процессе зашифровывания информации, зато алгоритм ElGamal показал в 10 раз лучшую пропускную способность по сравнению с алгоритмом RSA в процессе расшифровывания информации; длина зашифрованных данных алгоритмом ElGamal в 2 раза длиннее исходных данных, в то время как размер зашифрованных алгоритмом RSA данных больше размера исходных данных в среднем на коэффициент 1,4; для всех длин ключей алгоритм ElGamal создает пару открытого и закрытого ключей в среднем в 10 раз быстрее, чем алгоритм RSA, что особенно заметно при значительном увеличении размеров ключей; для алгоритма ElGamal время генерирования ключей растет линейно с увеличением размеров ключей, в то время как для алгоритма RSA оно растет в геометрической прогрессии.

Ключевые слова: *асимметричные алгоритмы, шифрование, дешифрование, криптостойкость, RSA, ElGamal.*

RESEARCH AND COMPARATIVE ANALYSIS OF ALGORITHMS OF ASYMMETRIC ENCRYPTION

T. Matveichuk, V. Smychok

Using a developed software product, a comparative analysis of asymmetric text data encryption algorithms, their advantages and disadvantages, cryptographic strength, experimental evaluation of their characteristics with respect to the efficiency of their computer memory usage, the duration of key generation, data encryption and decryption ability of algorithms, key dimensions, volumes of encrypted and decrypted files has been made. Based on the results obtained, recommendations were given on the use of the encryption methods considered. The RSA and ElGamal algorithms are chosen as asymmetric encryption algorithms.

From the point of view of practical implementation, both in software and hardware, there is no tangible difference between these two methods. However, in their characteristics they are noticeably different. Briefly, the main estimated results obtained are as follows: the cryptographic strength of the ElGamal algorithm is significantly higher than that of the RSA algorithm; the RSA algorithm has a higher speed when encrypting information, and the ElGamal algorithm has the best during decryption; as the key sizes increase, the decryption time by the RSA algorithm grows exponentially, while the duration of the decryption by the ElGamal algorithm has a linear growth order; the RSA algorithm showed 2 times better bandwidth than the ElGamal algorithm in the process of encoding information, but the ElGamal algorithm proved 10 times better throughput compared to the RSA algorithm in the process of decrypting information; the length of the encrypted data by the ElGamal algorithm is 2 times longer than the original data, while the size of the data encrypted by the RSA algorithm is larger than the size of the original data by an average of 1.4; for all key lengths, the ElGamal algorithm creates a pair of public and private keys on average 10 times faster than the RSA algorithm, which is especially noticeable with a significant increase in key sizes; for the ElGamal algorithm, the key generation time increases linearly with increasing key sizes, while for the RSA algorithm it grows exponentially.

Keywords*: asymmetric algorithms, encryption, decryption, cryptographic resistance, RSA, ElGamal*.

УДК 358.1 DOI: https://doi.org/10.33577/2312-4458.20.2019.28-32

Д.А. Новак, І.Д. Волков

Науково-дослідний центр ракетних військ і артилерії, м. Суми

МЕТОДИЧНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ЗАЛЕЖНОСТІ ВІДХИЛЕННЯ ПОЧАТКОВОЇ ШВИДКОСТІ СНАРЯДІВ ЧЕРЕЗ ПОДОВЖЕННЯ ЗАРЯДНОЇ КАМОРИ АРТИЛЕРІЙСЬКИХ ГАРМАТ, ВИМІРЯНЕ ЗА ДОПОМОГОЮ ПЗК

Моніторинг технічного стану артилерійського озброєння Збройних Сил України свідчить про достатній ступінь зносу каналів стволів для значної кількості артилерійських систем, що безпосередньо впливає на ефективність виконання вогневих завдань артилерією. У статті наведено порядок та особливості визначення відхилення початкових швидкостей снарядів через подовження зарядної камори артилерійських гармат з використанням таблиць внутрішньої балістики; надано інформацію про взаємозв'язок між основними параметрами внутрішньої балістики та їх впливом на значення початкової швидкості снарядів; визначено перелік вхідних даних, необхідних для визначення рівня падіння початкової швидкості снарядів для артилерійських систем з відомим рівнем зносу каналу ствола.

