1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

2. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf

3. Система захисту інформації Лоза™-1, ВЕРСІЯ 4 [Електронний ресурс]. – Режим доступу: http://avtoprom.kiev.ua/avtoprom/ru/content/Система-защиты-информации-ЛОЗА™-1-версия-4

АНАЛІЗ МЕТОДІВ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕЦІ

Онищенко Ю. М., Доманов Б. Г.
Харківський національний університет внутрішніх справ, Харків, Україна

Стрімкий розвиток інформаційних технологій та обчислювальних процесів зумовлюють необхідність чіткого розуміння та обґрунтування сучасних напрямків науки та техніки. Потужним інструментом прийняття рішень, які відіграють значення для прогресивного науково-технічного розвитку, є штучний інтелект. Вирішення надскладних завдань, пов'язаних із застосуванням технологічних процесів та наукових рішень напряму залежить від ефективного використання алгоритмів та систем штучного інтелекту. Проблематика застосування методів та систем штучного інтелекту є новим напрямком прикладної науки, який повинен мати ґрунтовну теоретичну деталізацію. Зважаючи на потребу у розвитку інтелектуальних технічних систем, спрямованих на розв'язання найскладніших виробничих завдань, дослідження методів та систем є штучного інтелекту є актуальним напрямом наукових узагальнень та пошуків [1]. У той же час активний розвиток технологій штучного інтелекту та аналізу великих даних відкриває для держави та бізнесу нові можливості оптимізації операційної та управлінської діяльності за рахунок цифровізації окремих процесів та цілих галузей. Тому актуальним та своєчасним є розгляд можливостей застосування технологій штучного інтелекту до такої галузі як оцінка ризиків [3].

Метою доповіді є визначення методів оцінки ризиків безпеки підприємства із застосуванням штучного інтелекту та надання практичних рекомендації щодо попередження ризиків інформаційних систем з використанням системи штучного інтелекту.

В доповіді розглянуто правові основи застосування технологій штучного інтелекту, проаналізовано методи оцінки стану інформаційної безпеки та надано практичні рекомендації щодо застосування технологій штучного інтелекту для нівелювання ризиків інформаційної безпеки підприємства. Подальші дослідження повинні бути спрямовані на з'ясуванні можливості розподілу методів за напрямками використання та за критерієм ефективності

відповідно до пріоритетів, закріплених Концепцією розвитку штучного інтелекту в Україні [4].

Список літератури

1.Батареєв В.В. Методи та системи штучного інтелекту. Вісник Хмельницького національного університету. 2021. №1 (293). С. 17-21.

2.Ковтуненко Ю.В. Застосування штучного інтелекту у системі управління підприємством: проблеми та переваги. Economic journal Odessa polytechnic university. 2019. №2 (8). С. 93-99.

3.Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.

4.Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації. 2020. № 4 (44). С. 6-11.

РОЛЬ КРИПТОГРАФІЇ В ЗАБЕЗПЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ДАНИХ В АНТИВІРУСНИХ СИСТЕМАХ

Хівренко Д. В., Медведєв С. О.
Харківський національний університет внутрішніх справ, Харків, Україна

Кожне антивірусне ПО крім своєї основної функції виявлення та запобігання дії зловмисних файлів має забезпечувати належну конфіденційність даних своїх користувачів. Адже лише за виконанням цієї умови особисті дані як звичайних користувачів, так і великих корпорацій можуть бути у безпеці. [1]. Метою доповіді є аналіз можливостей криптографії в антивірусних системах.

В доповіді визначенні методи захисту даних в специфікаціях і базах даних, захисту телекомунікацій та підписи і цифрового сертифікату [2]. Значна увага приділяється можливостям використання апарату криптографії у цих найважливіших сферах забезпечення конфіденційності.

Таким чином, криптографія важлива для забезпечення конфіденційності даних в антивірусних системах, оскільки вона допомагає захистити інформацію від несанкціонованого доступу та забезпечує безпеку важливих даних і комунікацій. Використання криптографії сприяє підвищенню ефективності та надійності антивірусних систем.

Список літератури

1. Про електронний цифровий підпис : Закон України від 22.05.03 р. № 852-IV. – URL: https://zakon.rada.gov.ua/laws/show/852-15 (дата звернення 13.10.2023)

2. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І. Горбенко ; Харк. нац. ун-т радіоелектрон., ЗАТ “Ін-т інформ. технологій”. – Х. : Форт, 2012. – 868 с.