загрози через межі системи безпеки та апарат аналізу реакції системи захисту на цю загрозу.

Отже, визначивши шляхи вирішення цих завдань, можна суттєво спростити початковий етап побудови систем безпеки.

**Список використаних джерел:**


1. Грищук Р. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р. Грищук, К. Молодецька-Гринчук // *Захист інформації*. 2017. Т. 19, № 4. С. 254-262 URL: http://nbuv.gov.ua/UJRN/Zi_2017_19_4_3.
2. Kahler M. Economic security in an era of globalization. *The Pacific Review*. Vol. 17. No. 4. URL: https://www.tandfonline.com/doi/full/10.1080/09512740 42000326032?scroll=top&needAccess=true
3. Radchenko, S.G. (2015), Formalizovannie i jevristicheskie reshenija v regressionnom analize [Formalized and heuristic solutions in regression analysis], Kornijchuk, Kyiv, Ukraina.
4. Варналій З.С., Онищенко С.В., Маслій О.А. Механізм попередження загроз економічній безпеці України. Економічний часопис XXI. 2016. № 159(5-6). С. 20-24.
5. Системи забезпечення інформаційної безпеки. URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review
6. Економічна безпека підприємств, організацій та установ URL: https://pidru4niki.com/1663080551264/ekonomika/ekonomichna_bezpeka_pidpriyemstv_organizatsiy_ta_ustanov


## ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ КОРИСТУВАЧІВ

***Ломановська А. В.***

*студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»*

Одним з важливих завдань є захист даних користувачів від втрати і пошкодження. Це пояснює зростаючий інтерес до способів захисту, які могли б забезпечити безпеку даних користувачів. На даний момент одним з прогресивних напрямків у цій галузі є використання нейронних мереж для вирішення цієї проблеми.

Важливою особливістю нейромереж, яка використовується у сфері забезпечення безпеки даних користувачів, є їх здатність аналізувати складні багаторівневі алгоритми умисних атак на дані користувачів.

Класичним прикладом такого використання є проект STAMINA [1].

STAMINA представляє собою нейромережу яка здатна конвертувати програмний код в монохромне зображення. Надалі зображення піддається аналізу

вбудованими алгоритмами, в результаті якого нейромережа може визначити, чи є файл шкідливим або ж виявити в ньому ознаки зараження. Проект STAMINA був навчений на великому масиві даних, які компанія Microsoft зібрала з допомогою аналізу дистрибутивів, пропущених через антивірус Windows Defender на комп'ютерах мільйонів користувачів. Завдяки цьому нейромережа навчилася виявляти заражені файли, візуально порівнюючи їх з отриманим «зображенням» шкідливого коду.

Антивірус, функціонування якого було засновано на результатах роботи нейромережі STAMINA в 99% випадків виявляє шкідливий програмний код.

Таким чином, застосування нейромережі дозволило організувати [3]:

- виявлення вторгнень;
- виявлення шкідливих дій;
- класифікацію шкідливих дій;
- впровадження навчання програмного забезпечення для захисту від виявлених шкідливих дій;
- оцінку можливих ризиків втрати даних, пов'язаних з функціонуванням самої нейромережі.

Функціонування нейромереж засновано на використанні штучного інтелекту (ШІ), який можна класифікувати за двома рівнями.

ШІ першого рівня широко застосовується в державних і корпоративних структурах. Одним з прикладів цього типу ШІ є пошук і блокування шкідливих програм евристичним методом. ШІ другого рівня являє собою самопрограмоване середовище, яке має особливість до автоматичної модифікації власних алгоритмів через механізм корекції помилок при виробленні рішень. У сфері кібербезпеки його використовують для виявлення різних типів атак і їх попередження.

Застосування нейромереж дозволило значно скоротити час на розпізнавання атак наступних типів:

1. *DDos* - атак, які зводяться до генерації надлишкового трафіку від хоста, з-за чого відбувається перенавантаження обслуговуючого сервера і послідуюче його відключення.
2. *R2L* – невідомий користувач отримує управління комп'ютером віддалено;
3. *Probe* – отримання конфіденційної інформації за допомогою сканування портів;
4. *U2R* – отримання зареєстрованим користувачем прав суперкористувача (root);
5. *Main-in-the-Middle* – перехоплення даних, з допомогою якого можна впроваджуватися в існуюче підключення;
6. *Session Hijacking* – один з варіантів Main-in-the-Middle, який дозволяє втручатися у відкритий канал передачі даних, для отримання доступу до інформації або до служб у комп'ютерній системі.

Проведені дослідження на виявлення нейромережею перших чотирьох атак показало, що вони можуть успішно справлятися з визначенням цих атак з великою точністю. Для виявлення п'ятого і шостого типів атак застосовувалися рекурентні нейронні мережі, які орієнтовані на обробку послідовних значень.

Таким чином, можна з упевненістю стверджувати, що дослідження в області захисту даних користувачів з використанням нейронних мереж відкрили перспективні можливості для використання їх у сфері кібербезпеки.

**Список використаних джерел:**

1. Нейромережа STAMINA. URL: https://www.iguides.ru/main/security/microsoft_i_intel_sozdayut_idealnyy_antivirus/.
2. Штучний інтелектURL: https://spydell.livejournal.com/633585.html.
3. Нейромережі в кібербезпеки. URL: https://habr.com/ru/post/587694/

***Науковий керівник: доцент Задерейко О.В.***

## МЕТОДИ ЗАХИСТУ БАЗ ДАНИХ

***Маскименко А.С.***

*студентка 1 курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»*

Сучасні компанії обов’язково мають свою особисту конфіденційну інформацію різних видів, яку треба забезпечити максимальну безпеку в середовищі бази даних.

База даних (БД) – це впорядкований набір логічно взаємопов’язаних даних або сукупність матеріалів, які можуть бути найдені і оброблені за допомогою комп’ютера. БД використовується спільно, та призначена для задоволення інформаційних потреб користувачів.

Система керування базами даних (СКБД) - це комплекс програмних і мовних засобів, необхідних для створення баз даних, підтримання їх в актуальному стані та організації пошуку в них необхідної інформації.

Головним завданням БД є збереження значних обсягів інформації (даних).

На сьогоднішній день існують такі аспекти захисту інформації [1]:

- цілісність;
- захист інформації від несанкціонованої модифікації;
- конфіденційність;
- захист від несанкціонованого ознайомлення з інформацією;
- доступність в сенсі підтримання системи в робочому стані та способи швидко відновити втрачену чи пошкоджену інформацію.

Відповідно, до даних аспектів захисту інформації, виділяють такі загрози:

- загрози цілісності (знищення та модифікація інформації);