DOI: 10.18372/2410-7840.24.16862
УДК 004.492

ПРОГРАМНИЙ ПРОДУКТ ДЛЯ ПОШУКУ ТА ВИЯВЛЕННЯ ПРОГРАМ ТИПУ SPYWARE

Олександр Ковальов, Олександр Чобаль, Василь Різак, Михайло Пригара

На сьогоднішній день наявність в системі якісного антивірусного програмного забезпечення не може у повній мірі гарантувати, що користувацька персональна інформація не потрапить до чужих рук. Не дивлячись на те, що методи пошуку та знешкодження потенційно небезпечних програмних кодів щодня поновлюються, існує категорія програм які операційна система не розцінює як загрозу, оскільки програми такого типу не завжди мають за мету пошкодити та/або знищити цінну для користувача інформацію. Мова йде про так зване шпигунське програмне забезпечення. Основною особливістю таких програм є те, що вони для збору інформації з системи використовують стандартні методи, якими користується ряд інших програм. Завдяки цьому вони можуть не лише збирати, обробляти та передавати зібрані дані третім особам, але і при цьому залишаються непомітними як для користувача так і для захисних програм. В даній роботі була розглянута проблематика програм типу spyware, особливості їх роботи та виявлення. Більш детально було описано підтип шпигунських програм – системний монітор. В середовищі програмування Microsoft Visual Studio, на мові C# був розроблений програмний продукт, завданням якого є сканування системи на предмет наявності в ній програм, які потенційно мають змогу збирати, обробляти та передавати користувацьку інформацію без відома останнього. Були описані методи та функції, якими оперує дана програма з метою пошуку в системі шпигунського програмного забезпечення.
Ключові слова: *Spyware, malware, програмний засіб, сканер, програмний шпигун, кейлогер, Windows.*

Вступ. Шпигунське програмне забезпечення (Spyware) – це шкідливе програмне забезпечення, яке непомітно відстежує поведінку користувачів, записує їх звички під час веб-серфінгу або викрадає їх конфіденційні дані (логіни, паролі тощо). Як правило, зібрана інформація відправляється назад розповсюджувачу шпигунських програм, де вона використовується для цільової реклами або в маркетингових дослідженнях. Це відрізняє їх від інших типів шкідливих програм, таких як віруси та хробаки, які зазвичай прагнуть поширитися на інші системи та завдати їм шкоди [9].

Оскільки проблема шпигунських програм загострилася, був введений ряд комерційних рішень, спрямованих на виявлення і видалення небажаних шпигунських програм. Ці інструменти схожі на антивірусні продукти в тому, що вони ідентифікують відомі екземпляри шпигунських програм, порівнюючи бінарне зображення невідомих зразків з базою даних відомих сигнатур [10].

Часто ці сигнатури генеруються вручну шляхом аналізу відомих зразків шпигунських програм (що є досить складним завданням, врахувати те що кожного дня доводиться аналізувати сотні нових випадків). На жаль, засоби виявлення шпигунських програм страждають від відомих недоліків детекторів які працюють на основі сигнатур, таких як постійна необхідність оновлення бази даних сигнатур і неможливість ідентифікувати раніше невідомі зразки. Зауважимо, що основним недоліком сигнатурних методів є те, що вони також часто не можуть впоратися із простими методами обфускації коду [11].

У загальному випадку шпигунське ПЗ відноситься до категорії шкідливих програм, які відстежують користувача без його згоди, як правило, в інтересах третьої сторони [1]. Існує декілька форм шпигунських програм, кожна з яких представляє унікальні загрози:

Adware – це рекламне програмне забезпечення, яке відображає спливаючу рекламу щоразу під час роботи програми. Часто програмне забезпечення доступне в Інтернеті безкоштовно, і реклама використовується в ньому для створення доходу для розробника. Однак в той же час рекламне ПЗ може встановлювати на користувацькі комп'ютери компоненти, що відстежують особисту інформацію (включаючи вік, стать, місце розташування, переваги при покупках або звички до серфінгу) в маркетингових цілях [5].

