УДК 004.056.54

Мельничук Р. С., здобувач 3 курсу
спеціальності 125 «Кібербезпека»
Зелінська О.В., к.т.н., доцент,
доцент кафедри інформаційних технологій

СУЧАСНИЙ СТАН ТЕХНОЛОГІЙ КІБЕРЗАХИСТУ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Донецький національний університет імені Василя Стуса, м. Вінниця

Зростання ринку інформаційних технологій породило нові можливості та виклики для приватних та державних організацій. Потреба в захисті інформації, оброблюваної в інформаційно-обчислювальних системах створила великий ринок програмних та апаратних рішень для захисту від кіберзагроз.

Розвиток галузі кібербезпеки - це безперервний процес, в якому безпосередню участь приймають кіберзлочинці, розробники систем захисту та звичайні користувачі, які є проміжною ланкою між попередніми двома. Кіберзлочинці створюють нові інструменти для виявлення вразливостей в програмних продуктах, мережевих протоколах, системних службах тощо; пишуть шкідливий софт для здійснення будь-яких дій всередині систем, в які змогли проникнути; розробляють тактики, техніки й процедури для вчинення атак. Розробники в свою чергу орієнтуються на відомі та вивчені проблеми, а також на потенційні загрози, створюючи нові технології та методики протидії несанкціонованим діям. Користувачі слугують зворотнім зв'язком та своєрідним полігоном як для злочинців, так і розробників, адже саме на них випробовують власні розробки та досягнення і ті, й інші. Інтеграція систем кіберзахисту з новими сторонніми технологіями відкриває можливості зовсім інших масштабів.

В публікації "Вдосконалення кіберзахисту інформаційних систем за рахунок адаптивних технологій розпізнавання кібератак" автори В.Лахно, Терещук А. та Петренко Т. вказали на необхідність проводити дослідження, спрямовані на розвиток методологічних і теоретичних основ інформаційного синтезу систем кібер-захисту, здатних до самонавчання та запропонували модель створення адаптивної системи розпізнавання кіберзагроз [1, с.1].

В статті "Застосування штучного інтелекту в сфері кіберзахисту" автори Кузьмина В.І.,Стародубець І.О. та Ткач Ю. М. розповіли про тенденції зміни галузі кібербезпеки та навели проблеми й перспективи застосування штучного інтелекту [2].

У статті "Інтелектуальна система кіберзахисту" автори Скумін Т.Ф. та Стасишин Р.М. описали архітектуру нейромережевої штучної імунної системи кіберзахисту, що складається з інтелектуальних датчиків (імунних детекторів) [3, с.1].

Як видно, автори найбільш докладно дослідили саме напрям розвитку засобів кіберзахисту, пов'язаний зі штучним інтелектом. Однак зовсім не розкрита тема розвідки та активного виявлення загроз.

Часи, коли хостові системи виявлення/попередження вторгнень були передовими засобами для кіберзахисту, давно позаду. Нині настала епоха глобальної інформатизації та цифрової трансформації. Мережеві системи набули величезних масштабів, велике різноманіття обчислювальної техніки з різними технічними характеристиками, вразливостями спричинило появу значної кількості нових програмно-технічних засобів. Великі корпоративні мережі потребували нових рішень для комплексного управління інформаційною безпекою. Було створено хмарні сервіси, що включають в себе більшість сучасних безпекових рішень: міжмережеві екрани нового покоління, системи виявлення/попередження вторгнень на базі штучного інтелекту, антивіруси нового покоління, системи захисту кінцевої точки тощо.

