AKTUELNOSTI 36
2016

ACTUALITIES
Journal of Social Issues
First launched in 1996
The Journal has a scientific orientation

ISSN 0354-9852

By the Decision of the Ministry of Information of the Republika Srpska, No. 01-492 / of 12.23.1996., Journal »Actualities« Banja Luka, has been inscribed into the Register of Public Editionsunder the number 183
Journal »Actualities« is on the list of categorized national scientific journals in accordance with the Regulations on Publication of Scientific Papers (Official Gazzete of the RS No. 77/10), with the Ministry of Science and Technology of the Government of the Republika Srpska.

AKTUELNOSTI
Časopis Banja Luka College-a
Prvi put pokrenut 1996.g.
Časopis ima naučnu orijentaciju

ISSN 0354-9852

Rješenjem Ministarstva informacija Republike Srpske, broj 01-492/ od 23.12.1996. g. časopis »Aktuelnosti« Banja Luka, upisan je u Registar javnih glasila pod brojem 183.
Časopis »Aktuelnosti« nalazi se na rang-listi kategorisanih nacionalnih naučnih časopisa u skladu sa Pravilnikom o publikovanju naučnih publikacija (Službeni glasnik RS br. 77/10) kod Ministarstva nauke i tehnologije Vlade Republike Srpske.

Banja Luka College Journal

ACTUALITIES

number 36

BLC
Banja Luka College
Banja Luka, 2016.

Časopis Banja Luka College-a

AKTUELNOSTI

broj 36

BLC
Banja Luka College
Banja Luka, 2016.

CONTENTS

SADRŽAJ

ISSN 0354-9852
Originalni naučni rad
Original scientific paper

UDK 519.857:004.021
DOI 10.7251/AKT1636001D
COBISS.RS-ID 6277656

ALGORITHM AES – STRUCTURE, TRANSFORMATIONS AND PERFORMANCE

Boris Damjanović[1]

Abstract

Today's cryptographic algorithms are designed in a way that they combine mathematical theory and practice of computer science in order to improve resistance to cryptanalysis. Cryptographic algorithms are designed around the binary data format keeping in mind the presumption of hardening possibility of cracking the algorithm. One of the algorithms whose resistance to cryptanalysis during the past 16 years is extensively tested algorithm AES. The Advanced Encryption Standard (AES) is the first cryptographic standard aroused as the result of public competition established by U.S. National Institute of Standards and Technology (NIST). AES has emerged as restriction on winner of this competition, called Rijndael algorithm on the block size of 128 bits. From the moment of its acceptance of the standard in 2001, testing and research of its resistance on cryptanalysis and research focused on improving its performance are made. This paper presents a detailed overview of the algorithm AES, together with all its transformations and with ideas to speed up its work.

Keywords: *Cryptogaphy, Algorithm AES, performance*
JEL classificaiton:C00

INTRODUCTION

Today's cryptographic algorithms are designed in a way that they combine complex mathematical procedures and the theory and practice of computer science in order to improve resistance to cryptanalysis. As stated in [1] AES (Advanced Encryption Standard) algorithm is a complex cipher whose resistance to cryptanalysis has been extensively tested over the last 15 years. This algorithm has become the de facto global standard for commercial and open source software and hardware. In addition to the U.S. administration, a number of institutions and individuals around the world use this algorithm. Advanced Encryption Standard (AES) is the first cryptographic standard aroused as a result of public competition that was esta-

1 Boris Damjanović Ph.D., Banja Luka College, Banja Luka; boris.damanovic@blc.edu.ba

blished by U.S. National Institute of Standards and Technology. Standard can theoretically be divided into three cryptographic algorithms: AES-128, AES-192 and AES-256.

In January 1997, the US National Institute of Standards and Technology (NIST) announced the start of an initiative to develop a new encryption standard: the AES . The new encryption standard was to become a Federal Information Processing Standard (FIPS), replacing the old Data Encryption Standard (DES) and triple-DES. Unlike the selection of prior cryptographic algorithms, NIST had announced that the AES selection process would be open. Anyone could submit a candidate cipher. Each submission, provided it met the requirements, would be considered on its merits. NIST would not perform any security or efficiency evaluation itself, but instead invited the cryptology community to mount attacks and try to crypt analyse the different candidates, and anyone who was interested to evaluate implementation cost. All results could be sent to NIST as public comments for publication on the NIST AES web site or be submitted for presentation at AES conferences. NIST would merely collect contributions using them to base their selection. NIST would motivate their choices in evaluation reports [2].

NIST has prescribed the following rules [3]:

- AES shall be publicly defined.
- AES shall be a symmetric block cipher.
- AES shall be designed so that its key length may be increased as needed.
- AES shall be implementable in both hardware and software.
- AES shall either be
  - freely available, or
  - available under terms consistent with the ANSI Patent Policy.
- Algorithms which meet the above requirements will be judged based on the following factors:
  - security (resistance to cryptanalysis),
  - computational efficiency,
  - memory requirements,
  - hardware and software suitability,
  - simplicity,
  - flexibility, and
  - licensing requirements

The required effort to produce a 'complete and proper' submission package would already filter out several of the proposals. The 15 submissions that were completed in time and accepted were: CAST-256, Crypton, DEAL, DFC, E2, Frog, HPC, LOKI97, Magenta, Mars, RC6, Rijndael, SAFER+, Serpent and Twofish [1, 2, 4, 5, 6].

After the series of workshops (Ventura-California, august 1998., Rome, march 1999.) and researchs conducted and papers published, there was a relatively calm period that ended with the announcement of the five candidates by NIST in August 1999. The finalists were: MARS, RC6, Rijndael, Serpent and Twofish [1, 2, 4, 5, 6].

Next round of testing was held in April 2000 in New York at a conference that was dedicated to this algorithm. The conference was combined with the results of the next workshop titled Fast Software Encryption Workshop, which was also held in New York [1, 2].

On 2 October, 2000, NIST officially announced that Rijndael would become Advanced Encryption Standard [1, 2].

AES algorithm, as defined by FIPS-197 document [7] cites a data block must be always 128 bit-long, while the key sizes could be 128, 192 or 256 bits. On the other hand, Rijndael (from which AES evolved) allows for both key and block sizes to be chosen from the set of {128, 160, 192, 224, 256} bits. The very fact that AES is really just a subset of Rijndael emphasize its large flexibility.

As mentioned, AES algorithm described in FIPS-197 document [7, 8, 9] transforms 128 bit block of data during 10, 12 or 14 rounds using the initial key lengths of 128, 192 and 256 bit. The initial key is then enlarged to (10+1)*16, (12+1)*16 or (14+1)*16 bytes in the key expansion routine. Each round repeats the SubBytes(), MixColumns(), ShiftRows() and AddRoundKey() transformations. AES authors redefine both addition operation within the $GF(2^8)$, which is then conducted by XOR operation at the byte level and multiplication operation which is thus conducted as polynomial multiplication with the conditional modulo polynomial 0x11B. The mentioned multiplication is the most time consuming in the aspect of optimization, because it is intensively used during the MixColumns() transformation.

Inverse cipher transforms 128 bit block of ciphertext during 10, 12 or 14 rounds using the same keys as cipher. Each round repeats the InvSubBytes(), InvMixColumns(), InvShiftRows() and AddRoundKey() transformations.

In the following text, the theoretical assumptions and basic transformation of this algorithm will be displayed.

MATHEMATICAL PRELIMINARIES

The field GF(28)

Every byte of data in the AES algorithm is treated as a series of bits which are elements of a finite field. A byte b, consisting of bits b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0, is considered as a polynomial with coefficient in {0,1} [10]:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{i=0}^{7} b_i x^i \quad (1)$$

For example, {01100011} identifies the specific finite field element [7]

$$x_6 + x_5 + x + 1 \quad (2)$$

Addition

Authors of the AES algorithm redefine the addition operation. The addition [7] of two elements in a finite field is achieved by "adding" the coefficients for the corresponding powers in the polynomials for the two elements. The addition is performed with the XOR operation (denoted by $\oplus$) - i.e., modulo 2 - so that

$1 \oplus 1 = 0$, $1 \oplus 0 = 1$, and $0 \oplus 0 = 0$.

