з найбільшою вагою[3]. Таким чином, теорія графів забезпечує математично обґрунтований підхід до пріоритизації заходів кібербезпеки в умовах активного кіберпротистояння у російсько-українській війні, переводячи проблему з технічної площини у стратегічну.

Отже, застосування теорії графів до аналізу кібербезпеки в контексті російсько-української війни демонструє складну, динамічну природу сучасного кіберпротистояння. Ключові висновки:

1. Кіберпростір став невід'ємною складовою сучасної війни, де віртуальні атаки безпосередньо впливають на фізичний вимір конфлікту
2. Критична інфраструктура залишається найуразливішим і найпривабливішим об'єктом для кібератак
3. Ефективний кіберзахист потребує системного підходу, що враховує взаємозв'язки між різними елементами цифрових систем

Методологія графів дозволяє не лише аналізувати поточний стан кібербезпеки, але й прогнозувати майбутні загрози та оптимізувати розподіл ресурсів для захисту найбільш вразливих компонентів. У світлі продовження російсько-української війни, такий аналітичний підхід стає особливо актуальним для розробки проактивних стратегій кіберзахисту та підвищення цифрової стійкості України.

1. Безкоровайний М.М., Татузов А.Л. "Кібербезпека – підходи до визначення поняття" // Питання кібербезпеки. – 2022.
2. Гнатюк С.О. "Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи" // Безпека інформації. – 2023.
3. Microsoft Digital Defense Report 2023-2024. – Microsoft Corporation, 2024.
4. "Ukraine: Timeline of Cyberattacks" // CyberPeace Institute, 2024.
5. Newman M. "Networks: An Introduction". – Oxford University Press, 2022.

Розробка фільтр генератора псевдовипадкових послідовностей на основі хеш функцій

УДК 621.395.7 (043.2)

Роман Корольов[1], Ейюб Аббаскулієв[2], Ірада Рагімова[3], Станіслав Мілевський[4]

Національний технічний університет "Харківський політехнічний інститут", [1]korolevrv01@ukr.net, [4]milevskiysv@gmail.com

Азербайджанський технічний університет, [2]formemaybe23@yahoo.com, [3]ika1402@icloud.com

Генератори псевдовипадкових послідовностей (ГПВП) відіграють ключову роль у сучасних інформаційних технологіях, зокрема в криптографії, моделюванні, статистиці та програмуванні. Їхня важливість зумовлена здатністю створювати послідовності чисел, які здаються випадковими, але генеруються детермінованим алгоритмом із початковим значенням.

Генератори псевдовипадкових послідовностей повинні відповідати певним вимогам, які залежать від їхнього призначення — від простих симуляцій до криптографічних застосувань. До основних вимог які пред'являються до ГПВП можна віднести[1]:

–*статистична випадковість* (числа в сформованій послідовності повинні бути рівномірно розподілені, без видимих закономірностей чи кореляцій між сусідніми значенням);

–*великий період сформованої послідовності* (кількість чисел до повторення послідовності має бути значно більшим за обсяг даних, який потрібно згенерувати);

– *непередбачуваність (* знання частини послідовності чи алгоритму не повинно дозволяти передбачити наступні значення без доступу до початкового стану);

– *криптографічна стійкість (* за наявності значного обсягу вихідних даних неможливо визначити внутрішній стан ГПВП);

– *швидкість генерації* (ГПВП мають працювати достатньо швидко для цільового застосування);

– *простота реалізації* (ГПВП має бути придатним для реалізації на доступних платформах (мікроконтролери, FPGA, процесори)).

– *стійкість до квантових обчислень* (ГПВП має базуватися на задачах, які залишаються складними навіть для квантових алгоритмів).

Безперервне вдосконалення обчислювальних технологій та зростання їхньої потужності, що відповідає закону Мура, а також прогрес у математичних підходах до криптоаналізу вимагають регулярного перегляду розмірів ключових даних.

У цьому контексті особливу важливість набувають ГПВП заснованих використанні на хеш-функціях, які відповідають суворим вимогам криптографічної стійкості[1]. Його значущість полягає у здатності генерувати непередбачувані послідовності з використанням детермінованих алгоритмів, таких як SHA-256, що робить його незамінним для створення ключів і захисту даних в умовах обмежених ресурсів та загроз квантового криптоаналізу.

В NIST SP 800-90A запропонований ГПВП оснований на використанні хеш функції HMAC (Hash_DRBG). Структурна схема даного ГПВП представлена на рисунку 1.

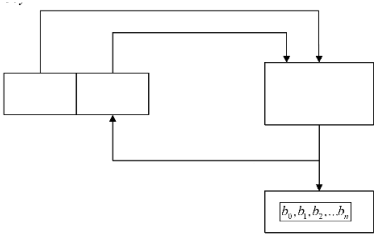

Рис.1. Структурна схема ГПВП на основі хеш функції HMAC

В доповіді пропонується фільтр генератор псевдовипадкових послідовностей на основі хеш функцій з гарантованою довжиною періоду. Структурна схема запропонованого ГПВП представлена на рисунку 2.

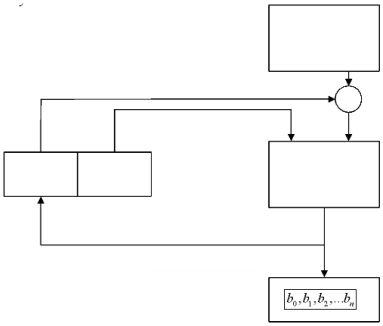

Рис.2. Структурна схема запропонованого фільтр ГПВП на основі хеш функції HMAC

В якості функції *f* можливо використання операцій *xor* або *mod* 2^n. Використання регістра зсуву з лінійним зворотнім (РЗЗЗЗ) зв'язком дає можливість формувати псевдовипадкові послідовності гарантованого періоду, а завдяки хеш-функції (наприклад, SHA-256) запропонований ГПВП забезпечує високу непередбачуваність та легко реалізовується на програмному та апаратному рівні.

1. NIST SP 800-90A Rev.1. URL: https://csrc.nist.gov/pubs/sp/800/90/a/r1/final

Теоретико-множинний підхід до класифікації сучасних методів соціотехнічних атак

УДК 004.056.53(045)

Анна Корченко[1], Кирило Давиденко[2]
[1,2]*Національний технічний університет «Дніпровська політехніка», Україна,*
[1]annakor@ukr.net, [2]kirilldavy@gmail.com,

Постійний розвиток інформаційних технологій і цифрових послуг породжує нові кіберзагрози, зокрема соціотехнічні атаки. Зловмисники застосовують психологічні маніпуляції для отримання несанкціонованого доступу до інформаційних ресурсів, що становить загрозу конфіденційності, цілісності та доступності даних. Особливу небезпеку такі атаки становлять для об'єктів критичної інформаційної інфраструктури (КІІ) та кіберфізичних систем, де наслідки можуть виходити за межі віртуального простору й впливати на реальні технологічні процеси, безпеку життєдіяльності й національну безпеку в цілому.

Відсутність систематизованої класифікації актуальних підходів та відповідних методів реалізації таких атак ускладнює розробку ефективних