з кібербезпеки для персоналу компанії і навчати новим технологіям захисту.

**Література**


1. Шифрування: типи і алгоритми/ [Електронний ресурс] – Режим доступу: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms
2. Використання аутентифікації в мережі як способу виконання безпечних хмарних обчислень/ Григоренко О.Г., Полікарпова Ю.Г. // Збірник "Перспективи телекомунікацій" ПТ-2021. – К.: КПІ ім. Ігоря Сікорського, 2021. – С.44-46. ISSN (print) 2663-502X ISSN (online) 2664-3057 http://journals.uran.ua/ за посиланнями: http://conferenc.its.kpi.ua/proc/issue/archive, http://journals.uran.ua/ (ISSNonline 2664-305).
3. Системи забезпечення інформаційної безпеки/ [Електронний ресурс] / – Режим доступу: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.
4. WHAT IS SSL, TLS & HTTPS/ [Електронний ресурс] – Режим доступу:https://www.digicert.com/what-is-ssl-tls-and-https
5. Bacek / Принципы организации VPN // [Електронний ресурс] – Режим доступу: http://ciscotips.ru/vpn