ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

СЕКЦІЯ 22. ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

СЕКЦІЯ 23. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Щербина Юрій Володимирович
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

АНАЛІЗ ЕФЕКТИВНОСТІ ПРОГРАМНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

В сучасних системах захисту даних значну роль відіграють потоки псевдовипадкових чисел, що отримуються алгоритмічним рекурентними способами. На їх основі відбувається генерація сеансових ключів для шифрування і від їх якості залежить рівень криптографічного захисту. Ця якість повністю визначається тим, наскільки створена псевдовипадкова послідовність чисел відрізняється від дійсно випадкової. Чим більше сформована послідовність наближається до випадкової, тим більше захищеність криптографічного алгоритму, в якому вона використовується. Для початкової оцінки таких алгоритмів дослідники використовують статистичне тестування, а остаточна оцінка перевіряється шляхом випробування на реальних криптографічних атаках.

Високий рівень безпеки криптографічної системи досягається в тому випадку, коли в основу її алгоритму закладено принцип Керкгоффа, який стверджує, що "безпека системи залежить виключно від ключового матеріалу, а не від дизайну системи" [1]. Це пояснюється тим, що перш ніж зламати сучасну криптографічну систему, зловмисник повинен визначити ключі, які використовуються при розробці алгоритмів, а також протокол, у якому втілено цю систему шифрування.

Стійкість системи захисту основується на припущені, що зловмисник не має уявлення про розподілення ймовірностей символів у ключових послідовностях та аномаліях, що відрізняють їх від справжньої випадковості.

Посилена атака на криптографічну систему виявляє додаткові ключові біти, які можна обчислити, спостерігаючи канальний потік даних, що передається між суб'єктами інформаційного обміну. Безпека програмного забезпечення на основі алгоритмів генерації псевдовипадкових чисел вимагає їх високої якості, що передбачає абсолютну рівномірність розподілення бінарних символів у вихідному потоці зашифрованих повідомлень [2].

Необхідною умовою безпеки криптографічного протоколу є високий рівень випадковості ключів шифрування. Приховування важливих закономірностей щодо виходу генератора випадкових чисел від зловмисників, а також осіб, які знають, як розроблений алгоритм генератора випадкових чисел, є важливою умовою розроблення сучасних систем захисту. Ентропія виходу генератора випадкових чисел повинна бути настільки близькою, наскільки це можливо з урахуванням довжини вихідного бітового потоку.

Ідеальним є генератор псевдовипадкових чисел який формує послідовність, що не є простою для прогнозування зловмисником. Це пов'язано з тим, що іноді

супротивник може знати використовуваний криптографічний алгоритм, і це те, що складає суть принципу Керкгоффа [3].

Згідно з постулатами Голомба, статистична складова генератора псевдовипадкових чисел показує, що кожне значення або результат у заданому діапазоні має однакові шанси на випадіння. Кожне бінарне число має ймовірність 1/2 в діапазоні [0, 1]. Кожна пара вихідних бінарних чисел матиме входження 1/4 і частоту 1/8 для кожного триплету [4]. В такому разі ентропія отриманих вихідних чисел вважається незміщеною, а послідовний вихід – некорельованим. В статистичний тест на випадковість також повинні бути включені обчислення середнього та дисперсійного значення. Якщо вихід для середнього значення близький до 0,5, а вихід дисперсії близький до 0,08, то псевдовипадкові числа можна вважати однорідними.

Недоліком програмних способів генерації псевдовипадкових чисел є циклічність їх повторення і, тому, величина такого періоду є важливим додатковим показником їх ефективності. Чим віт більший, тим більше послідовність буде відповідати потребам криптографії. Запускаючи криптографічний генератор, слід визнати початкове число, від якого буде залежати вигляд вихідної послідовності.

Нарешті, рівномірність розподілення ймовірностей вихідних чисел також залежить від довжини періоду і, для генераторів з малим періодом повторення забезпечити її вкрай важко. Через це, більшість таких генераторів не проходять статистичне тестування, оскільки всередині числового потоку існують серйозні кореляції [5].

В роботі [5] було показано, що ідеальною ситуацією є випадок, коли вихідні числа корелюють послідовно і безпека генератора залежить від співвідношення вихідних чисел. Це означає, що чим кореляція менша, тим більший рівень захисту забезпечує генератор.

Тест χ^2 Пірсона сьогодні є найбільш популярним серед фахівців, що займаються статистичною оцінкою випадкових процесів [6]. Розподілення χ^2 – це негативна величина і пропорція, які показують, як часто реальний випадковий ряди повинен перевищувати обчислене число або значення, отримане в результаті підрахунку нулів і одиниць в певному файлі даних. Для цього використовують наступні процедури.

- Створити програмну реалізацію генератора, що має пройти тестування з використанням χ^2 критерію.
- Створити реалізацію із 100 випадкових чисел в інтервалі від 0 до 1000.
- Розділити інтервал чисел від 0 до 1000 і підрахувати кількість чисел вихідного потоку, що попадають у кожний інтервал.
- Підрахувати різницю між отриманими у кожному інтервалі числами та числом 50.
- Обчислити показник χ^2 за формулою

$$\chi^2 = \sum_{i=1}^{k} \frac{(n_i - p_i N)^2}{p_i N}.$$

Тут $k = 20$, а N дорівнює 1000.

Отриманий показник має бути меншим за табличне значення з урахуванням обраної точності оцінки.

Випробування, що виконувались з лінійними конгруентними генераторами, генераторами побудованим на принципі Фібоначчі з запізненням та генераторах на регістрах зі зворотним зв'язком показали, що вони можуть використовуватись для потреб криптографії лише у якості складових елементів для створення більш складних алгоритмічних конструкцій. Оцінка придатності нового алгоритму генерації псевдовипадкових чисел має розпочинатись з частотного тесту, що є першим тестом у пакеті американського стандарту NIST. Цей тест дає відповідь на питання про те, наскільки співвідношення нулів і одиниць у числовому потоці відрізняється від значення 1/2. Якщо цей тест не виконується, подальше тестування не має смислу. Всі інші тести з пакету NIST – це різні варіанти реалізації тесту χ^2 Пірсона, в яких оцінюється розподілення окремих видів числових комбінації у складі вихідного числового потоку.

Список використаних джерел:

1. Christophe D., Diethelm W. A note on random number generation. URL: http://cran.rproject.org/web/packages/ randtoolbox/ vignettes/fullpres.pdf.

2. Mike H., Paul K., Mark E. M. Analysis of Intel's Ivy Bridge digital random number generator. URL: http://www.cryptography.com/public /pdf/Intel_TRNG_Report_20120312.pdf.

3. Yehuda L. Introduction to cryptography, 89-656. URL: http://u.cs.biu.ac.il/~lindell/89-656/Intro-to-crypto89-656.pdf.

4. Golomb S. W. Shift Register Sequences. San Francisco : Holden Day, 1967. URL: https://dl.acm.org/doi/10.5555/3153732

5. Christophe D., Diethelm W. A note on random number generation. URL: http://cran.rproject.org/web/packages/ randtoolbox/ vignettes/fullpres.pdf.

6. Biege T. Analysis of a strong pseudo random number generator. URL: http://www.suse.de/~thomas/papers/random-analysis.pdf.

Ключові слова: Псевдовипадкова послідовність, алгоритм шифрування, криптографічна атака.

Keywords: Pseudorandom sequence, encryption algorithm, cryptographic attack.