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.

У сучасному світі найбільш надійними методами захисту інформації є криптографічні алгоритми і побудовані на їх основі протоколи захищеного обміну інформації та цифрові підписи. Взагалі, криптографія – це наука про математичні методи захисту, цілісності та автентичності інформації. До основних алгоритмів криптографічного захисту можна віднести: DES, AES, Camellia, Twofish, Blowfish, IDEA, RC4, RSA, Elgamal тощо. Розглянемо основні типи криптографічного захисту, а саме: хешування, асиметричне та симетричне шифрування, електронний цифровий підпис (ЕЦП).

Хешування – це метод криптографічного захисту, що представляє собою контрольне перетворення інформації: з даних необмеженого розміру шляхом виконання криптографічних перетворень обчислюється хеш-значення фіксованої довжини, однозначно відповідне вихідними даними [1].

Симетричне шифрування (DES, AES, Camellia, Twofish, Blowfish, IDEA, RC4) – схема шифрування, в якій ключ шифрування та ключ розшифровки однакові або один легко обчислюється з іншого та навпаки. Симетричні алгоритми шифрування можна розділити на потокові та блочні алгоритми шифрування. Потокові алгоритми шифрування послідовно обробляють текст повідомлення. Блочні алгоритми працюють з блоками фіксованого розміру. Як правило, довжина блоку дорівнює 64 бітам. Перевагою симетричного шифрування перед асиметричним є більша швидкість обчислень. Недоліком є необхідність часто змінювати ключі та важливість їх передачі безпечними каналами.

Асиметричне шифрування (RSA, Elgamal) характеризується застосуванням двох типів ключів: відкритим – для зашифровування інформації та секретного – для її розшифрування. Використовуючи такий метод не потрібно передавати ключ надійним каналом, ключ розшифровки має лише одна сторона. До недоліків можна віднести складність внесення зміни в алгоритм та необхідність у більших обчислювальних ресурсах ніж у симетричному методі.

ЕЦП дозволяє підтвердити авторство електронних даних та їх цілісність. Електронний підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Основною перевагою цього алгоритму є складність підробки підпису.

Для вирішення задачі захисту конфіденційної інформації найбільш доцільно використовувати алгоритм AES та комбінації з

ним. Це симетричний алгоритм блочного шифрування. Перевагою даного алгоритму є висока швидкодія на різних платформах. Вважається, що на даний момент не існує реальної можливості злому даного алгоритму, так як він використовує 128, 192 та 256 бітні ключі [2, 3]. Деяким недоліком можна вважати те, що режим зворотної розшифровки відрізняється від режиму зашифровки слідування функції, і самі ці функції відрізняються своїми параметрами від застосовуваних у режимі шифрування.

ВИСНОВКИ

Питання інформаційної безпеки стає наріжним каменем у діяльності організації, адже найменша втрата конфіденційної інформації може завдати значних витрат на відновлення роботи установи. Захист інформації повинен здійснюватися комплексно, відразу за декількома напрямками. Дані повинні зберігатися у цілісній, доступній та захищеній формі. Чим більше методів буде задіяно, тим менше ймовірність виникнення загроз і витоку інформації, тим стійкіше положення підприємства на ринку.

ЛІТЕРАТУРА

1. Классификация криптографических алгоритмов [Електронний ресурс] // Your Private Network. – 2009. – Режим доступу до ресурсу: http://ypn.ru/228/classification-of-cryptographic-algorithms/.
2. Как устроен AES [Електронний ресурс] // Habr. – 2011. – Режим доступу до ресурсу: https://habr.com/ru/post/112733/.
3. Шифрование AES и RSA [Електронний ресурс] – Режим доступу до ресурсу: https://www.boxcryptor.com/ru/encryption/.

Цюпко В. В.,
Криворізький національний університет
Музика І. О.
канд. техн. наук, доц., Криворізький національний університет

ПРИНЦИПИ ПІДВИЩЕННЯ НАДІЙНОСТІ WEB-САЙТІВ НА БАЗІ СИСТЕМ УПРАВЛІННЯ КОНТЕНТОМ

Проведено аналіз надійності та безпеки систем управління контентом. Описано архітектури платформ та їх вразливості з точки безпеки та надійності, а також наведено принципи щодо захисту системи управління.