

ЗАХИСТ ІНФОРМАЦІЇ ПРИ ВПРОВАДЖЕННІ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ІНФОРМАЦІЙНО- ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Актуальність роботи пов'язана з потребою широкого використання електронних документів, зберіганням великих обсягів інформації та захистом систем електронного документообігу.

Необхідність захисту інформації виникла з моменту створення систем документообігу, а коли почали з'являтися електронні системи, то це питання було поставлено дуже гостро, оскільки неможливо впроваджувати і використовувати систему, яка не має захисту належного рівня.

Тому доцільним є впровадження систем електронного документообігу (СЕДО) різного рівня складності та архітектури, що дозволяють прискорити процес обробки даних та підвищити надійність зберігання та обробки документів.

Внаслідок збільшення потоків інформації у всіх сферах людського життя, введення СЕДО є необхідною і обов'язковою умовою для успішного розвитку інформаційних систем. Сьогодні такі системи мають свою аналітичну базу, готові рішення для розв'язання поставлених задач, моделі бізнес-проектів та виконують надскладні операції, які людина не може опрацювати без використання обчислювальної техніки, а також дозволяють автоматизувати процес обробки без втручання людини або мінімізувати її втручання в роботу системи. Це дасть можливість зменшити кількість помилок кваліфікованим персоналом, оскільки системам присутні підказки та обмеження, що допомагають працівникам діяти тим чи іншим чином у різних ситуаціях.

Над вдосконалення СЕДО працюють спеціалісти різних сфер, які виявляють недоліки та знаходять нові рішення щодо їх функціонування. Але важливою проблемою залишається захист інформації. Через відсутність комплексу рішень, який слід використовувати при захисті систем неможливе широке використання СЕДО, оскільки вони не можуть бути захищені необхідним рівнем захисту від порушників цілісності системи. Зараз СЕДО дозволяють здійснювати навіть віддалене керування системою, а це підвищує й вимоги до безпеки і вже не можна обмежитись лише засобами технічного захисту інформації.

Таким чином, в роботі розглянуто засоби захисту, які повинні включати в собі наступні елементи: консоль адміністратора, міжмережевий екран, систему виявлення вразливостей, систему виявлення атак, засоби криптографічної обробки інформації захищених віртуальних мереж, засоби розмежування повноважень користувачів.

Науковий керівник – к.т.н., с.н.с., доц., Ю.І. Хлапонін