4. Мінаєва В.О., Нінова Т.С., Шафорост Ю.А. Аналітична хімія. Титриметричний аналіз: Навчальний посібник для студентів вищих навчальних закладів. Черкаси, Вид. від. ЧНУ імені Богдана Хмельницького, 2010, 456 с.

УДК 004.49

Кручинська Дар'я,
асистент кафедри комп'ютерних наук та інформаційних технологій
Житомирський державний університет імені Івана Франка

АДАПТАЦІЯ КІБЕРБЕЗПЕКИ ДО СУЧАСНИХ ВИКЛИКІВ: ОГЛЯД СУЧАСНИХ ПРАКТИК У КІБЕРБЕЗПЕЦІ З АНАЛІЗОМ ЗАСТАРІЛИХ

Останні роки стали досить важкими для України у різних аспектах життя, в яких кібербезпека відіграла не останню роль та теж зазнала низки проблем. Винахідливість та методи кібератак як на бізнес, так і на державні установи вражає. Тому постає питання про нові підходи безпеки та аналізу вже існуючих, для визначення актуальності на сьогодні.

Зокрема у лютому 2024 року, міністр освіти Оксен Лісовий у своєму Twitter, повідомив про хакерську атаку на сайт Міністерства освіти, та додатково були опубліковані дописи на офіційних сторінках Міністерства освіти, про російську кібератаку. Це була далеко не перша атака, яка здійснювалась як зі сторони російських хакерів, так і інших. Саме тому актуальність адаптації кібербезпеки до нових тенденцій залишається досить важливою та актуальною.

Всесвітній економічний форум у своєму звіті, який вийшов в січні цього року, вніс кіберзлочинність до десятки глобальних ризиків найближчого десятиліття. Зокрема у проєкції десятиліття кібербезпека посіла 8 місце, та стала на ряду з такими проблемами як вимушена міграція, забруднення тощо. А у проєкції на найближчі 2 роки, кібербезпека посіла 2 місце у ряді глобальних проблем [4, ст. 8].

Також у звіті 2024 року SonicWall зазначено, що загальна кількість спроб вторгнення у 2023 році, порівняно із 2022 роком зросла близько на 20% і найголовніше, що це було зафіксовано у різних галузях дослідження, таких як охорона здоров'я, освітні заклади, фінансові тощо. Хоча і деякі звернення не несли великих загроз, але все ж вони відбувались [3, ст. 8].

Деякі експерти вважають, що глобально фіксують лише до 25% усіх кіберзлочинів які відбуваються, що є досить малим показником. Ризик кібератак лише стрімко зростає, адже є попит на дистанційну роботу, та у зв'язку з важкою політичною ситуацією, саме кібератаки стають одним із засобів нанесення ключових економічних, політичних ударів. Значна частина кіберзлочинців, які пов'язані з Росією, реалізовують DDos атаки тощо, і на інші країни світу. Тому кожен має дбати про свою кібербезпеку.

IT-компанія WEZOM у своїх дослідженнях виділяє ключові тренди у 2024 році, за якими саме стоїть майбутнє кібербезпеки:

1. Використання блокчейн для кіберзахисту.
2. Штучний інтелект по обидва боки кіберпростору.
3. Поняття "Кіберстійкості" як альтернатива захисту від кіберзагроз.
4. Модель з нульовою довірою.
5. Реалізація посиленого регулювання кібербезпеки.
6. Протидія кібервійні.[1]

Використання блокчейн для кіберзахисту. На сьогодні технологія блокчейн ніяк не асоціюється у більшості людей саме із кіберзахистом, а в більшості випадків виникає думка про криптовалюту. Але насправді така думка є хибною, адже блокчейн базується на криптографічних методах, консенсусі та розподілених мережах.

Методи які базуються на основі блокчейну, використовуються при авторизації користувачів без пароля для забезпечення безпеки від витоку даних. І це тільки один варіант використання технологій блокчейн для кіберзахисту. Досить інтенсивно технологія блокчейн використовується у централізованому збереженні даних. Це є досить актуальним на сьогодні, а особливо в нашій країні,

оскільки більшість реєстрів для надання послуг, перейшли у цифровий варіант. Тому зі стрімким використанням цифрових технологій у різних сферах життя, буде зростати й використання технології блокчейн для кіберзахисту.

Штучний інтелект по обидва боки кіберпростору. Штучний інтелект з кожним днем набирає все більше обертів та методів застосування. Звичайно кіберзлочинці використовують його також для завдання шкоди, зокрема генерування шкідливого коду, для подальшого застосування, або ж генерування фото, відео тощо, у соціальній інженерії й не тільки.

