Адаптивні засоби захисту інформації на основі апарату нейронних мереж

Виконав студент IV курсу групи КА-45
Коломбет Микола Валентинович

Керівник професор кафедри ММСА
Мухін Вадим Євгенійович

Об’єкт і предмет дослідження

Об’єкт дослідження - адаптивні засоби захисту інформації та доцільність використання різних видів нейронних мереж.

Предмет дослідження - моделі і методи захисту інформації на основі нейронних мереж.

Мета дослідження - розробити програмний продукт для розпізнавання загроз з використанням сучасних моделей глибокого навчання, дослідити роботу використаних моделей.

Актуальність

На даний час проблема захисту інформації на електронних носіях є однією з ключових для організацій, фірм та індивідуумів. Це пов’язано з тим, що більшість інформації збігається на комп’ютерах або великих серверах тому дуже важливим є своєчасне виявлення загрози та запобігання діям зловмисника.

Постановка задачі

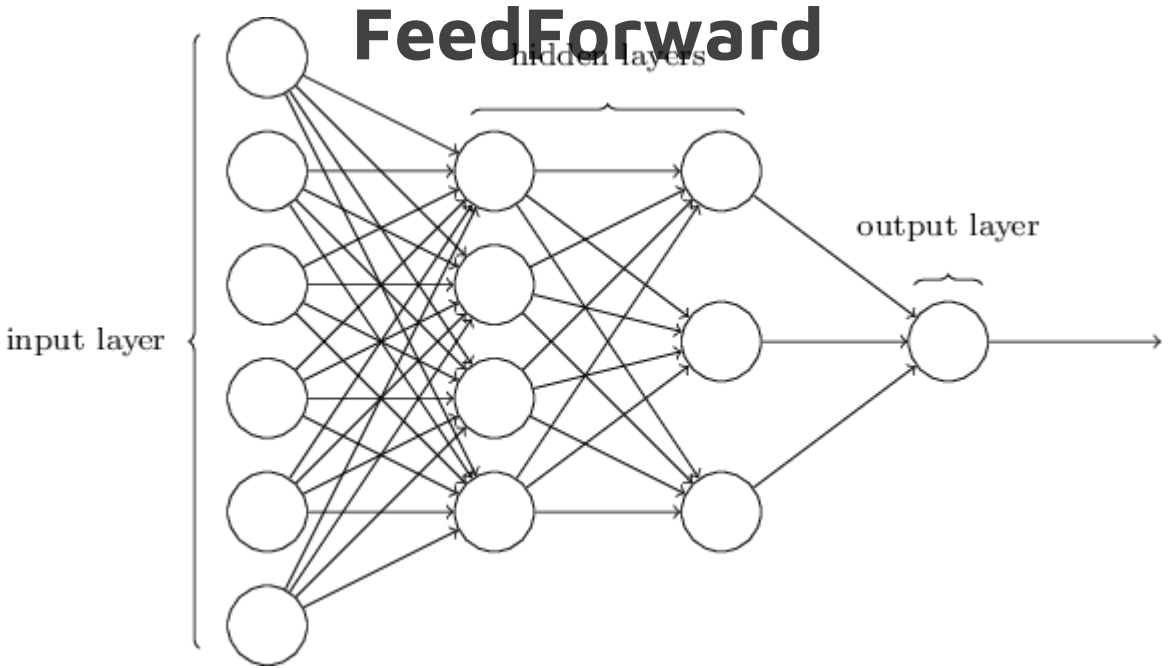
- Визначити доцільність використання нейронних мереж для захисту інформації.
- Провести дослідження найкращих моделей нейронних мереж, на задачах розпізнавання загроз на основі популярних баз даних.
- Проаналізувати отримані результати, визначити переваги та недоліки.
- Розробити програмний продукт для виявлення загроз на основі проведених досліджень.

Переваги застосування нейронних мереж

Набір даних. KDD-99

Attack type	Class	Group	Sub attacks types
Normal	1	A	normal
DoS	3	B	smurf, teardrop, pod, back, land, apache2,udpstrom,mailbomb, processtable, neptune
Probe	4	C	ipsweep, portsweep, nmap, satan, saint, mscan
R2L	2	D	dictionary,ftp_write,guess_passw ord, imap, named, sendmail, spy, xlock, xsnoop, snmpgetattack, httptunnel, worm,snmpguess, multihop, phf, wraezclient, wrazemaster
U2R	5	E	perl, ps, xterm, loadmodule, eject, buffer_overflow, sqlattack

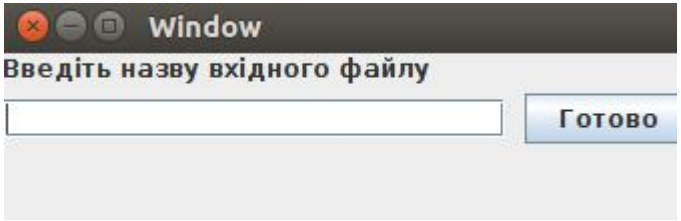
Модель використаної нейронної мережі

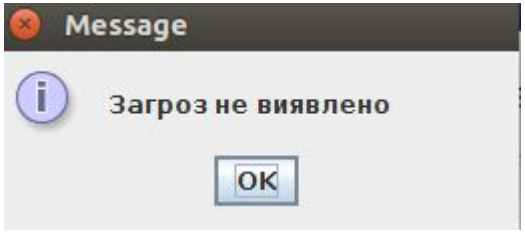


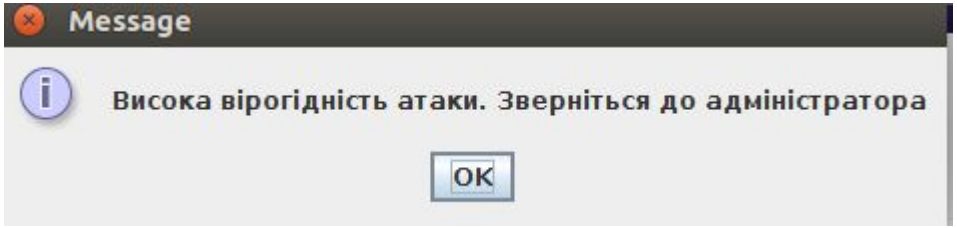
Точність роботи системи

	Розмір вибірки	Правильно вгадано	Відсоток
Prob	200	160	80%
R2L	180	135	75%
U2R	160	134	84%

Інтерфейс користувача







Подальші дослідження

- Подальші дослідження полягають в збільшенні вхідного набору даних
- Навчання на основі інших типів загроз
- Досягнення більшої точності

Висновки

- Розглянуто доцільність використання нейронних мереж для захисту інформації
- Проведено аналіз різних типів нейрониих мереж на відповідність потребам
- Розроблена система для виявлення загрози
- Проведено функціонально-вартісний аналіз програмного продукту з метою оцінки можливості подальшого розвитку

Дякую за Увагу