УДК 004.031
Д.М. Холод, Г.В. Шимчук
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ПРОБЛЕМИ ЗАХИСТУ КОМП'ЮТЕРНИХ СИСТЕМ

D. Kholod, G. Shymchuk

FEATURES MODERN CS AS OBJECT OF PROTECTION

Пропорційно розвитку комп'ютерних технологій також зростає й рівень злочинності в комп'ютерному середовищі. У зв'язку з цим, використання локальних мереж для передачі та зберігання інформації, вимагає побудови ефективної системи захисту.

Тому створення системи захисту інформації, у даний час, стає невід'ємною частиною політики безпеки будь-якої організації. Для правильного функціонування системи захисту необхідні знання можливих дій порушника, а отже, можливих загроз КС.

Все більше актуальною стає побудова комплексної системи захисту, що використовує всі можливі методи та способи захисту, в тому числі й ті, що входять до складу операційних систем. Вбудовані засоби дозволяють зменшити витрати на побудову системи захисту. Мова йде про так звані специфічні протоколи захисту, тобто протоколи та алгоритми, які забезпечують конфіденційність та цілісність інформації, яка передається.

Таким чином, аналіз таких протоколів є передумовою обґрунтованого відбору протоколів для побудови на їх основі комплексної системи захисту, що є актуальною задачею в загальній проблемі забезпечення інформаційної безпеки сучасних об'єктів інформаційної діяльності.

Метою роботи є підвищення рівня безпеки мережевої взаємодії шляхом створення комплексної системи захисту на основі протоколів різних рівнів моделі OSI.

Як практичний метод досягнення цілей будемо проводити налаштування та конфігурування безпечної мережевої взаємодії на основі різних протоколів захисту.

Для досягнення поставленої в роботі мети потрібно вирішити наступні задачі:

- розглянути модель порушника та основні класи загроз безпеки в КС;
- провести аналіз протоколів захисту інформації в автоматизованих системах різних рівнів моделі OSI;
- практично виконати налаштування протоколів захисту інформації.

Новизна отриманих результатів полягає у залученні до створення системи захисту інформації протоколів різних рівнів моделі взаємодії OSI. В єдиний комплекс зведені протоколи канального, мережевого та транспортного рівнів, що дозволяє ефективно об'єднати їх функціональні можливості і досягти високого рівня захисту.

Розглянемо основні проблеми захисту КС та проведемо теоретичний та практичний аналіз вбудованих засобів захисту інформації.

Розглянемо аналітичний огляд сучасних автоматизованих систем обробки інформації. Який показує, що уразливими є буквально всі основні структурно-функціональні елементи розподілених КС: робочі станції, сервери (Host-машини), міжмережеві мости (шлюзи, центри комутації), канали зв'язку.

Виходячи з основних нормативних документів із захисту інформації розглянемо чотири основних класи загроз: порушення конфіденційності, цілісності, доступності, спостережності. Інформаційна безпека КС забезпечується у випадку, якщо

для будь-якого інформаційного ресурсу в системі підтримується певний рівень конфіденційності, цілісності, доступності та спостережності.

Розглянемо модель загроз, згідно з якою всі потенційні загрози за природою їх виникнення розділяються на два класи: природні (об'єктивні) і штучні (суб'єктивні). А джерела загроз по відношенню до КС можуть бути зовнішніми або внутрішніми.

Виходячи з можливих загроз та суб'єктів їх вчинення, розглянуто модель порушника, в якій відбиваються його практичні і теоретичні можливості – важлива складова для побудови надійної системи захисту.

З розглянутого широко спектру загроз інформаційної безпеки випливає, що тільки комплексний підхід до захисту інформації може забезпечити сучасні вимоги безпеки в КС. Він має на увазі комплексний розвиток усіх методів і засобів захисту.

Елементами комплексної системи захисту КМ є засоби, механізми яких входять до складу мережевих операційних систем. Їх використання є доцільним, оскільки не потребує затрат коштів та робочої сили. Виходячи зі специфіки мережевої взаємодії, на кожному рівні моделі взаємодії відкритих систем, можна застосовувати свої відповідні протоколи.

Для безпечної мережевої взаємодії на основі вбудованих засобів захисту інформації необхідним є практичний аналіз протоколів захисту інформації, що включає налаштування серверів, клієнтів, служб, протоколів та з'єднань.

В роботі практично налаштовано та продемонстровано правильність функціонування таких протоколів захисту: IPSec, SSL, PPTP та L2TP. Всі ці протоколи забезпечуються надійний захист від загроз конфіденційності та цілісності.

Результатами роботи є розглянуті особливості сучасних загроз і уразливість інформації в КМ та забезпечення безпеки. Проведений аналіз протоколів захисту інформації різних рівнів моделі OSI. Практично налаштовані протоколи захисту інформації в КС.

Література

1. Алферов А.П. Основы криптографии. Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М. Гелиос АРВ, 2002. – 480 с. – ISBN 5-85438-025-0.

2. Антонюк А. О. Основи захисту інформації в автоматизованих системах / А. О. Антонюк. Національний ун-т «Києво-Могилянська академія». – К.: КМ Академія, 2003. – Бібліогр.: с. 242-243. – ISBN 966-518-211-0.

3. Бабак В.П. Теоретичні основи захисту інформації. Підручник / В.П. Бабак. – НАУ, 2008. – 752 с. – ISBN 978-966-598-4047

4. Бабаш А.В. История криптографии / А.В. Бабаш, Г. П. Шанкин. – Часть I. – М.: Гелиос АРВ, 2002. – 240 с. – ISBN 5-85438-043-9.

5. Бабаш А. В. Криптография / А.В. Бабаш, Г. П. Шанкин. – М.: СОЛОН–Р, 2002. – 511с. – ISBN 5-93455-135-3.

6. Бевз О.М. Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню / О.М. Бевз, Р.Н. Квєтний. – Вінниця: ВНТУ, 2010. – 96 с. – ISBN 978-966-641-340-9.