УДК 004.56
Квач П. – ст. гр. СІмс-61
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОГО ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Науковий керівник: проф., д. т. н. Грицик В. В.

Kvach P.
Ternopil Ivan Pul'uj national technical university

COMPLEX PROTECT OF NETWORKS METHODS AND MEANS ARE RESEARCHED

Supervisor: V. Hrytsyk

Ключові слова: задача захисту, порушника безпеки, розмежування доступу
Keywords: problem protection offender security credentials of access control.

Задача захисту комп'ютерних мереж і систем від несанкціонованого доступу в сучасних умовах набула особливу гостроту. Стрімкий розвиток комунікаційних технологій дозволяє будувати мережі розподіленої архітектури, що об'єднують велику кількість сегментів, розташованих на значній відстані один від одного. Усе це викликає збільшення числа вузлів мереж і кількості різних ліній зв'язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до мережі і доступу до важливої інформації. З позиції порушника безпеки і цілісності види порушень відповідно поділяються на умисні і ненавмисні. До умисним відноситься розкрадання (знищення) носіїв інформації, підслуховування, несанкціоноване копіювання інформації за допомогою терміналів та ін.

Об'єктом дослідження є спосіб автоматичного класифікації формалізованих документів в системі електронного документообігу.

Предметом дослідження є властивості способу автоматичної класифікації формалізованих документів в системі електронного документообігу, що забезпечують безпечну обробку інформації

В методах розмежування доступу, побудованих за принципом надання прав неформально право доступу може бути описане як "білет", у тому сенсі, що володіння "білетом " дозволяє доступ до деякого об'єкту, що описаний в "білеті". Основними типами методу, побудованих на наданні прав, є методи дискретного та мандатного доступу, що використовуються в більшості реальних систем, створених на сьогоднішній день.

Метод мандатного розмежування доступу забезпечує інформаційну безпеку за допомогою присвоєння всім сутностей системи рівнів конфіденційності (доступу). Дані рівні або мітки визначають всі можливі доступи між ними. Проте з цього випливає, що мандатне управління доступом не розрізняє сутностей одного рівня доступу, і на їх взаємодії обмеження не поширюються. Тому мандатна модель, як правило, застосовується обов'язково спільно з дискреционной, яка використовується для контролю за взаємодіями між сутностями одного рівня і установки додаткових обмежень, що підсилюють мандатну модель. В ході дослідження аналізується різні методи розмежування доступу з метою реалізації захищеності комп'ютерних мереж у мандатному методі, робота над якою здійснюється у дипломній роботі.