For example:

$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$, as polynomial:
{01010111} $\oplus$ {10000011} = {11010100} , binary (3)
{57} $\oplus$ {83} = {d4} , hexadecimal.

Consequently, subtraction of polynomials is identical to addition of polynomials.

Multiplication

In the polynomial representation, multiplication in GF(2^8) (denoted by $\bullet$) corresponds with the multiplication of polynomials modulo an irreducible polynomial of degree 8. A polynomial is irreducible if its only divisors are one and itself. For the AES algorithm, this irreducible polynomial is

$$m(x) = x^8 + x^4 + x^3 + x + 1 \quad (4)$$

or in hexadecimal representation.:

{01}{1b} (5)

For example:

57h $\bullet$ 83h

{57} $\bullet$ {83} = {c1}
1010111 $\bullet$ 10000011 = 11000001
$(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) = x^{13} + x^{11} + x^9 + x^8 + x^7 +$
$x^7 + x^5 + x^3 + x^2 + x +$
$x^6 + x^4 + x^2 + x + 1$
$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$ (6)

Finally:

$$(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + 1 \quad (7)$$

Dividing with this polynomial ensures that the result will always be a binary polynomial of degree less than 8 so that it can be represented by a single byte.

Multiplication by x

As stated in [1, 7], if we have to multiply the following polynomial:

$$b(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 \quad (8)$$

With polynomial x, we get the result:

$$b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x^1 \quad (9)$$

The result of multiplication of the x*b(x) is then reduced to the degree 8 by applying the modulo operation with irreducible polynomial m(x). If b7 = 0, the polynomial is already in the reduced form. If b7 = 1, the reduction is carried out by subtracting (using an XOR operation) the polynomial m (x) [1].

At the bit level, multiplication by x ({00000010} or {02}) can be done by using the left Shift after which the (conditional) follows with xor {00011011} or {1b}.

For example, to multiply {57} • {13} = {fe}, we wil use [1]:

$$\begin{array}{ll} \{57\} \bullet \{01\} = \{57\} & 1 \\ \{57\} \bullet \{02\} = \text{xtime}(\{57\}) = \{ae\} & 1 \\ \{57\} \bullet \{04\} = \text{xtime}(\{ae\}) = \{47\} & 0 \\ \{57\} \bullet \{08\} = \text{xtime}(\{47\}) = \{8e\} & 0 \\ \{57\} \bullet \{10\} = \text{xtime}(\{8e\}) = \{07\} & 1 \end{array} \quad (10)$$

Bearing in mind that the {13h} is equal to {10011b}, if we need to multiply {57} • {13} = {fe}, we will use:

$$\begin{aligned} &\{57\} \bullet \{13\} = \{57\} \bullet (\{01\} \oplus \{02\} \oplus \{10\}) \\ &= \{57\} \oplus \{ae\} \oplus \{07\} \\ &= \{fe\} \end{aligned} \quad (11)$$

Alternativelly, description of AES multiplicatio is given in [11], where is stated that the finite field element {00000010} is the polynomial x, which means that multiplying another element by this value increases all it's powers of x by 1. This is equivalent to shifting its byte representation up by one bit so that the bit at position i moves to postion i+1. If the top bit is set prior to this move it will overflow to create an x^8 term, in which case the modular polynomial is added to cancel this additional bit to leave a result that fits within a byte. When {11001000} is multiplied by x, {00000010}, the initial

result is 1{10010000}. The 'overflow' bit is then removed by adding the modular polynomial, 1{00011011}, using an exclusive-or operation to give the final result as {10001011}.

Polynomials with coefficients in gf(28)

Four term polynomials can be defined with coefficients that are finite field elements as [7, 11]:

$$a(x) = a_3x^3 + a_2x^2 + a_1x^1 + a_0 \quad (12)$$

where the four coefficients will be denoted as a word in the form [a0 , a1 , a2 , a3] (note that the index increases from left to right in this notation) [11]. With a second polynomial:

$$b(x) = b_3x^3 + b_2x^2 + b_1x^1 + b_0 \quad (13)$$

define a second four-term polynomial.

Multiplication is achieved in two steps. In the first step, the polynomial product $c(x) = a(x) \bullet b(x)$ is algebraically expanded, and like powers are collected to give

$$c(x) = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x^1 + c_0 \quad (14)$$

where

$$\begin{aligned}
c_0 &= (a_0 \bullet b_0),\\
c_1 &= (a_0 \bullet b_1) \oplus (a_1 \bullet b_0),\\
c_2 &= (a_0 \bullet b_2) \oplus (a_1 \bullet b_1) \oplus (a_2 \bullet b_0),\\
c_3 &= (a_0 \bullet b_3) \oplus (a_1 \bullet b_2) \oplus (a_2 \bullet b_1) \oplus (a_3 \bullet b_0),\\
c_4 &= (a_1 \bullet b_3) \oplus (a_2 \bullet b_2) \oplus (a_3 \bullet b_1),\\
c_5 &= (a_2 \bullet b_3) \oplus (a_3 \bullet b_2),\\
c_6 &= (a_3 \bullet b_3).
\end{aligned} \quad (15)$$

The result, c(x), does not represent a four-byte word. Therefore, the second step of the multiplication is to reduce c(x) modulo a polynomial of degree 4; the result can be reduced to a polynomial of degree less than 4. For the AES algorithm [1, 11], this is accomplished with the polynomial

$$x^4 + 1 \quad (16)$$

so that:

$$x^i \bmod (x^4 + 1) = x^{i \bmod 4} \quad (17)$$

The modular product of a(x) and b(x), denoted by $a(x) \otimes b(x)$, is given by the four-term polynomial d(x), defined as follows [1, 11]:

$$d(x) = d_3x^3 + d_2x^2 + d_1x^1 + d_0 \quad (18)$$

where

$$
\begin{aligned}
&d(x) = c(x) \bmod (x^4+1) = (c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x^1 + c_0) \bmod (x^4+1) = \\
&c_6x^{6 \bmod 4} + c_5x^{5 \bmod 4} + c_4x^{4 \bmod 4} + c_3x^{3 \bmod 4} + c_2x^{2 \bmod 4} + c_1x^{1 \bmod 4} + c_0x^{0 \bmod 4} = \\
&c_6x^2 + c_5x^1 + c_4x^0 + c_3x^3 + c_2x^2 + c_1x^1 + c_0x^0 = \\
&c_3x^3 + c_6x^2 + c_2x^2 + c_5x^1 + c_1x^1 + c_4x^0 + c_0x^0 = \\
&d_3x^3 + d_2x^2 + d_1x^1 + d_0
\end{aligned}
\tag{19}
$$

and

$$
\begin{aligned}
&d_0 = c_0 \oplus c_4 = (a_0 \bullet b_0) \oplus (a_1 \bullet b_3) \oplus (a_2 \bullet b_2) \oplus (a_3 \bullet b_1), \\
&d_1 = c_1 \oplus c_5 = (a_0 \bullet b_1) \oplus (a_1 \bullet b_0) \oplus (a_2 \bullet b_3) \oplus (a_3 \bullet b_2), \\
&d_2 = c_2 \oplus c_6 = (a_0 \bullet b_2) \oplus (a_1 \bullet b_1) \oplus (a_2 \bullet b_0) \oplus (a_3 \bullet b_3), \\
&d_3 = c_3 = (a_0 \bullet b_3) \oplus (a_1 \bullet b_2) \oplus (a_2 \bullet b_1) \oplus (a_3 \bullet b_0).
\end{aligned}
\tag{20}
$$

When a(x) is a fixed polynomial, the operation defined in equation (18) can be written in matrix form as [1, 7, 11]:

$$
\begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} б_0 \\ б_1 \\ б_2 \\ б_3 \end{bmatrix}
$$

Figure 1: Modular product a(x) ⊗ b(x)

Because x4 +1 is not an irreducible polynomial over GF(2^8), multiplication by a fixed four-term polynomial is not necessarily invertible. However, the AES algorithm specifies a fixed four-term polynomial that does have an inverse [1, 7, 11]

$$
\begin{aligned}
&a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \\
&a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}
\end{aligned}
\tag{21}
$$

Another polynomial used in the AES algorithm (RotWord function) has coefficients [1]:

