Комбінована система інформаційного захисту на муніципальних підприємствах: інструментарій та особливості застосування

Авершин С.В., *здобувач*, ***Новиков А.О.***, *здобувач*, ***Лукашов О.О.***, *здобувач*, *Харківський національний університет міського господарства*

Розвиток крупних мегаполісів пов'язаний із потоками інформації, на основі яких приймаються управлінські рішення. У цьому контексті слід вказати на необхідності отримання повної й достовірної інформації на муніципальних підприємствах, яка повинна мати високий рівень захисту.

Для забезпечення інформаційного захисту застосовуються відповідні системи, зокрема: спискові системи, що орієнтуються на ключ, що орієнтуються на керівника, комбіновані системи.

У результаті дослідження визначена необхідність застосування на муніципальних підприємствах комбіновані системи, які узагальнюють у собі ознаки та функції попередніх трьох систем і дозволяють приймати обґрунтовані управлінські рішення щодо інформаційного захисту на кожному етапі функціонування цих підприємств.

У рамках комбінованих систем інформаційного захисту запропоновано використовувати відповідний інструментарій, який складається із:

- програми користувача, що визначається системою дій і заходів, в якій подані загальні положення й особливості захисту формування й використання інформації відносно користувачів. Крім того, визначено поведінку користувачів, можливі відхилення й напрями удосконалення систем захисту;
- розпізнавальні механізми, які спрямовано на перевірку особині, яка використовує інформацію. Крім того, користувач і система зв'язку підприємства об'єднані в єдиний комплекс, який входити до загальної інформаційної системи підприємства. Отже, всі суб'єкти інформаційної системи взаємозалежні й реалізуються через розробку й впровадження паролів та інформаційних фільтрів. Важливим завданням системи є забезпечення захисту паролів та їх ідентифікація із користувачем. Слід зазначити, що при виборі й використанні паролю виникають деякі ускладнення. Зокрема, при виборі паролю користувачі, у більшості випадків, формують його найлегший варіант, що знижує рівень безпеки й доступність іншим користувачам. При розробці ускладнених паролів виникає можливість втрати паролю користувачем, що призводить до технологічних й технічних проблем. Тому, одним із важливих напрямів удосконалення розпізнавальних механізмів у системі інформаційного захисту є розробка й забезпечення генератора визначених випадкових паролів. Іншою проблемою паролізації інформаційної системи є можливість її перехопленню. У таких випадках запропоновано застосовувати сучасні розпізнавальні механізми: використання сенсорних систем, запровадження відбитків пальців для ідентифікації користувачів, електронних підписів та ін. У якості розпізнавального механізму використовують електронні ключі, пластикові карти, які ідентифіковано під відповідного користувача. Проте, в

поданих механізмах виникають ускладнення, пов'язані зі зміною терміналу зловмисником або втратою цих інструментів захисту користувачем. Можуть застосовуватись технологічні втручання й отримання паролів через використання відповідного програмного забезпечення. У багатоканальних і складних інформаційних системах застосовуються шифрування інформації із використанням ключа, який, наприклад, може складатись із 1000 двійкових цифр, що прочитуються із магнітної пластикової карти. Цей розпізнавальний інструмент дозволяє збільшити рівень захисту інформації на основі посилення ідентифікаційних процедур;

- віртуальних бібліотек, в яких зосереджено інформацію про всіх користувачів інформації підприємства. Крім того, в них зосереджено ретроспективу всіх входів і виходів у інформаційну систему, напрями формування й використання інформації. Віртуальні бібліотеки дозволяють провести аналіз й сформувати відповідні дії щодо захисту інформації;
- списків контролю, які створюють базис для забезпечення управління процесами формування й використання інформації на підприємстві, застосування кодування, шифрування й паролей для кожного із внутрішніх і зовнішніх користувачів, які знаходяться у списку контролю, визначаються обмеження використання інформації.

У результаті дослідження визначено, що комбінована система інформаційного захисту для муніципальних підприємств може бути побудована на основі ознак, якостей і особливостей систем електронного, персонального, психологічного, віртуального захисту, орієнтованих систем. Комбіновані системи інформаційного захисту можуть постійно трансформуватись залежно від змін зовнішнього й внутрішнього середовища муніципальних підприємств.