Спеціалісти з кібербезпеки також вже використовують штучний інтелект у своїй роботі, а саме для налаштування автоматизованого виявлення загроз у реальному часі, або ж недостовірного згенерованого контенту тощо. Тому з розвитком ШІ й зростає його використання з обох сторін кіберпростору.

Поняття "Кіберстійкості" як альтернатива захисту від кіберзагроз. Звичайно будь-який фахівець налаштований зробити все можливе аби запобігти кібератакам та захиститись від них, але враховуючи нові тренди та можливості, не завжди це можливо. На жаль поки захистити систему, компанію чи мережу на 100% неможливо. Саме тому і постає поняття "кіберстійкості" у даному процесі.

Сутність даного поняття полягає у тому, що компанії чи організації за основу ставлять не кібербезпеку, а саме можливість стійкості створеного захисту на нові атаки. Адже такий варіант допомагає мінімізувати втрати різного характеру та головне не зупиняє роботу системи, що є важливим. Звичайно такий перехід не є легким та потребує фінансів, але саме за цим майбутнє.

Модель з нульовою довірою. Актуальність використання моделі нульової довіри все більше стає популярною, особливо після низки різних кібератак як на світові компанії, так і на державні установи. Досить велика кількість внутрішніх систем компанії виходить за межі корпоративної мережі, наявні віддалені співробітники та компанії партнери, ну і звичайно пристрої інтернету речей. Саме тому більше неможливо забезпечити внутрішній периметр, який буде під контролем та у безпеці. Логіка даної моделі базується на тому, що не можна

довіряти ні користувачу, ні пристрою тощо, доки ретельно не пройде перевірка. Тому під час дистанційної роботи, це стає ще більш актуальним.

Реалізація посиленого регулювання кібербезпеки. Не тільки компанії чи організації занепокоєні виникненням кіберзагроз, а й уряди країн. Тому це питання стає таким важливим та актуальним на рівні держав. Багато країн світу вже почали приймати різні види законів для регламентування кіберпростору, зокрема спрямовані на захист особистих даних, безпеку різноманітних програмних продуктів і не тільки, впровадження новітніх трендів тощо.

Звичайно Україна не залишається осторонь даних питань і оновлює вже існуючі закони і не тільки. Зокрема затверджено план заходів на 2023-2024 роки, які будуть реалізовувати стратегію для забезпечення кібербезпеки в Україні. [2] Даний план налічує 63 пункти, які мають бути реалізовані у державі протягом зазначеного терміну. Це значно покращить захист держави від кібератак та спрямує цей напрямок на кіберстійкість, яка розглядалась вже раніше. Тому досить важливо впроваджувати регулювання кібербезпеки на всіх рівнях.

Протидія кібервійні. Тренди змінились не тільки у кіберзахисті, але й в методах та наживах кіберзлочинців. Наразі ще більшою загрозою стали країни-агресори, які все більше застосовують методи кібератак для досягнення своїх цілей. Із війни в Україні вже видно, що як правило напади проводяться як проти військової, так і проти цивільної інфраструктури. Такі країни як росія, КНДР та Іран інвестують великі суми для впровадження кібервійни.

Особливу увагу приділяють таким видам як DDoS-атаки на будь-які сфери і організації, фішингові та інші атаки для отримання доступу до даних, або ж системи. Тому всі галузі повинні бути готові до даних атак.

Оскільки час не стоїть на місці, а технології розвиваються досить стрімко, тому вже досить значна частина тих методів, які були базовими та дієвими буквально рік-два тому, вже не мають тої сили. Але є низка методів, які компанії все ж продовжують використовувати, хоча це і не є доцільним.

Розглянувши актуальні підходи для захисту в кіберпросторі, є ті, які вже ідуть на другий план, та є не такими ефективними у реаліях сьогодення, але все

ж залишаються у використані. Можна виділити чотири неактуальних підходи у кіберзахисті:

1. Реалізація кіберзахисту виключно у IT-підрозділах, вважаючи їх вразливими.
2. Стратегія реагування.
3. Ігнорування аналітики інцидентів.
4. Концепція захисту периметра.

Реалізація кіберзахисту виключно у IT-підрозділах, вважаючи їх вразливими. На сьогоднішній день, вже одного програміста, чи фахівця з цифрових технологій недостатньо для реалізації захисту компанії або ж установи. Кібербезпека - це не просто захист від шкідливого ПЗ, а це ціла логічна стратегія, тому важливо вкладати ресурси у цей захист. З різних досліджень велика частка кібератак залежить від людського фактора, адже більшість співробітників у різних відділах навіть не підозрюють, що саме вони відкрили фішинговий лист, для прикладу. Саме тому варто вкладати ресурси і в навчання персоналу, особливо вразливих відділів.

