АНАЛІЗ СИСТЕМ І ЗАСОБІВ ЗАХИСТУ ПІДПРИЄМСТВА

Ляшенко О. С., Мусаб Нур Еддін Аллахам, Кісь О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Безпека підприємства є найважливішим чинником, що впливає на функціонування підприємства. Під терміном «безпека підприємства» мається на увазі комплекс заходів, що оберігають підприємства і його життєво важливих функцій (інтересів) від загроз зовнішнього і внутрішнього характеру і від випадкового або навмисного втручання в його функціонування [1]. Створення системи безпеки, як правило, має починатися з розробки концепції безпеки – узагальнення системи поглядів на проблему безпеки даного об'єкту на різних етапах і рівнях його функціонування, визначення основних принципів побудови системи, розробки напрямків і етапів реалізації заходів безпеки.

При розгляді загроз інформаційній безпеці об'єкту особливу увагу необхідно приділити класифікації об'єктів які підлягають захисту інформаційної безпеки підприємства. Таким чином, можна зробити висновок про те, що дія загроз інформаційній безпеці об'єкту спрямовано на створення можливих каналів витоку інформації, що захищається (передумов до її витоку) і безпосередньо на витік інформації [2-4]. Одне з ключових понять в оцінці ефективності прояви загроз об'єкту інформаційної безпеки – збиток, що наноситься цьому об'єкту (підприємству) в результаті впливу загроз.

Метою роботи є аналіз існуючих методів та засобів, які використовуються для захисту підприємства. В роботі розглянуті існуючі підходи забезпечення безпеки, для створення комплексних систем захисту інформації. Запропоновано використання інтелектуального підходу, базованого на використанні штучних нейронних мереж, для створення системи керування системою управління доступом на підприємство. Створено програмний модуль за допомогою мови Python, який використовується для моніторингу показників підприємства [5].

Список літератури

1. Коваленко А.А. Подходы к синтезу технической структуры компьютерной системы, образующей систему управления объектом критического применения. *Збірник наукових праць Харківського університету Повітряних сил*. 2014. № 1. С. 116–119

2. Jakobson G. Mission-Centricity in Cyber Security: Architecting Cyber Attack Resilient Missions. International Conference on Cyber Conflict, CYCON. 2013. P. 1-18.

3. Коваленко А. А. Подходы к синтезу информационной структуры системы управления объектом критического применения / А.А. Коваленко // Системи обробки інформації. – 2014. – № 1(117). – С. 180-184.

4. Кучук, Г.А. Концептуальний підхід до синтезу структури інформаційно-телекомунікаційної мережі / Г.А. Кучук, І.В. Рубан, О.П. Давікоза // Системи обробки інформації : збірник наукових праць. – Х.: ХУ ПС, 2013. – Вип. 7 (114). – С. 106-112.

5. McKinney Wes. Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython. O'Reilly Media, 2012. - 470 p.