Ключові слова: *внутрішня балістика, артилерійська система, початкова швидкість снарядів, знос каналу ствола, подовження зарядної камори артилерійської гармати.*

Постановка проблеми

Відомо, що визначення ступеня зносу каналу стволів артилерійських гармат та його можливого впливу на ефективність виконання вогневих завдань артилерійськими підрозділами здійснюється під час виконання заходів балістичної підготовки шляхом визначення відхилення початкових швидкостей снарядів від їх табличних значень. Як правило, зазначені заходи балістичної підготовки здійснюються за допомогою артилерійської балістичної станції (АБС) або приладу заміру камори (ПЗК) з подальшим використанням спеціальних таблиць залежностей. На даний час у Збройних Силах (ЗС) України через недостатність забезпечення артилерійських підрозділів АБС визначення зміни початкової швидкості снарядів проводиться за допомогою ПЗК. У той же час не для всіх артилерійських систем, які знаходяться на озброєнні ЗС України, складено практичні рекомендації (таблиці залежності) з визначення відхилення початкової швидкості снарядів через подовження зарядної камори. До таких систем належать 152-мм гаубиці 2С19 та 2А65, гармати 2С5 та 2А36, а також 203-мм самохідні гармати 2С7. Враховуючи зазначене, питання визначення залежності відхилення початкової швидкості снарядів через подовження зарядної камори є актуальним і важливим завданням. В основі рішення подібних завдань покладено розв'язання системи диференційних рівнянь внутрішньої балістики. На даний час найбільш точним способом визначення відхилення початкових швидкостей снарядів через зміну того чи іншого параметра внутрішньої балістики вважається програмно-математичний спосіб, при якому усі розрахунки здійснюються із застосуванням електронно-обчислювальних машин [1]. Разом з тим, зазначений спосіб має суттєвий недолік – необхідність створення спеціального програмного забезпечення. Як альтернативний та більш доступний спосіб визначення відхилення початкових швидкостей снарядів через подовження зарядної камори артилерійських гармат пропонується методичний підхід із застосуванням таблиць внутрішньої балістики.

Аналіз останніх досліджень і публікацій

Результати аналізу бойового застосування артилерії в Антитерористичній операції на території Донецької і Луганської областей протягом 2014-2015 років свідчать, що частка участі артилерії у вогневому ураженні противника сягала майже 90%, а інтенсивність виконання вогневих завдань становила інколи до 15% на артилерійську батарею (липень-вересень 2014 року та січень-лютий 2015 року) [2]. Зазначене неминуче вплинуло на технічний стан артилерійських систем. Моніторинг технічного стану артилерійського озброєння ЗС України свідчить про достатній ступінь зносу каналів стволів для значної кількості артилерійських систем. Дані обставини мають безпосередній вплив на ефективність виконання вогневих завдань артилерією [3].

Формулювання мети статті

Метою статті є опис порядку та особливостей визначення відхилення початкової швидкості снарядів через подовження зарядної камори, виміряне за допомогою ПЗК табличним способом, який може бути застосований під час проведення попередніх балістичних розрахунків у ході розроблення та складання відповідних таблиць залежностей для 152-мм гаубиць 2С19 та 2А65, гармат 2С5 та 2А36, а також 203-мм самохідної гармати 2С7.

Виклад основного матеріалу

Знос каналу ствола артилерійської гармати під час стрільби є результатом комплексного механічного, теплового, газодинамічного та хімічного впливу снаряда і порохових газів на поверхневий шар металу, в результаті якого діаметр каналу ствола (особливо початкова ділянка його нарізної частини) збільшується, а значення початкової швидкості снаряда зменшується. Розрахунок зміни початкової швидкості снарядів у наслідок зносу каналу ствола артилерійської гармати вважається однією з основних задач внутрішньої балістики. Дана задача передбачає, що в умовах відомого рівня зносу каналу ствола потрібно знайти значення падіння максимального тиску порохових газів та, відповідно, падіння дульної (початкової) швидкості снаряда [1, 4, 5, 6]. Під дульною швидкістю снаряда ($V_д$) розуміють швидкість снаряда відносно ствола в момент проходження його дном дульного зрізу гармати. Дана швидкість є відносною та, як правило, на 1…2 % менша за початкову швидкість снаряда (V_0), але під час розв'язання задач внутрішньої балістики дані швидкості зазвичай ототожнюють [1, 4, 5, 6].

Аналіз системи рівнянь внутрішньої балістики вказує на те, що на значення дульної швидкості снаряда впливає сукупність параметрів внутрішньої балістики, якими є [1, 4, 5, 6]:

конструктивні параметри каналу ствола;

параметри умов заряджання;

енергетичні характеристики пострілу.

Враховуючи зазначене, дульну швидкість снаряда можна представити наступною залежністю:

$$V_д = f(d, s, q, f, a, \theta, \delta, J_K, k, \lambda, \mu, p_0, \chi, \omega, W_0, \varphi, l_д), \quad (1)$$

де d – калібр гармати;

s – площа поперечного перетину каналу ствола;

q – маса (вага) снаряда;

f – “сила” пороху (робота, яку міг би здійснити 1 кг порохових газів під час свого розширення в межах температури від T_1 до 0 °С при постійному значенні тиску);

a – коволюм порохових газів (об’єм молекул і твердих залишків пороху, які утворюються після згорання порохового заряду);

θ – показник адіабатичного процесу;

J_K – імпульс тиску порохових газів;

(k, λ, μ) – коефіцієнти геометричної форми зерна порохового заряду;

p_0 – тиск порохових газів (тиск форсування);

χ – коефіцієнт подовження зарядної камори;

ω – маса (вага) порохового заряду;

W_0 – початковий об’єм зарядної камори;

φ – коефіцієнт фіктивності (коефіцієнт врахування опору руху снаряда каналом ствола);

$l_д$ – повний шлях снаряда каналом ствола.

Зазначений перелік параметрів внутрішньої балістики впливає також і на значення максимального тиску порохових газів (тиск газів наприкінці згорання порохового заряду).

Для гармат з відомими характеристиками порохового заряду сукупність параметрів, що впливають, дещо зменшується та має наступний вигляд [1, 4, 5, 6]

$$V_д = f(s, q, p_0, \omega, W_0, \varphi, l_д). \qquad (2)$$

Задаючись певними значенням зносу каналу ствола можна знайти рівень падіння максимального тиску та відповідно падіння дульної швидкості снаряда артилерійської гармати.

Для визначення відхилення початкової швидкості снарядів (ΔV_0) через подовження зарядної камори із застосуванням запропонованого методичного підходу в якості вхідних даних використовуються наступні параметри внутрішньої балістики:

1. Калібр гармати (d).

2. Коефіцієнт врахування глибини нарізів (n_s).

3. Номінальна (формулярна) довжина зарядної камори (λ_0).

4. Об’єм зарядної камори (W_0).

5. Повний шлях снаряда каналом ствола ($l_д$).

6. Вага снаряда (q).

7. Максимальний тиск порохових газів (p_m).

8. Вага порохового заряду (ω).

Зазначені вихідні дані зазвичай вказуються в технічній, експлуатаційній та конструкторській документації на артилерійську систему (паспорти та формуляри, технічні описи та інструкції з експлуатації, таблиці стрільби тощо), а також у відповідній довідковій літературі.