З початком пандемії COVID-19 інтерес великих компаній до захисту в кіберпросторі суттєво зріс. В умовах домашньої ізоляції споживання електронно-інформаційних послуг онлайн-індустрії піднялось на новий рівень. Внаслідок переведення спеціалістів кібербезпеки на дистанційну роботу продуктивність їх праці знизилась, а отже виросли ризики та чинники, що призвели до реалізації кіберзагроз. На рисунку 1 вказано тенденції їх зростань під час глобальної ізоляції:

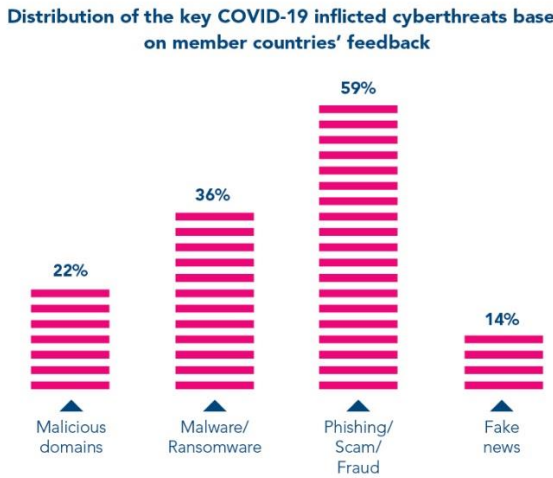

Рисунок 9. Зростання впливу кіберзагроз під час пандемії

Значна частина компаній врешті почала розглядати задачі захисту власних інфраструктур від кібернападів всерйоз, чого досі не було.

Все більшу популярність здобуває концепція активного виявлення загроз, призначена для виявлення гіпотетичних загроз, або загроз, що наявні в системі, але не усунені. Тому що складні кіберзагрози можуть обходити найскладніші автоматизовані системи кіберзахисту. Згідно зі статистикою, автоматизовані інструменти безпеки та аналітики центрів управління безпекою (SOC) рівня 1 і 2 повинні бути в змозі впоратися приблизно з 80%

загроз, все одно потрібно турбуватися про 20%, що залишилися. Інші 20% загроз, швидше за все, включають складні загрози, які можуть завдати значної шкоди [4]. Більшість традиційних систем захисту призначені для виявлення та блокування загроз на етапі їх спроби втручання в систему об'єкта інформаційної діяльності, отже, якщо загроза все ж проникне, то зможе безперешкодно існувати в скомпрометованій системі. Активним виявленням загроз займаються так звані "мисливці" - досвідчені фахівці з кібербезпеки, що діють за певним алгоритмом, в залежності від вихідних даних, отриманих розвідкою загроз. Розвідка даних - це знання, створені з фактичних даних (механізми, послідовності подій, контекст).

ІТ-індустрія відчуває значне піднесення галузі кібербезпеки завдяки сприятливим умовам та інвестиціям бізнесу й державних організацій. Концепція активного виявлення загроз є зручною та дуже гнучкою, цілком можливо, що ще багато компаній почне адаптувати власні продукти кіберзахисту під неї.

Список літератури

1. Вдосконалення кіберзахисту інформаційних систем за рахунок адаптивних технологій розпізнавання кібератак: https://jrnl.nau.edu.ua/index.php/ZI/article/view/10588

2. Застосування штучного інтелекту у сфері кіберзахисту: http://ir.stu.cn.ua/bitstream/handle/

3. Інтелектуальна система кіберзахисту: http://elartu.tntu.edu.ua/bitstream/

4. Threat-hunting: https://www.ibm.com/topics/threat-hunting

УДК 004.94+004.8

Мисько Б.В. та Первачук Р.Ю.
спеціальності 122 «Комп'ютерні науки»
Ніколюк П.К., професор
кафедри інформаційних технологій

БАЗОВЕ ВИКОРИСТАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ЗВУКУ

Донецький національний університет імені Василя Стуса, м. Вінниця

У сучасному світі відбулося багато інноваційних досягнень, які сильно вплинули на життя людей. Одним із найбільш актуальних відкриттів був «Штучний інтелект».

Штучний інтелект (ШІ) – це набір алгоритмів, за допомогою яких, машина обробляє і використовує інформацію. Наприклад, вдосконалює знання та вміння, вчиться ухвалювати правильні рішення, тобто імітує людину.
Поняття штучного інтелекту пов'язане з такими термінами, як: