39. Використання засобів захисту інформаційного обміну в комп'ютерних мережах промислового призначення

Андрій Шинкаренко
Національний університет харчових технологій

Вступ. Завдання захисту інформації від несанкціонованого доступу вирішувалося в усі часи протягом історії людства. Уже в стародавньому світі виділилось два основних напрямки вирішення цього завдання, існуючі і по сьогоднішній день: криптографія і стеганографія. Метою криптографії є приховування вмісту повідомлень за рахунок їх шифрування. На відміну від цього, при стеганографії ховається сам факт існування таємного повідомлення.

У доповіді проведено огляд сучасних засобів захисту інформації, які можуть бути використані в системах автоматизованого керування промисловими об'єктами. Виділено такі засоби: фізичні, законодавчі, управління доступом, криптографічне закриття. Обмежуючи дослідження саме криптографічними засобами, задача полягає в розробці рекомендацій щодо вибору конкретних протоколів інформаційного обміну та програмного забезпечення під час проектування та розгортання інформаційних систем на заданому об'єкті.

Матеріали і методи. В комп'ютерних системах найефективнішими є криптографічні способи захисту інформації, що характеризуються найкращим рівнем захисту. Для цього використовуються програми криптографічного перетворення (шифрування) та програми захисту юридичної значимості документів (цифровий підпис). Шифрування забезпечує засекречування і використовується в ряді інших сервісних служб. Шифрування може бути симетричним і асиметричним. Перше базується на використанні одного і того ж секретного ключа для шифрування і дешифрування. Друге характеризується тим, що для шифрування використовується один ключ, а для дешифрування – інший, секретний.

Також використовують комп'ютерну стеганографію — це напрям класичної стеганографії, що базується на особливостях форматів, які використовуються для представлення інформації. Приклади: стеганографічна файлова система StegFS для Linux, приховування даних у невикористовуваних областях форматів файлів, підміна символів у назвах файлів, текстова стеганографія і т. д. Останнім часом набули популярності методи, коли прихована інформація передається через комп'ютерні

мережі з використанням особливостей роботи протоколів передачі даних. Такі методи одержали назву «мережева стеганографія».

Результати. Розроблено програму, написану на мові С++, яка дозволить приховати при передаванні блок текстової інформації у графічних файлах нерухомих зображень. В останній 8-й біт / піксель вбудовується приховане повідомлення. На вході ми маємо текст і зображення, на виході — зображення, в якому знаходиться повідомлення.

Висновки. Користувачами програми можуть бути підприємства, які потребують захисту електронних документів, що передаються через незахищені мережі загального користування.

Науковий керівник: д. т. н., проф. Савченко Ю. Г.

Література.

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Конахович Г. Ф., Пузыренко А. Ю. — К. : МК-Пресс, 2006.

2. Грибунин В. Г. Цифровая стеганография / Грибунин В. Г., Оков И. Н., Туринцев И. В. — М. : Солон-Пресс, 2002.

3. Вольшенбах М. Криптография на С и С++. — М. : Триумф, 2004. — 464 с.

4. Панасенко С. П. Алгоритмы шифрования. — СПб. : БХВ-Петербург, 2009. — 576 с.