У цілому запропонований методичний підхід до визначення зміни початкової швидкості снарядів через подовження зарядної камори артилерійських гармат, виміряне за допомогою ПЗК, матиме наступний вигляд (рис. 1):

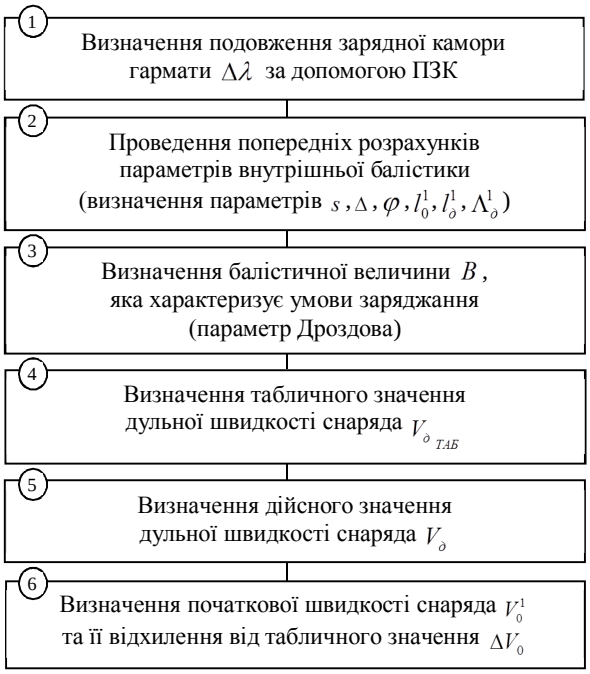

Рис. 1. **Структурна схема методичного підходу до визначення зміни початкової швидкості снарядів через подовження зарядної камори артилерійських гармат, виміряне за допомогою ПЗК**

Визначення відхилення початкової швидкості снарядів через подовження зарядної камори із застосуванням запропонованого методичного підходу здійснюється наступним чином:

1-й крок. Визначається подовження зарядної камори гармати.

Подовження зарядної камори ($\Delta\lambda$) вимірюється ПЗК та визначається як

$$\Delta\lambda = \lambda - \lambda_0, \qquad (3)$$

де λ – довжина зарядної камори (умовна), виміряна за допомогою ПЗК.

Умовна довжина зарядної камори (рис. 2) більша за дійсну ($l_{кам}$) на довжину від передньої кромки ведучого паска до дна снаряда (l^*) та визначається як

$$\lambda = l_{кам} + l^*. \qquad (4)$$

На рис. 2 також позначено:

l_0 – приведена довжина зарядної камори – довжина прямого циліндра, об’єм якого дорівнює об’єму (W_0), а площа основи – площі поперечного перетину каналу ствола (s);

$l_д$ – повний шлях снаряда каналом ствола – довжина від дна снаряда до дульного зрізу ствола (без врахування дульного гальма). Як правило, відома довжина нарізної частини канала ствола ($l_н$), тому значення повного шляху снаряда каналом ствола можна розрахувати як

$$l_д = l_н + l^*. \quad (5)$$

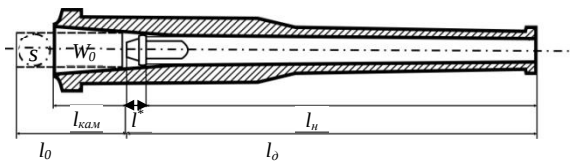

Рис. 2. **Схема каналу ствола артилерійської гармати з зарядною каморою**

2-й крок. Проводяться попередні розрахунки параметрів внутрішньої балістики.

Дані розрахунки зводяться до визначення окремих конструктивних параметрів артилерійської системи та параметрів умов її заряджання, а саме:

1. Визначається площа поперечного перетину канала ствола, як

$$s = n_S \times d^2. \quad (6)$$

Коефіцієнт врахування глибини нарізів ствола гармати (n_s) звичайно приймається [1, 5]: для стволів з глибиною нарізів у 1% калібру n_s = 0,8; для стволів з глибиною нарізів у 2% калібру n_s = 0,82; для ненарізних стволів n_s = 0,785.

2. Визначається щільність заряджання як

$$\Delta = \frac{\omega}{W_0}. \quad (7)$$

3. Визначається коефіцієнт фіктивності як

$$\varphi = K + \frac{\omega}{3q}, \quad (8)$$

де K – коефіцієнт Слухоцького.

4. Визначається відхилення приведеної довжини зарядної камори внаслідок її подовження як

$$l_0^1 = l_0 + \Delta\lambda = \frac{W_0}{s} + \Delta\lambda. \quad (9)$$

5. Визначається повний шлях снаряда каналом ствола з врахуванням його зносу як

$$l_д^1 = l_д - \Delta\lambda = (l_н + l^*) - \Delta\lambda. \quad (10)$$

6. Визначається відхилення відносного шляху снаряда каналом ствола внаслідок його зносу як

$$\Lambda_д^1 = \frac{l_д^1}{l_0^1}. \quad (11)$$

3-й крок. Визначається балістична величина, яка характеризує умови заряджання гармати (параметр Дроздова)

$$B = f(\Delta, p_m). \quad (12)$$

Параметр Дроздова (B) знаходиться шляхом інтерполяції за допомогою таблиць внутрішньої балістики [7] за відомим значенням максимального тиску порохових газів (p_m) та розрахованим значенням щільності заряджання (Δ).

4-й крок. Визначається відносне (табличне) значення дульної швидкості снаряда.

Табличне значення дульної швидкості ($V_{д\ ТАБ}$) знаходиться шляхом інтерполяції за допомогою таблиць внутрішньої балістики [8] за визначеним значенням параметра Дроздова (B) та розрахованим значенням відхилення відносного шляху снаряда каналом ствола внаслідок його зносу ($\Lambda_д^1$).

5-й крок. Визначається дійсне значення дульної швидкості снаряда.

Дійсне значення дульної швидкості снаряда ($V_д$) визначається як:

$$V_д = V_{д\ ТАБ}\sqrt{\frac{\omega}{\varphi q}}. \quad (13)$$

6-й крок. Визначається початкова швидкість снаряда та її відхилення від табличного значення внаслідок зносу каналу ствола.

Як зазначалося вище, дульна швидкість є відносною характеристикою, а її значення менше за значення початкової швидкості снаряда [1, 6], тобто

$$V_0^1 = (1{,}01...1{,}02)V_д. \quad (14)$$

Отримане значення початкової швидкості відповідає ступеню зносу канала ствола внаслідок подовження зарядної камори артилерійської гармати.

Рівень падіння початкової швидкості можна знайти як

$$\Delta V_0 = V_0 - V_0^1. \quad (15)$$

де V_0 – номінальне (табличне) значення початкової швидкості снаряда (початкова швидкість снаряда нової гармати).

Отримане значення у відсотках відповідатиме рівню відхилення початкової швидкості снаряда внаслідок подовження зарядної камори гармати.

Висновки

Запропонований методичний підхід розроблений з метою удосконалення заходів балістичної підготовки, які проводяться в артилерійських підрозділах, та вивчення можливості розроблення практичних рекомендацій (таблиць залежностей) з визначення зміни початкових швидкостей снарядів за допомогою ПЗК для артилерійських систем, у

таблицях стрільби яких відсутні залежності зміни початкової швидкості снарядів через подовження зарядної камори.

Запропонований методичний підхід з достатнім ступенем точності дає можливість здійснювати попередні балістичні розрахунки, і після підтвердження отриманих результатів дослідними стрільбами може бути застосований в якості альтернативного способу здійснення балістичних розрахунків у ході розроблення та складання таблиць залежностей для артилерійських систем, що перебувають на озброєнні артилерійських підрозділів ЗС України.

Список літератури

1. Захаренков В. Ф. Внутренняя баллистика и автоматизация проектирования артиллерийских орудий. – СПб.: БГТУ, 2010. – 276 с.

2. Методичний посібник щодо узагальнення досвіду застосування артилерії загальної та безпосередньої підтримки за досвідом участі в антитерористичній операції – К.: РВіА ЗСУ, 2016. – 62 с.

