НЕСТЕРОВ Дмитро Сергійович,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
СВІТЛИЧНИЙ Віталій Анатолійович,
доцент кафедри протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

РОЛЬ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЦИФРОВОЇ БЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ СТАБІЛЬНОСТІ ТА ПРОЦВІТАННЯ СУСПІЛЬСТВА ТА ДЕРЖАВИ

У сучасному світі інформаційні технології є неодмінною складовою успішного розвитку суспільства та держави. Цифровізація стала ключовим фактором, що дозволяє більш ефективно використовувати ресурси та забезпечує зручний доступ до інформації та послуг. Завдяки сучасним інформаційним технологіям та цифровізації, суспільство та держава мають можливість досягнути нових рівнів розвитку та процвітання. Проте, разом з розвитком цифрових технологій зростає і загроза кіберзлочинності. Кіберзлочини можуть мати серйозні наслідки. Кіберзлочини можуть мати різні форми – від крадіжок особистої інформації до атак на критичну інфраструктуру держави такі, як енергетичні мережі, системи транспорту або телекомунікацій.

Такі атаки можуть мати серйозні наслідки, включаючи економічні збитки, порушення прав людини та загрозу національній безпеці. У зв’язку з цим, необхідно зробити акцент на забезпеченні цифрової безпеки та розробці ефективних стратегій захисту.

Щоб боротися з цими загрозами, потрібні ефективні стратегії цифрової безпеки. Один з підходів до забезпечення цифрової безпеки – це використання інноваційних технологій, таких як блокчейн та штучний інтелект, для створення більш безпечних та надійних систем. Застосування технології блокчейн може допомогти забезпечити безпеку та прозорість в області фінансів, медицини та енергетики. Технологія блокчейн може допомогти забезпечити надійність транзакцій та даних, а штучний інтелект може використовуватися для виявлення та усунення загроз та вразливостей у реальному часі [0]. Штучний інтелект може виявляти аномальні вчинки та атаки на комп’ютерні системи, що дозволяє реагувати на них швидко та ефективно, наприклад [2]:

Штучний інтелект (ШІ) може бути використаний для виявлення аномальних вчинків та атак на комп’ютерні системи за допомогою різних методів. Ось декілька з них:

1) Машинне навчання: ШІ може бути навчений на основі великої кількості даних про нормальну поведінку користувачів та систем. За допомогою алгоритмів машинного навчання, таких як навчання з учителем або без учителя, можна побудувати модель, яка буде виявляти аномальні вчинки та атаки.

2) Аналіз великих даних: ШІ може бути використаний для аналізу великих обсягів даних, що дозволяє виявляти патерни та залежності. Це допомагає виявляти аномальні вчинки та атаки, які можуть бути непомітними для людського ока.

3) Нейронні мережі: ШІ може використовувати нейронні мережі для виявлення аномальних вчинків та атак. Нейронні мережі здатні вивчати складні залежності між даними та виявляти аномалії.

4) Аналіз поведінки: ШІ може аналізувати поведінку користувачів та системи, щоб виявляти аномальні вчинки та атаки. Наприклад, ШІ може аналізувати те, як користувач зазвичай взаємодіє з системою, і виявляти відхилення від цієї поведінки.

Загалом, ШІ може бути використаний для виявлення аномальних вчинків та атак на комп'ютерні системи за допомогою різних методів, що базуються на машинному навчанні, аналізі даних та поведінки. Помітною проблемою цифрової безпеки є також недостатня освіта та усвідомлення простих користувачів. Необхідно надавати доступну та зрозумілу інформацію про можливі загрози та методи їх запобігання, а також проводити тренінги та навчання з цифрової грамотності.

Недостатня освіта та усвідомлення користувачів є ще однією проблемою цифрової безпеки. Більшість людей не розуміють ризики, пов'язані з використанням інтернету та цифрових технологій, тому необхідно надавати доступну та зрозумілу інформацію про можливі загрози та методи їх запобігання. Також, проведення тренінгів та навчання з цифрової грамотності може допомогти користувачам розуміти загрози та захищати свою приватність та безпеку в Інтернеті. Мені на все життя запам'яталась фраза з якогось художнього фільму який оснований на реальних подіях про кіберзагрози, не пам'ятаю вже назву, але ось ця фраза – «у системі головна загроза розшифровки даних, або ж їх втраті та оприлюдненню – це людина», тому я вважаю, що треба ще зі школи розповідати які є способи, яким чином, і найголовніше, як на це не попастися, і таке інше, на даний момент, технології з кожним днем оновлюються, доповнюються, та відносно, що кібератак все більше, способів також!

Список використаних джерел:

1. Блокчейн, що це, і для чого він потрібен. URL : https://fincult.info/article/blokcheyn-chto-eto-takoe-i-kak-ego-ispolzuyut-v-finansakh/

2. Штучний інтелект від Ш до І, що це і для чого його можна використовувати URL : https://speka.media/ai/vid-s-do-i-shho-take-stucnii-intelekt-ta-yak-vin-transformuje-svit-xv7039.