Рекламні файли cookie – це частини програмного забезпечення, які веб-сайти зберігають на жорсткому диску під час відвідування сайтів. Деякі

файли cookie існують тільки для того, щоб заощаджувати час, наприклад, в момент коли проставляється прапорець для веб-сайту щоб запам'ятати пароль на робочому комп'ютері. Однак деякі сайти також зберігають рекламні файли cookie, які містять в собі особисту інформацію (наприклад, звички до серфінгу, імена користувачів, паролі, а також області інтересів) і діляться цією інформацією з іншими веб-сайтами. Такий обмін інформацією дозволяє маркетинговим фірмам створювати профіль користувача на основі користувацької інформації і продавати цей профіль іншим фірмам [4].

Троянські коні – це шкідливі програми, які встановлюються під виглядом бажаних програм. Троянські коні призначені для крадіжки, шифрування або навіть знищення комп'ютерних даних. Деякі троянські коні, так звані Rats (Remote Administration Tools), надають зловмисникам необмежений доступ до комп'ютера щоразу, коли користувач знаходитесь в мережі. Зловмисник може виконувати такі дії як передача файлів, додавання або видалення документів і програм, а також управління клавіатурою та мишею [1, 2].

Системні монітори можуть фіксувати практично все що робить користувач під час роботи за комп'ютером – починаючи від натискання клавіш, електронної пошти та діалогу в чаті до того, які сайти користувач відвідує та які програми запускає. Системні монітори зазвичай працюють у фоновому режимі так, що користувач навіть не здогадується що за ним спостерігають. Інформація, зібрана системним монітором, зберігається в системі в зашифрованому файлі журналу для подальшого вилучення. Деякі програми також можуть надсилати файли журналу електронною поштою [6, 7].

Розробка програмного засобу для протидії spyware

В ході дослідження програм типу програмний шпигун, а саме підтипу системні монітори вдалося не лише ознайомитись із їх основними функціональними можливостями та принципом їх роботи, але також і виявити їх слабкі місця. Ось деякі з них:

- Під час вивчення роботи функції кейлогера програма «позичає» певний відсоток ресурсів центрального процесора. При повсякденному використанні комп'ютера даний процес є непомітним навіть для досвідченого користувача, однак, у випадку якщо кількість фактичних натисків клавіш буде занадто великою на одиницю часу – програмі доведеться запозичити більше ресурсів системи, аби мати змогу обробити кожну натиснуту клавішу. В результаті цього, програма буде значно виділятись на фоні інших робочих процесів за показником використання CPU (Central Processing Unit).
- Вдалось встановити, що при активній роботі програми із зображеннями або великою кількістю зібраної інформації - розмір споживаної оперативної пам'яті, яка виділяється під роботу програми, може різко змінюватись.
- Під час збору інформації, для того аби залишатись непомітною, програма змушена зберігати зібрані дані в системі. Скануючи файлову систему на наявність нових файлів або файлів які постійно змінюються, цілком ймовірно відстежити файл, який використовується програмним шпигуном в якості тимчасового сховища даних [1].

Завдяки отриманій інформації був розроблений програмний засіб, завданням якого є виявлення в системі програм, які потенційно можуть збирати користувацьку інформацію з подальшою її обробкою та передачею. Програма створюється на мові C#, середою розробки виступатиме середовище Microsoft Visual Studio. Функціонал програми було умовно розділено на 4 основні складові, кожна з яких виконує свою окрему функцію.

Scanner

Під час першого запуску користувачеві представлена робоча область під назвою «Scanner». Функціонал що запропонований в даній секції спрямований на виявлення та представлення у зручній формі списку всіх активних процесів.

Для зручності користувачеві представлена робота з такою інформацією як назва програмного процесу (Process Name), час першого запуску програми (Start time), показник поточного та пікового використання оперативною пам'яттю (Memory Usage та Peak memory usage відповідно). При бажанні, користувач здатен відмічати для себе процеси, які, на його думку, є підозрілими, проставляннням прапорця поруч із обраним процесом. Розглянемо більш детально запропоновану програмою інформацію.

Стовбець «Start time» відображає час, коли відбувся перший запуск програми. Даний показник є цінним, оскільки, як відомо, у більшості випадків програмний шпигун активізується одразу після запуску системи. Таким чином користувач отримує змогу переглянути всі програмні проце-

си, які були запущені одразу після запуску системи.