3. Теоретические основы управления огнем наземной артиллерии / А.И. Аверьянов, В.В. Каревый и др. – Л.: ВАА им. М.И. Калинина, 1978. – 454 с.

4. Баев И. В. Основы баллистического проектирования артиллерийских орудий. – Пенза.: ПВАИУ, 1975. – 69 с.

5. Основы устройства и конструирования орудий и боеприпасов наземной артиллерии. УК РВиА СВ. – М.: Воениздат, 1976. – 459 с.

6. Чурбанов Е.В. Внутренняя баллистика артиллерийского орудия. – М.: Воениздат, 1973. – 103 с.

7. Таблицы внутренней баллистики. Ч. I. Давления. Издание второе. ГАУ ВС СССР. – М.: Воениздат, 1968. – 347 с.

8. Таблицы внутренней баллистики. Ч. II. Скорости. Издание второе. ГАУ ВС СССР. – М.: Воениздат, 1968. – 335 с.

Рецензент: кандидат військових наук, професор П.Є. Трофименко, Сумський державний університет, Суми.

Методический подход к определению зависимости отклонения начальной скорости снарядов из-за удлинения зарядной каморы артиллерийских орудий, измеренного с помощью прибора измерения каморы

Д.А. Новак, И.Д. Волков

Мониторинг технического состояния артиллерийского вооружения Вооруженных Сил Украины свидетельствует о достаточной степени износа каналов стволов для значительного количества артиллерийских систем, что непосредственно влияет на эффективность выполнения огневых задач артиллерией. В статье приведен порядок и особенности определения отклонения начальных скоростей снарядов из-за удлинения зарядной каморы артиллерийских орудий с использованием таблиц внутренней баллистики; предоставлена информация о взаимосвязи между основными параметрами внутренней баллистики и их влиянием на значение начальной скорости снарядов; определен перечень исходных данных необходимых для определения уровня падения начальной скорости снарядов для артиллерийских систем с известным уровнем износа канала ствола.

Ключевые слова: *внутренняя баллистика, артиллерийская система, начальная скорость снарядов, износ канала ствола, удлинение зарядной каморы артиллерийского орудия.*

Methodical approach to determine the dependence of the deviation of the initial speed of the shells through the extension of the charging chamber artillery guns, measured with the help of the instrument for measuring the chambers

D. Novak, I. Volkov

The analysis results of the military use of artillery in the anti-terrorist operation in the east of the country indicate a significant amount of fire tasks, which relied on artillery and the high intensity of their implementation by artillery units, which negatively affected the technical condition of artillery systems. The monitoring of the technical state of the artillery armament of the Armed Forces of Ukraine indicates a sufficient degree of the trunk channels wearing out for a significant number of artillery systems, which directly affects the effectiveness of the fire tasks execution by artillery units.

Due to the lack of artillery units provided by artillery ballistic stations, the determination of the change in the initial speed of the shells is usually carried out with the help of gunmeters, and not all artillery systems have tables of dependence on deflection of the initial speed of the projectiles due to the extension of the charging chamber. Taking into account the above, the question of determining the dependence of the deviation of the initial speed of the projectiles due to the extension of the charging chamber is a vital and important task. As an accessible method of determining deflection parameters of initial velocities of shells through the extension of the artillery gun charging chamber, a methodological approach with the use of internal ballistics tables is proposed.

The basis of this approach is to take into account the effect of mechanical wearing out on the gun barrel channel to change the initial velocity of the projectile using known tabular dependencies. Input parameters of the methodical approach are: gauge caliber; coefficient of taking into account the depth of cuts; formular length of the charging chamber; volume of charging chamber; full path of the projectile by the trunk channel; the weight of the projectile; maximum pressure of powder gases; weight of powder charge.

The proposed methodological approach is designed to improve the ballistic training activities carried out in artillery units and to develop dependency tables to determine the change in the initial velocity of the shells with the help of a gun measuring instrument for artillery systems.

Keywords: *internal ballistics, artillery system, initial velocity of projectiles, barrel bore wear, lengthening of the artillery gun charging chamber.*