UDC 004.056: 519.766.23 DOI: 10.18372/2073-4751.78.18964

[1]**Pechurin M.K.**, Doctor of Engineering Sciences,
orcid.org/0000-0003-1727-7455,
e-mail: nkpech@i.ua,
[2]**Kondratova L.P.**, Candidate of Engineering Sciences,
orcid.org/0000-0002-9170-4198,
e-mail: ljupav@ukr.net,
[2]**Pechurin S.M.**, Candidate of Engineering Sciences,
orcid.org/0000-0002-4098-5727,
e-mail: serg11se@i.ua

ONE-DIRECTIONAL MAPPING FOR CRYPTOGRAPHIC SECURITY OF THE QUASI-REGULAR LANGUAGE SENTENCES TO INTERACT LIGHT AVIATION SYSTEMS SUBJECTS

[1]**National Aviation University**
[2]**National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"**

Introduction

The problem of creating effective methods and means of protection, in all interpretations of this term, of the interaction processes (communication) between aviation objects that functioning (perform targeting) in an autonomous mode, arose, apparently, since appearing the terms the "link" and "wing". Here, probably even before Alan Matheson Turing time, in searching the methods and means for the cryptographic protection of the subjects interaction of an autonomous mobile aircraft system was carried out under the understandable assumption that the latter (subjects) exchange sentences – messages of natural language (German – at the time of Enigma). Such assumption with a red thread stretched to the current moment, when interacting subjects – pilots – were replaced by automatons in unmanned aviation complexes (at this time, in particular, computer systems of artificial intelligence). At the same time, the classic universal methodology for building a (cryptographically) protected computer computing and telecommunications infrastructure of autonomous unmanned aerial vehicles system, where the processes of intermediate transformations of uplink messages are regulated by the parameters of the Reference Model of Open Systems Interaction (RMOSI), remained unchanged [1]. This "provokes" designers of computing and telecommunications infrastructure to demand software and hardware resources adequate to the existing RMOSI protocol implementation toolkit, which may not correspond to the technical capabilities of aircraft equipment, in particular, the capabilities of energy capacities [2].

It is natural to try to take into account resource parameters by (forced) limitation of functionality at individual RMOSI levels when designing systems for cryptographic protection of unmanned aircraft systems.

The current situation prompts us to pay special attention to methods of protecting communications in a relatively new and specific system of interacting entities, the system of unmanned aerial vehicles (UAVs) that operate in autonomous mode, performing predetermined targeting. As for piloted autonomous systems, we have, among all vulnerabilities, the potential possibility of unauthorized detection of the content (semantics) of messages (sentences) exchanged by subjects – elements of the autonomous UAV system.

The choice of methods and means of the interaction processes (communications) protection between subjects of the aviation autonomous system largely depends on the availability of the necessary information and computing resources, which in turn depend on the physical and technical parameters of the UAVs themselves as carriers (in the literal

sense) of the computer and telecommunication equipment.

Current domestic circumstances of the production and use of aviation equipment encourage us to limit ourselves (at least in this opus) to consideration of autonomous UAV systems of the light and ultralight classes. This class (the first according to the classification [3]) includes light, low-power aircraft with small values of such quantitative characteristics as maximum take-off weight, transmitter power, available height and range, energy consumption level, etc. As a result, we indirectly have significant limitations in available information, computing and telecommunication resources [4, 5]. The low speed of data transmission through the (wireless) environment, limited computing power and memory capacity, the need to use economical computing algorithms for encryption and decryption, with the unconditional implementation of RMOSI recommendations (protocols), can significantly reduce the security degree of such UAV systems, which prompts to search theopportunities improving their cryptographic security.

It should be kept in mind that there is a wide variety of approaches that can be applied in the aforementioned resource-constrained systems. This is, for example, the toolkit considered in the works [6-8]. In particular, in work [6], the method of cryptographically strict identification of remote users is based on the properties of irreversibility of cryptographic generators of pseudorandom sequences; this made it possible to integrate cryptographically strict identification of the user before the session, constant mutual authentication during the session, as well as to provide the possibility of stream encryption of data exchange between the user and the system within the framework of a single technological solution; the use of the proposed method allows to reduce identification time and increase protection against attacks on remote interaction between the system and the user through its capture. In [7], a zero-disclosure two-factor authentication cryptographic protocol over an extended field of elliptic curves using biometric data and a user's personal key is proposed to increase cryptographic stability and speed up the authentication process. In [8], a method for building symmetric NTRU-like cipher systems, which have reasonable resistance to attacks based on selected open messages, was developed.

In the article [9], it is proposed to use models of context-dependent languages and grammars to describe the translation processes of the data protocol module with the possibility of safe interaction of Class I UAVs (micro-, mini-, small).

