УДК 674.047
О. Огірко
(Українська академія друкарства)

БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ

Фахівці в області захисту інформації пропонують розділяти систему безпеки на дві частини: внутрішню і зовнішню . У внутрішній частині здійснюється, в основному, контроль доступу шляхом ідентифікації і аутентифікації користувачів при допуску в мережу і при доступі в базу даних. Крім цього шифруються і ідентифікуються дані під час їхньої передачі і зберігання. Безпека в зовнішній частині мережі в основному досягається криптографічними засобами. По результатах проведених досліджень було визначено основні вразливі місця в мережевих системах . Ними є апаратура, інформаційний сервер, паролі і середовище передачі даних. Один із підходів захисту інформації за допомогою шифрування є використання спеціального програмного забезпечення. Мета дисципліни – закласти фундамент, навчити студентів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

JSafe функціонує на рівень нижче за Java-інтерфейс прикладного програмування Crypto API. До складу JSafe входять алгоритми шифрування із закритим ключем RC2, RC4 і RC5, алгоритми формування сертифікатів цілісності повідомлень MD-5 і SHA-1, а також алгоритми хешування для формування цифрових підписів. JDK (Java Development Kit) надає обмежений набір таких засобів, включаючи шифрування на основі стандартних алгоритмів, проте він не підтримує методів шифрування з відкритим і закритим ключем. Встановлено, що ці методи складають основу сучасних засобів захищеної передачі даних по Internet. Розглядаючи протоколи, що дозволяють згортати і приховувати від сторонніх очей протоколи високого рівня, шифруючи, а також підтверджуючи їх походження і цілісність, найбільше поширення набув SSL. Встановлено, що найпопулярнішими захищеними серверами є Apache і Stronghold. Кожен з засобів має свої переваги і недоліки. Тому необхідно аналізувати особливості програмного і апаратного забезпечення, що використовується у мережі. Існуюча система криптографії використовує два типи криптографічних алгоритмів: класичні алгоритми, основані на використанні закритих, секретних ключів і алгоритми з відкритим ключем, в яких використовують один відкритий і один закритий ключ. Для класичної криптографії характерне використання однієї секретної одиниці – ключа, який дозволяє відправнику зашифрувати повідомлення, а одержувачу розшифрувати його. Секретні ключі є основою криптографічних перетворень, для яких, слідуючи правилу Керкхофа, стійкість хорошої шифрувальної системи визначається лише секретністю ключа. Алгоритм DES достатньо надійний. Він володіє великою гнучкістю при реалізації різних додатків обробки даних, оскільки кожний блок даних шифрується незалежно від інших. Алгоритм може реалізовуватися як програмним, так і апаратним засобами. Встановлено, що даний алгоритм може реалізовуватися як апаратним, так і програмним засобами, задовольняє всім криптографічним вимогам, що склалися в світовій практиці і дозволяє здійснювати криптографічний захист будь-якої інформації, незалежно від ступеня її секретності. Серед алгоритмів шифрування є алгоритм RC6 фірми RSA Data Security. Алгоритм RC6 є еволюційним удосконаленням відомого алгоритму RC5.