Якщо компанія відслідковує нові можливості у кіберзахисті, то вона швидше адаптується до нових викликів та стає більш кіберстійкою. Використання новітніх технологій, таких як ШІ буде тільки покращувати ситуацію, та може стати тією основою захисту, якої не вистачало.

Стратегія реагування. Даний метод полягає в тому, щоб реагування відбувалось лише при виникненні проблеми. Такий варіант зумовлений тим, що організація обирає варіант реагування, замість підготовки чи попередження інциденту. Цей варіант є досить небезпечним, адже за час вирішення і реагування, зловмисник може вже отримати доступ до того, що саме шукав.

Саме тому на заміну такому методу приходить кіберстійкість, як метод протидії кіберзагрозам, який вже розглядався в актуальних методах. Потрібно не тільки резервування даних тощо, а й постійний моніторинг і звичайно це не все, що потребує уваги.

Ігнорування аналітики інцидентів. Значна частина компаній після того, як відбувся якийсь інцидент, особливо якщо його вдалось вирішити, ігнорує аналіз даного інциденту для запобігання у майбутньому, або для розуміння чому саме так сталось. Але дана аналітика є досить важливою, що допоможе дати відповіді на низку питань для наступного реагування, оновлення політик безпеки та головне інформування співробітників. Звичайно краще аналізувати інциденти інших компаній, аніж власної, але в даному випадку вся інформація важлива.

Концепція захисту периметра. Дана методика захисту базується лише на захисті окремого периметра, а все, що виходить за його рамки є небезпечним. Такий підхід використовують вже понад 30 років, але все ще є компанії які ним продовжують користуватись, не дивлячись на його неактуальність.

Хоча після того, як прийшла пандемія, та більшість працівників перейшли на дистанційну роботу, даний підхід став не те, що неактуальний, а неможливий. Саме тому на заміну цього методу приходить принцип нульової довіри, який дозволяє реалізувати гнучку, але й водночас прискіпливу політику доступу до системи та даних.

Отже, можна зробити висновок, що все ж кіберпростір не надто безпечний, так як технології не стоять на місці, а протидіяти новим кібератакам стає все складніше. Але все ж рішенням даного питання якраз і виступає застосування новітніх методів та принципів на практиці, що допоможе мінімізувати шкоду та ризик від заподіяних кібератак.

Список використаних джерел та літератури

1. Вікторія. 6 трендів кібербезпеки в 2024 році. IT-компанія повного циклу розробки програмних продуктів WEZOM - Київ, Україна. URL: https://wezom.com.ua/ua/blog/6-trendiv-kiberbezpeki-v-2024-rotsi.

2. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України : Розпорядж. Каб. Міністрів України від 19.12.2023 р. № 1163-р. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-р#Text.

3. SonicWall. 2024 sonicwall cyber threat report. URL: https://www.sonicwall.com/threat-report/.

4. World Economic Forum. Global risks report 2024. URL: https://www.weforum.org/publications/global-risks-report-2024/.

УДК 37.04

Кривонос Олександр,
кандидат наук, доцент, доцент
кафедри комп'ютерних наук та інформаційних технологій
Житомирський державний університет імені Івана Франка

ВИКОРИСТАННЯ ШІ В ПРОГРАМУВАННІ

Зі зростанням технологічного потенціалу штучного інтелекту розповсюдження та використання чат-ботів значно зросло. Ці системи, що базуються на різноманітних алгоритмічних моделях, відкривають нові можливості у багатьох сферах, від розважальних до професійних інструментів. Особливо варто відзначити застосування чат-ботів у освіті, електронній комерції, медичних консультаціях і, звісно, у програмуванні.

У сфері програмування чат-боти діють як помічники, які спрощують та оптимізують робочі процеси. Вони можуть давати поради з коду, відповідати на технічні питання і навіть допомагати вирішувати складні алгоритмічні задачі. Однак ця інноваційна можливість також викликала непередбачені наслідки, особливо в галузі освіти.

Особливо тривожною є тенденція деяких студентів використовувати чат-ботів не для навчання чи допомоги у вирішенні програмних завдань, а для прямого копіювання рішень. Така практика підриває освітній процес, оскільки студенти не розвивають необхідні навички і знання. Ця проблема особливо актуальна в галузі програмування мовою С, яка вимагає глибокого розуміння алгоритмів та логіки програмування.