The purpose of this article is to find a way to implement a special asymmetric system of cryptographic protection, for ultralight UAVs, by modifying the rules of a regular language production presented in works [10-12], where a method of converting data protocol units with a toolkit of regular grammars is proposed, which makes it possible to build algorithms of asymmetric encryption systems that do not require large computing resources.

About standard implementations of the cryptographic protection functions of EM OSI

The classic approach to the protection of wireless communications in the information and communication infrastructure of information networks is based on taking into account the requirements of the IEEE 802.11 – 802.16 standards and the corresponding protocols at all RMOSI levels. Here we have a wide selection of cryptographic protection methods and algorithms, both when using open (asymmetric) and private key systems.

For example, an "economical" implementation of the encryption function can be implemented using encryption algorithms from the WEP class, which are proven practice, effective enough, but not simple enough, from the point of view to apply in the conditions of the ultralight UAV system. Here, a stream encryption algorithm is used based on the organization of a key stream followed by merging with the upstream text stream. But such a simple method is dangerous because of the possibility of unauthorized determination of repetitions of the ascending text.

To prevent this, IEEE 802.11 – 802.16 offers simple but computationally intensive

measures, such as the use of modifications such as IV initialization vector or FM feedback [13, 14].

The statement of the problem

We have to modify, for the (cryptographic) protection of communication in an autonomous system of low-power UAVs, the regular grammar proposed in [2] for the purpose of obtaining a simple mechanism for applying its production rules, which will allow us to effectively implement encryption and decryption procedures in a special asymmetric encryption system, that is, to apply the relevant (resource limitations) unidirectional function (mapping).

Problem solving

It is proposed, in order to prevent the possibility of unauthorized determination of the ascending text, to use the "one-way function" of forming sentences of a modified regular ("quasi-regular") language using a grammar whose parameters are publicly available, that is, they play the role of a public key in the encryption system and in which: V_N is the set of non-terminals; V_T is the set of terminals; P is the set of the rules; σ is the initial non-terminal symbol.

We will consider the idea of modification using an example $|V_N| = |V_T| = 3$, де V_T = {w, c, r}, V_N = {W, C, R}, σ = W | C | R, P = {W → C, C → R, R → W, W → w, C → c, R → r}.

The role of a closed key is σ, which is equal to W or C or R, as well as the number k is the number of applications of production rules from P (in the simplest, degenerate case, k is a multiple of |VN|).

Well-known (open) parameters of grammar are, in particular, the set of the ways of parsing a sentence: canonical, top-down, etc. (fig. 1).

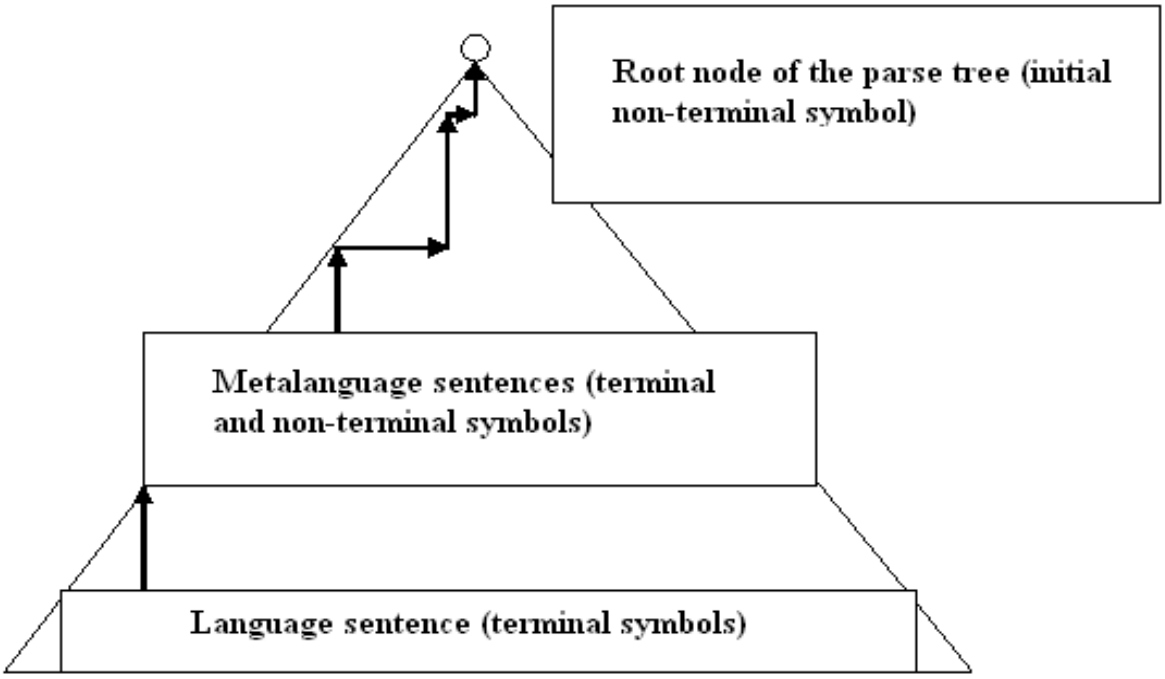


Fig. 1. One way of parsing a sentence in the conditions of regular grammar.