Під час роботи із фотоматеріалами (наприклад при взятті знімків з екрану монітору) та/або роботи із великою кількістю інформації (при її обробці) програми spyware здатні споживати більшу кількість оперативної пам'яті у порівнянні із її споживанням у період простою. Не зважаючи на те що подібні піки важко візуально помітити, у розробленому ПЗ ведеться логуваня даної інформації. Так, у стовпці «Memory Usage» відображається поточний розмір споживаної процесом пам'яті, а у стовпці «Peak memory usage» відзначається його піковий показник за увесь період роботи системи [12].

Окрім цього, під час першого запуску програми відбувається перевірка для кожного окремого процесу наявності цифрового підпису. Це робиться з метою виявлення в системі процесу, який міг би видавати себе за інший програмний процес використовуючи його ім'я.

Процеси, до яких все ж не вдалось отримати доступ відображаються жовтим кольором. Програми, що містять в собі цифровий підпис відображаються зеленим кольором, решта – червоним.

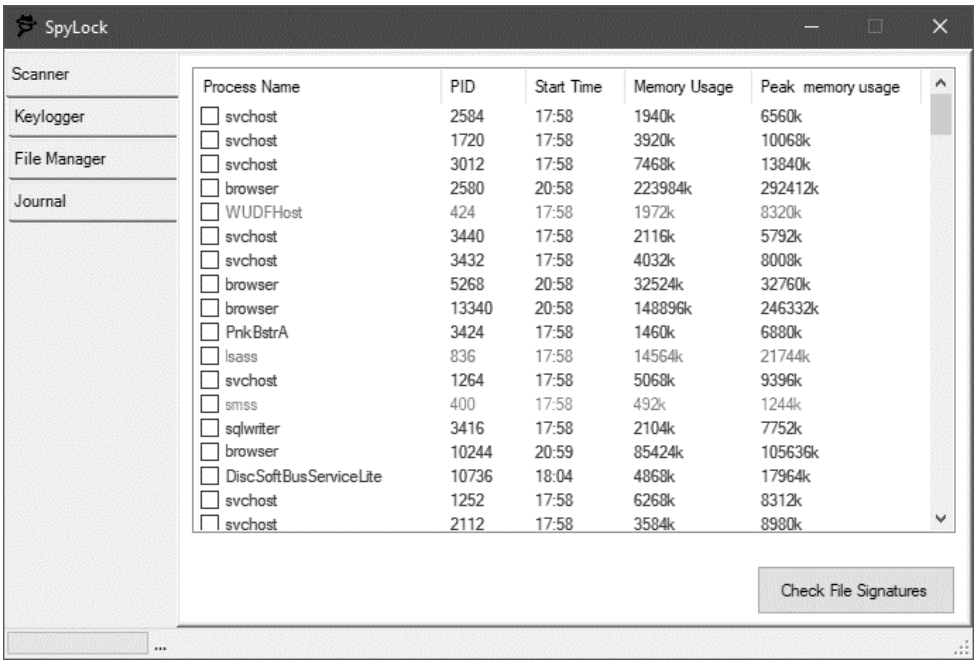

Рис. 1. Головне вікно програми

Користувачеві пропонується відзначити із представленої таблиці ті процеси, які, на його погляд, є підозрілими, для подальшої роботи з ними.

Keylogger

Наступною робочою областю програми є вікно «Keylogger». Однією із найрозповсюдженіших функцій що притаманна майже всім spyware програмам є так звана функція зчитування користувацького вводу з клавіатури (та інколи миші) з метою отримання бажаної інформації (логінів, паролів тощо) – keylogger [12].

Для протидії зчитуванню інформації з клавіатури був розроблений окремий функціонал, завданням якого є виявити програмні процеси, які так чи інакше реагують на користувацький ввід з клавіатури.

Принцип роботи даного функціоналу полягає в наступному: перш за все створюється окрема таблиця що містить в собі усі активні в системі процеси, з урахуванням їх поточної активності за показником використання ресурсів центрального процесора. Після цього на протязі однієї секунди розроблена програма імітує користувацький ввід шляхом програмного натискання на довільні клавіші. Для того аби даний ввід не зашкодив роботі із системою або іншими програмами - імітація проводиться саме для вікна даної програми. По закінченню однієї секунди програма проводить повторне сканування активності всіх процесів та записує зміни в показниках використання ресурсів CPU. У випадку якщо за період останнього сканування спостерігався зріст активності певного

процесу – програма додає до показника активності даної окремої програми значення в 0.1 одиницю. Повторивши дану процедуру ще 9 разів на екрані користувача відображається поточна таблиця з усіма процесами та їх активністю за останні 10 секунд. Програмні процеси, активність яких була найбільшою, можна вважати підозрілими. Однак це не може гарантувати що вони проявляли активність саме внаслідок натискання клавіш. Їх підвищена активність також може бути зумовлена різними факторами, наприклад, активною роботою програми у фоновому режимі або оновленням програми.

Тому навіть при наявності програм з високою активності слід у ручному режимі опрацювати отримані результати.

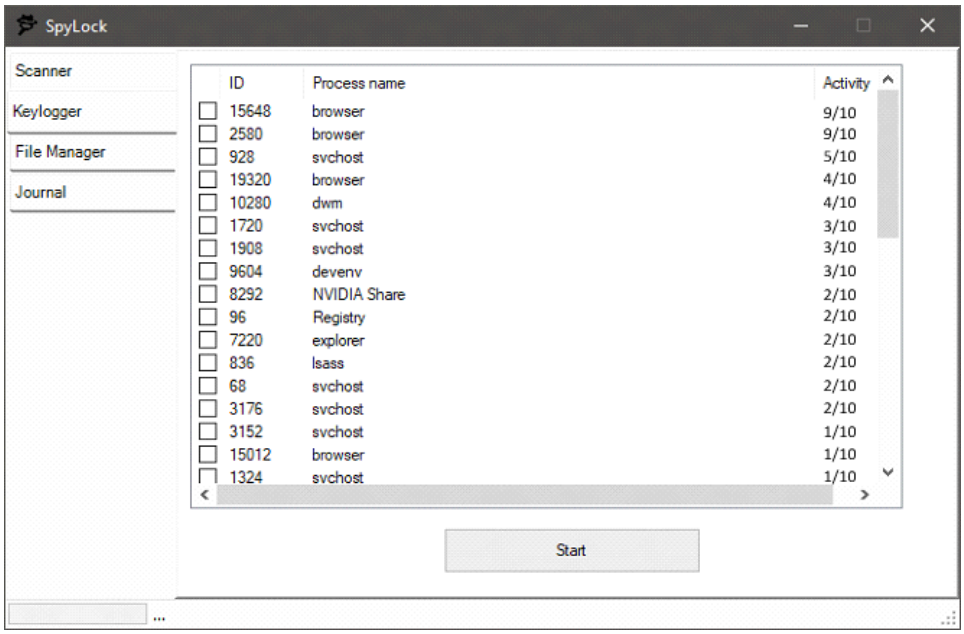

Рис.2. Вікно keylogger

File Manager

Під час своєї роботи, програмний продукт типу spyware здатний зберігати зібрані дані у окремих файлах. Це можуть бути як текстова інформація, так і зображення. За допомогою секції «File Manager» досвідчений користувач має змогу переглянути всі документи, які так чи інакше були створені в системі за виділений проміжок часу.

