**УДК 004.383.8**
**Б.В. Скоропад**
Тернопільський національний економічний університет, Україна

# ПІДВИЩЕННЯ НАДІЙНОСТІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**Skoropad**
# IMPROVING THE RELIABILITY OF THE INFORMATION SECURITY SYSTEM

На сьогоднішній день для захисту комп'ютерних систем від атак, в основному, використовується спеціалізоване програмне забезпечення (ПЗ) [1–2]. Проте, таке ПЗ є вразливим до самих вторгнень, через те, що можуть перехоплюватися системні функції операційної системи, що дає можливість активно протидіяти виявленню та видаленню їх програмними засобами. При цьому вторгнення здатні блокувати запуск спеціалізованого ПЗ, відслідковувати його дії та відновлювати видалені шкідливі процеси, змінювати налаштування в системному реєстрі тощо.

Тому пропонується захищати комп'ютерні системи захисту від атак апаратними засобами. Апаратне рішення працює не в середовищі зараженої операційної системи, тому всі дії комп'ютерних атак будуть безрезультатними, а вторгнення будуть швидко знешкодженими [3, 4].

При цьому, до апаратних засобів ставляться наступні вимоги:

1. Висока надійність системи захисту від комп'ютерних атак в цілому. Для цього необхідно виділити окремий комп'ютер для постійного аналізу мережевого трафіку.

2. Висока стійкість до атак інтелектуальної системи захисту. Для цього аналіз атак, навчання засобів виявлення атак і підготовка до модифікації апаратних засобів поточного виявлення та знешкодження комп'ютерних атак повинна здійснюватися на згаданому виділеному комп'ютері, який не підключено до мережі;

3. Висока стійкість до комп'ютерних атак підсистеми поточного виявлення та знешкодження загрози. Ця система повинна бути повністю апаратною;

4. Висока гнучкість підсистеми поточного виявлення та знешкодження загрози. Для цього слід забезпечити можливість динамічного періодичного оновлення засобів виявлення атак згідно результатів аналізу вторгнень. Для цього необхідно забезпечити запис нових засобів лише згаданим виділеним комп'ютером (а не комп'ютером, де функціонує апаратне забезпечення підсистеми поточного виявлення загроз).

Поділ структури системи захисту на апаратну та програмну частину та реалізація нейромережевих детекторів на ПЛІС дозволить підвищити безпеку самої системи захисту.

**Література**

1. Wee Y.Y., Cheah W. P., Tan S. C. Causal Discovery and Reasoning for Intrusion Detection using Bayesian Network / International Journal of Machine Learning and Computing. – 2011. – Vol. 1, № 2. – P. 185–192.

2. Komar M., Sachenko A., Bezobrazov S., Golovko V. Intelligent Cyber Defense System Using Artificial Neural Network and Immune System Techniques // Communications in Computer and Information Science, Springer, Cham. – 2017. – Vol. 783. – P. 36-55.

3. Komar M. Improving of the Security of Intrusion Detection System / Myroslav Komar, Volodymyr Kochan, Anatoly Sachenko, Victor Ababii // Proceedings of the 13th International Conference on Development and Application Systems (DAS-2016). – Suceava, Romania, May 19-21, 2016. – P. 315–319.

4. Комар М.П. Підвищення стійкості комп'ютерних систем до кібератак // Науковий вісник Чернівецького національного університету: Комп'ютерні системи та компоненти. – Чернівці. – 2016. – Т. 7, вип. 1. – С. 6-12.