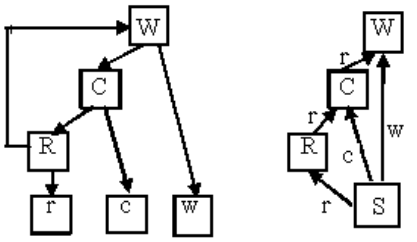
In our case, the regular grammar is extended by an additional set of production rules, which allows us to implement, say, such a variant of grammatical parsing that is no longer modeled by a tree (fig. 2).

The decryption of the message received by the subscriber (in our case – sentence r) is the essence of the reverse application of production rules according to the method of parsing determined by the public key. At the same time, k hops (applications) of rules from P are used.

If the result is a non-terminal, for example, C, which coincides with the secret one, then there is applied to it the rule of C → c (fig. 3).

W —[початковий символ
⇓ —[правило W → C
C
⇓ —[правило C → R
R
⇓ —[правило R → W
W
⇓ —[правило W → C
…
W
⇓ —[правило W → C
C
⇓ —[правило C → R
R
⇓ —[правило R → W
W
⇓
…
W —[початковий символ
⇓ —[правило W → C
C
⇓ —[правило C → R
R
⇓ —[правило R → r
r

Fig. 2. A variant of grammatical parsing of sentence r.



a) b)

Fig. 3. Scheme of grammatical parsing of the sentence r for the implementation of the encryption (a) and decryption (b) functions of the message.

The level of security of interaction depends to a large extent both on the values of the quantitative indicators (parameters) of the proposed modification (essentially moving towards the context-dependent class) of the grammar, and on the frequency of key changes (the detection of the corresponding ratio is outside the context of this article).

In other words, the difference from the procedure proposed in [9] is that a new protocol unit of data is introduced – "PDU of the 8th level", which is the sentence words of a special "quasi-regular" (not classical natural) language. At the same time, the generative grammar is similar to the one used for interlevel transformations according to RMOSI.

That is, we have a special asymmetric encryption system based on the use of a "quasi-regular" language relevant to the limited resources of ultralight aircraft systems.

Conclusions

1. The software and hardware infrastructure of ultralight aviation systems, in which the interaction of components is built on the basis of the ISO/IEC 7498-1 model and protocols, and the linguistic support (communication language) is based on the use of natural languages, is not balanced, at all levels of the Reference Model, according to the criterion "costs of information and telecommunication resources / level of protection against decryption" in the conditions of restrictions imposed on the physical parameters of such systems.

2. Assuming that the protection of the interacting components takes place taking into account the recommendations and protocols of ISO/IEC 7498-1, the balance of the hardware and software infrastructure can be achieved by modifying the parameters of the linguistic support with full preservation, in order to reduce the cost of manufacturing the software and hardware part of the ultralight aviation vehicles systems, standard protocols of interlevel interaction.

3. Adequate, in the conditions of limited information and telecommunication resources, the linguistic provision of communications in low-power ultralight unmanned aviation systems, in particular in autonomous UAV systems that implement classical navigation functions, should be considered to be based on the use of the proposed in the article language of subjects interaction (network components) , based on a quasi-regular grammar, which, in turn, generates a unidirectional mapping for use in a special asymmetric cryptographic system.

References

1. ISO/IEC 7498-1:1994(E). Information technology. Open System

Interconnection. Basic Reference Model: The Basic odel. Geneva : ISO/IEC, 1994. 62 p.

2. Pechurin N. K., Kondratova L. P., Pechurin S. N. Interaction language for ultralight UAVs. *XV International scientific and practical conference "Computer systems and network technologies" (CSNT-2024)* : proceedings, Kyiv, Ukraine, 25–26 April 2024 / National Aviation University. Kyiv, 2024. P. 122–123. URL: https://csnt.nau.edu.ua/files/ 2024/sbirnyk2024.

3. STANAG 3700 Ed: 8 /AJP-3.3 Ed. B. Allied Joint Doctrine for Air and Space Operations. Washington : NATO Standardization Office (NSO), 2016. 100 p.

