РОЛЬ СТАТИСТИЧНИХ ДОСЛІДЖЕНЬ ПОВЕДІНКИ КОРИСТУВАЧІВ У ВИЯВЛЕННІ ПОРУШНИКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Зайцев С. В., Заболотний В. І.
Харківський національний університет радіоелектроніки, Харків, Україна

Виявлення порушників, активна та превентивна протидія їм - важливий аспект безпеки функціонування комп'ютерних систем та мереж. Виявлення можна проводити як із використанням раніше отриманих статистичних даних, так і підготовленої моделі правил поведінки передбачуваних користувачів. Опис цих методів є у [1].

1. Виявлення на базі статистичних відхилень передбачає збирання даних, що характеризують поведінку легальних користувачів, протягом певного часу. Аналіз цих даних із застосуванням статистичних методів, дозволяє з високим ступенем достовірності визначити потенційну небезпеку конкретного певного користувача. Найбільш поширеними методами є: використання порогових значень частоти незвичайних дій у системі, використання профілю поведінки (створюється профіль активності користувача, виявляються відхилення в поведінці).

2. Виявлення на базі правил рішення про те, що даний тип поведінки є поведінкою порушника. Найбільш поширеними є виявлення аномалій та ідентифікація вторгнення.

Метою доповіді є виявлення доцільності статистичних досліджень поведінки користувачів для виявлення порушника, у тому числі і тих, що використовують закладені в ЕОМ пристрої перехоплення інформації. Він створює передумови для стандартизації та уніфікації статистичних спостережень та механізмів забезпечення конфіденційності даних [2].

Метод на основі статистики вимагає мінімальних затрат для користувача, проте його ефективність може достатньою.

Метод на основі бази правил передбачає детальний аналіз системи і мережі, він дозволяє організувати захист від порушників конкретного типу і ефективно захищати від нестандартних атак.

Список літератури

1. Семенов С. Г. Захист інформації в комп'ютерних системах та мережах. [Електронний ресурс] Режим доступу: аhttp://www.dgma.donetsk.ua/docs/kafedry/avp/metod/_БКМ_Пос_бник.pdf (дата звернення 07.04.2022 р.).

2. Осауленко О. Г. Офіційна статистика в системі національної інформаційної безпеки: монографія. Київ: ТОВ «Август Трейд», 2017. 367 с.