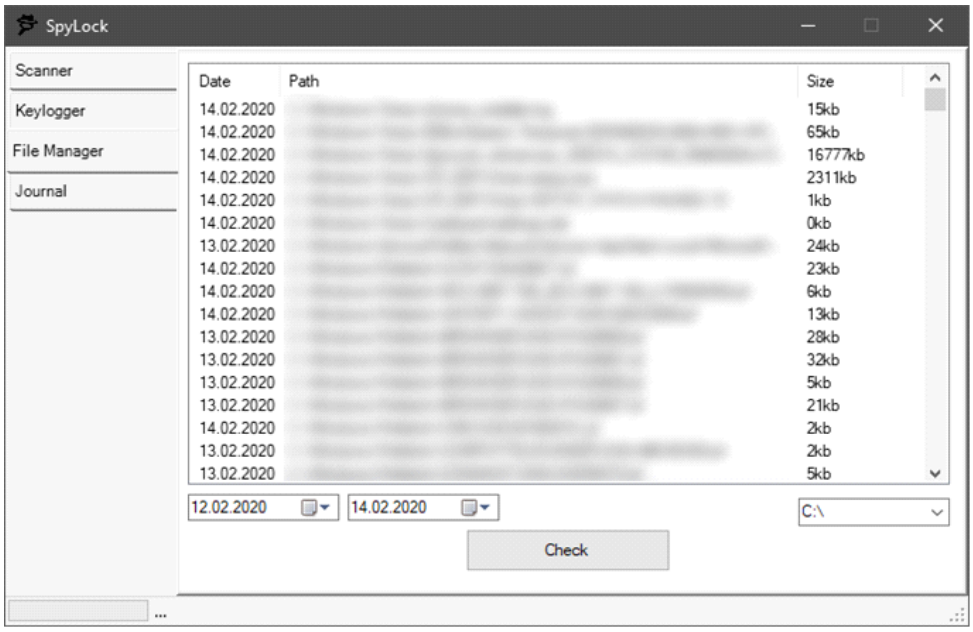

Рис. 3. Вікно File Manager

Journal

У секції «Journal» розробленого ПЗ користувачеві представлено список із усіх програмних процесів, які були відмічені як «підозрілі».

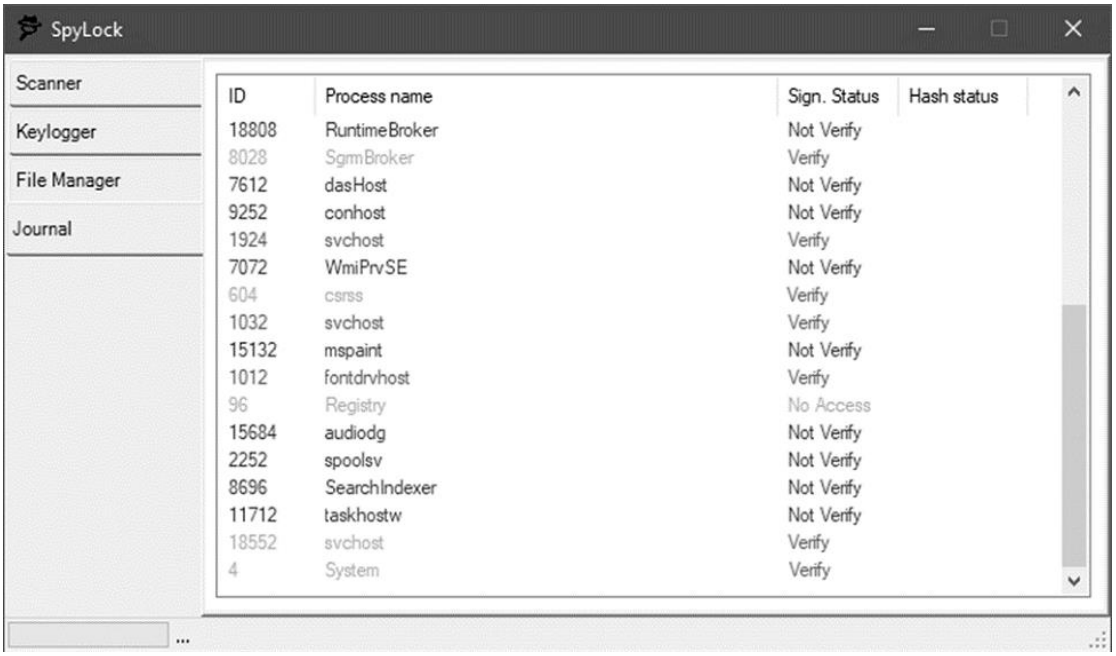

Рис. 4. Вікно Journal

На даній таблиці користувачеві надається можливість повторно провести аналіз отриманих результатів на предмет виявлення серед зазначених програмних процесів ті, які в результаті поведінкового аналізу відповідають поведінці програм типу spyware.

Висновки. В даній роботі було розглянуто проблему програмних шпигунів та основні небезпеки програм даного типу. Наведено класифікацію spyware та базові особливості системних моніторів. Був розроблений на мові програмування C# програмний засіб, основним завданням якого є пошук в системі підозрілих програм, які можуть зберігати в собі функціонал для зчитування користувацької інформації з подальшою її обробкою. В програмному засобі були реалізовані наступні функції: сканування наявних в системі процесів на предмет наявності в них цифрового підпису, перевірка та моніторинг показників споживання окремими програмами ресурсів CPU та оперативної пам'яті, розроблено механізм для пошуку програм які реагують на користувацький ввід з клавіатури, пошук створених в системі тимчасових файлових сховищ а також ведення журналу пошуку.

ЛІТЕРАТУРА

[1] Ковальов О.О., Чобаль О.І., Різак В.М. Програмний продукт типу spyware та аналіз його стійкості до виявлення засобами захисту // Захист інформації. Том 22, №3. 2020.

