Кундос М.Г, к.т.н., ст. викладач,
Соловей Л.Я., ст. викладач,
Багнюк О.М., ст. викладач,
ПВНЗ «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука»
Національний університет водного господарства та природокористування

РОЛЬ СУЧАСНИХ МОВ ПРОГРАМУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

В сучасному інформаційному суспільстві сфера кібербезпеки розвивається швидкими темпами. Все більше потрібно інноваційних підходів для забезпечення захисту цифрових систем і даних від кіберзагроз. Дане дослідження спрямоване на аналіз сучасних методів програмування для забезпечення кібербезпеки.

Сучасний кіберпростір у поєднанні із стрімким розвитком інформаційних технологій, вимагає нових підходів до забезпечення кібербезпеки. У відповідь на зростання кількості загроз з'являються інноваційні методи програмування, спрямовані на створення безпечних систем.

Державний документ [1], що визначає основні принципи, пріоритети, цілі та завдання у сфері забезпечення кібербезпеки країни, був ухвалений Радою національної безпеки і оборони України для протидії зростаючим кіберзагрозам і створення умов для безпечного функціонування кіберпростору.

Серед мов програмування, які успішно застосовуються у кібербезпеці, є C/C++. Є декілька сфер для застосування C++: програми безпеки мережі, криптографічні програми, програми безпеки системного рівня, аналіз шкідливих програм, інструмент для виявлення вразливостей [2].

Однією з ключових тенденцій є застосування сучасних мов програмування, орієнтованих на безпеку, таких як Java, Python, Rust, Go. Ці мови мінімізують помилки роботи з пам'яттю, що є поширеною причиною вразливості у програмах. Інший напрямок – використання криптографічних методів, які дозволяють захищати дані від несанкціонованого доступу. Наприклад, інтеграція перевірених бібліотек, таких, як OpenSSL, спрощує впровадження стандартів шифрування у програмне забезпечення.

Зрештою, інноваційні методи програмування перетворюються на потужний інструмент у боротьбі з кіберзагрозами, що дозволяє створювати надійне програмне забезпечення. Вони не лише забезпечують безпеку, а й підтримують стійкість систем у динамічному цифровому світі.

Багато авторів працюють у галузі інтеграції безпеки у програмуванні. Зокрема, у статті [3] досліджуються мови програмування з точки зору їх застосування в області кібербезпеки. Дослідники аналізують сильні та слабкі сторони кожної мови, демонструючи, яким чином вони можуть бути використані для побудови безпечних систем та програмних рішень. В роботі [4] розкривається питання забезпечення безпеки програмного забезпечення шляхом розробки й використання ефективних моделей та методів.

Спеціалізовані програми необхідні для забезпечення кібербезпеки, оскільки вони повинні аналізувати вразливості систем, моніторити мережеву активність і виявляти аномалії, які можуть свідчити про потенційні загрози. Тому програмісти, які працюють у сфері кібербезпеки повинні мати спеціалізовані навички і знання щоб створювати програми, які будуть ефективно захищати інформацію від кіберзагроз. Вони повинні знати різні мови програмування, володіти методами шифрування даних, а також розуміти як працюють мережі.

Аналіз інноваційних тенденцій щодо розробки інформаційних систем, розкриття їх впливу на сучасні бізнес-процеси, ринок програмного забезпечення та визначення перспективних напрямків розвитку технологій моделювання, проєктування і розробки інформаційних систем досліджено в роботі [5].

Сучасні мови програмування є не лише інструментами для розробки, але й фундаментом кібербезпеки. Вибір мови залежить від конкретних задач, але тенденція до використання більш захищених і продуктивних мов, таких як Rust і Go, свідчить про те, що безпека стає все більш інтегрованою у процес створення програмного забезпечення.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013
2. Куліков В. М., Рябцев В. В., Паршуков С. С. Об'єктно-орієнтоване програмування для фахівців з кібербезпеки: навч. посіб. / ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, 2023. 365 с.
3. Крихівський М.В., Ваврик Т.О., Гобир Л.М. Огляд мов програмування у ракурсі кібербезпеки. Науковий вісник Івано-Франківського національного технічного університету нафти і газу. – 2023, - №2. – С. 61-69
4. Давидов В. В. Моделі та методи підвищення безпеки програмного забезпечення (монографія). Харків, 2021. 146 с.
5. Ткаченко Ольга, Ткаченко Костянтин, Піддубченко Михайло Аналіз сучасних тенденцій розробки інформаційних систем. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» 4.24. 2024. с.205-220.