4. Zhukov I. A. et al. The model balancing parallel processing of photo- videoframes in computing cluster for UAV. *Problems of informatization and management*. 2017. Vol. 4, no. 60. P. 26–29. DOI: 10.18372/2073-4751.4.12816.

5. Boyarinova Yu.Ye. et al. Models of the topologies for the weak-emitting telecommunication system of interacting UAVs. *Problems of informatization and management*. 2022. Iss. 4(72). P. 48–54. DOI: 10.18372/ 2073-4751.72.17461.

6. Rusanova O. V., Daiko I. V. Method for cryptographically strict identification of remote abonents based on pseudorandom sequences generators. *Problems of informatization and management*. 2023. Vol. 4, no. 76. P. 88–96. DOI: 10.18372/2073-4751.76.18244.

7. Strelkovskaya I. V., Onatskiy O. V., Yona L. G. Two-factor authentication protocol in access control systems. *Information and telecommunication sciences*. 2023. Vol. 14, no. 2. P. 17–25. DOI: https://doi.org/10.20535/2411-2976.22023. 17-25.

8. Matiyko A., Alekseychuk A Method for design secure symmetric NTRU-like encryption schemes. *Information Technology and Security*. 2022. Vol. 10, iss. 2(19). P. 165–176. DOI: 10.20535/2411-031. 2022.10.2.270406.

9. Pechurin M. K., Kondratova L. P., Pechurin S. M. IEEE 802.15.1 MAC-to-physical level transition protocol and one-directional parsing function. *Problems of informatization and management*. 2024. Iss. 1 (77). P. 89–95. DOI: 10.18372/2073-4751.77.18662.

10. Zhukov I. A. et al. Representation of the interaction between the levels of a computer network of DSSS and FHSS by a model of regular languages and grammars. *Electronic modeling*. 2014. Vol. 36, no. 2. P. 49–55.

11. Pechurin N. K., Kondratova L. P., Pechurin S. N. The modeling of the secure intra-layer interaction in wireless computer networks by the facilities of the formal grammars' and languages' theory. *Problems of informatization and management*. 2014. Vol. 4, no. 48. P. 82–87. DOI: 10.18372/2073-4751.4.8042.

12. Zhukov I. A. et al. One-directional parsing function for information security in computer networks of unmanned aerial vehicles. *Problems of informatization and management*. 2021. Vol. 4, no. 68. P. 17–21. DOI: 10.18372/2073-4751.68. 16521.

13. 802.15.1 IEEE Standard for Information Computer Society. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). New York : IEEE Computer Society, 2005. URL: http://standards.ieee.org/getieee802/downloadtechnology.

14. 802.11ax-2021 IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks. Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN. New York : IEEE, 2021. DOI: 10.1109/IEEESTD.2021.9442429.

Pechurin M.K., Kondratova L.P., Pechurin S.M.

ONE-DIRECTIONAL MAPPING FOR CRYPTOGRAPHIC SECURITY OF THE QUASI-REGULAR LANGUAGE SENTENCES TO INTERACT LIGHT AVIATION SYSTEMS SUBJECTS

One from the problems of the interaction processes (communications) protection between subjects of ultralight aviation systems that functioning (perform targeting) in an autonomous mode is considered – the problem of communications cryptographic protection in conditions when the interacting components information and communication capabilities are low An asymmetric cryptographic protection system based on the use of a modified regular language of communications is proposed, relevant to the low availability of information and computing resources.

***Keywords**: protection of autonomous systems; low-power aircraft; asymmetric system; unidirectional function; regular language.*

Печурін М.К., Кондратова Л.П., Печурін С.М.

ОДНОНАПРАВЛЕНЕ ВІДОБРАЖЕННЯ ДЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ РЕЧЕНЬ КВАЗІРЕГУЛЯРНОЇ МОВИ ВЗАЄМОДІЇ СУБ'ЄКТІВ НАДЛЕГКИХ АВІАЦІЙНИХ СИСТЕМ

Розглядається одна з проблем захисту процесів взаємодії (комунікацій) між суб'єктами надлегких авіаційних систем, що вони функціонують (виконують цілевказівку) в автономному режимі, – проблема криптографічного захисту комунікацій в умовах малої інформаційно-комунікаційних потужностей взаємодіючих компонентів. Пропонується релевантна (слабій доступності інформаційно-обчислювальних ресурсів), асиметрична криптографічна система захисту, основана на використанні модифікованої регулярної мови комунікацій.

***Ключові слова**: захист автономних систем; малопотужний літальний апарат; асиметрична система; однонаправлена функція; регулярна мова.*