[2] Prateek Nigam "Malware Detection and Signature Generation" International Journal of Engineering Trends and Applications (IJETA) – Volume 7 Issue 5, Sep-Oct 2020.

[3] Yan, Y. Qi and Q. Rao, "Detecting malware with an ensemble method based on deep neural network", Secur. Commun. Netw., vol. 2018, Mar. 2018.

[4] Efraim TurbanJon OutlandDavid KingJae Kyu LeeTing-Peng LiangDeborrah C. Turban "Marketing and Advertising in E-Commerce" 13 October 2017.

[5] Anthony Ekanem "Adware and Spyware: How to Remove and Protect Your Computer against Adware and Spyware Paperback" March 17, 2016 70 pages.

[6] P. Wang and Y.-S. Wang, "Malware behavioural detection and vaccine development by using a support vector model classifier", J. Comput. Syst. Sci., vol. 81, no. 6, 2015.

[7] R. Islam, R. Tian, L. M. Batten and S. Versteeg, "Classification of malware based on integrated static and dynamic features", J. Netw. Comput. Appl., vol. 36, no. 2, 2013.

[8] Ladakis E., Koromilas L., Vasiliadis G., Polychronakis M., Ioannidis S. "You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger." In Proceedings of the 6th European Workshop on System Security. EuroSec, Prague,

Czech Republic, April 2013.
[9] Steven D. Gribble Alexander Moshchuk, Tanya Bragin and Henry M. Levy. A CrawlerBased Study of Spyware on the Web. In Proceedings of the Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2006.
[10] Saroiu, S., Gribble, S., Levy, H. Measurement and Analysis of Spyware in a University Environment. In Usenix NSDI (2004).
[11] Christodorescu, M., Jha, S. Testing Malware Detectors. In ACM International Symposium on Software Testing and Analysis (ISSTA) (2004).
[12] https://docs.microsoft.com.

SOFTWARE PRODUCT FOR SEARCHING AND DETECTING SPYWARE-TYPE PROGRAMS

To date, the availability of high-quality antivirus software in the system cannot fully guarantee that the user's personal information will not fall into the wrong hands. Despite the fact that the methods of searching for and clearing potentially dangerous software codes are updated daily, there is a category of programs that the operating system does not regard as a threat, since programs of this type do not always aim to damage and/or destroy information that is valuable to the user. We are talking about so-called spyware. The main feature of such programs is that they use standard methods used by a number of other programs to collect information from the system. This means that they can not only collect, process and transmit the collected data to third parties, but also remain invisible to both the user and the security software. In this paper, we considered the problems of spyware-type programs, the features of their operation and detection. The system monitor subtype of spyware was described in more detail. In the Microsoft Visual Studio C # programming environment, a software product was developed to scan the system for programs that could potentially collect, process, and transmit user information without the latter's knowledge. The methods and functions that this program uses to search for spyware in the system were described.
Keywords: Spyware, malware, software, scanner, keylogger, Windows.

Ковальов Олександр Олександрович, аспірант кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
Kovalev Alexander, PhD student, Department of Solid State Electronics and Information Security of the Physics Faculty, UzhNU.
E-mail: alexandr.kovalev@uzhnu.edu.ua.
ORCID: 0000-0003-0630-9132.

Чобаль Олександр Ілліч, кандидат фізико-математичних наук, доцент кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
Chobal Oleksandr, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Solid State Electronics and Information Security of the Physical Faculty, UzhNU.
E-mail: oleksandr.chobal@uzhnu.edu.ua.
ORCID: 0000-0002-8042-8052.

Різак Василь Михайлович, доктор фізико-математичних наук, професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.
Rizak Vasyl, Doctor of Physical and Mathematical Sciences, Professor, Head of the Department of Solid State Electronics and Information Security of the Physical Faculty, UzhNU.
E-mail: vrizak@uzhnu.edu.ua.
ORCID: 0000-0002-9177-0662.

Пригара Михайло Петрович, кандидат технічних наук, доцент кафедри технології машинобудування інженерно технічного факультету УжНУ.
Prygara Mykhailo, Candidate of Technical Sciences, Associate Professor of the Department of Machine Industry Technology of the Engineering Faculty, UzhNU.
E-mail: **mykhailo.prygara@uzhnu.edu.ua.**
ORCID: 0000-0002-0954-4480.