$a^0a^1a^2 = \{00\}$ i

$a^3 = \{01\}$

which is the polynomial x^3. If this polynomial is inserted in the previous matrix, we have [1]

$$
\begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{bmatrix} = \begin{bmatrix} 0_0 & 1_3 & 0_2 & 0_1 \\ 0_1 & 0_0 & 1_3 & 0_2 \\ 0_2 & 0_1 & 0_0 & 1_3 \\ 1_3 & 0_2 & 0_1 & 0_0 \end{bmatrix} \begin{bmatrix} б_0 \\ б_1 \\ б_2 \\ б_3 \end{bmatrix} = \begin{bmatrix} 0*б_0 + 1*б_1 + 0*б_2 + 0*б_3 \\ 0*б_0 + 0*б_1 + 1*б_2 + 0*б_3 \\ 0*б_0 + 0*б_1 + 0*б_2 + 1*б_3 \\ 1*б_0 + 0*б_1 + 0*б_2 + 0*б_3 \end{bmatrix} = \begin{bmatrix} б_1 \\ б_2 \\ б_3 \\ б_0 \end{bmatrix}
$$

Figure 2: RotWord

which gives the effect of rotation of bytes in word. Polynomial [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].

Array state

As stated in [11], Rijndael operations are internally performed on a two dimensional array of bytes called the state that consists of 4 rows of bytes, each of which contains Nb bytes, where Nb is the input sequence length divided by 32. In the state array, denoted by the symbol s, each individual byte has two indexes: its row number r, in the range 0 £ r < 4, and its column number c, in the range 0 £ c < Nb, hence allowing it to be referred to either as sr,c or as s[r, c]. For AES the range for c is 0 £ c < 4 since Nb has a fixed value of 4.

At the start (end) of an encryption or decryption operation the bytes of the cipher input (output) are copied to (from) this state array in the order shown in Figure 1.

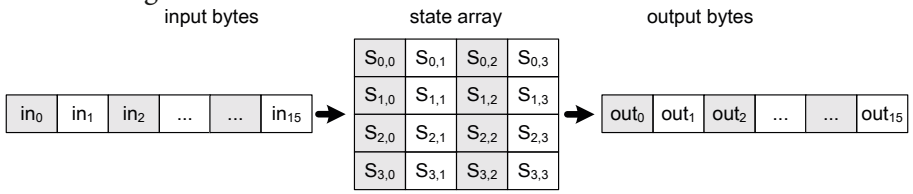


Figure 3: Input to the cipher state array and output from it

ALGORITHM SPECIFICATION

Rijndael is a key-iterated block cipher: it consists of the repeated application of a round transformation on the state. The number of rounds is denoted by N r and depends on the block length and the key length. [2].

The cipher transformation

Encryption function encompasses four AES transformations. Pseudo code encryption functions can be represented in the next few lines [7].

```
/* in out keys w */
Cipher (byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4, Nb]
state = in
/* initial mixing with key */
AddRoundKey( state, w[0, Nb-1])

/* „common“ rounds */
For round = 1 step 1 to Nr-1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
End for

/* final round */
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

Out = state
End
```

Listing 1: Pseudo code for Cipher() function

As stated in [7], individual transformations SubBytes() ShiftRows() MixColumns(), and AddRoundKey() transform the buffer State during each round. From the pseudo code can be seen that only the final round is different from previous Nr rounds, in that it does not perform the MixColumns() function. The article [2] states that the authors changed the names of some transformations according to the suggestions Dr. B.Gladmana in relation to the original document filed.

Subbytes transformation

The SubBytes() transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box). This invertible S-box is constructed by composing two transformations [1, 7]:

1 .Take the multiplicative inverse in the finite field GF(2^8), the element {00} is mapped to itself.

2. Apply the following affine transformation

$$б'_u = б_u \oplus б_{(u+4) \bmod 8} \oplus б_{(u+5) \bmod 8} \oplus б_{(u+6) \bmod 8} \oplus б_{(u+7) \bmod 8} \oplus ц_u \qquad (22)$$

for 0 <= i < 8 , where b_i is the i_{th} bit of the byte, and c_i is the ith bit of a byte c with the value {63} or {01100011}.

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Figure 4: Single S-Box element

Effect of the SubBytes() transformation on the State is

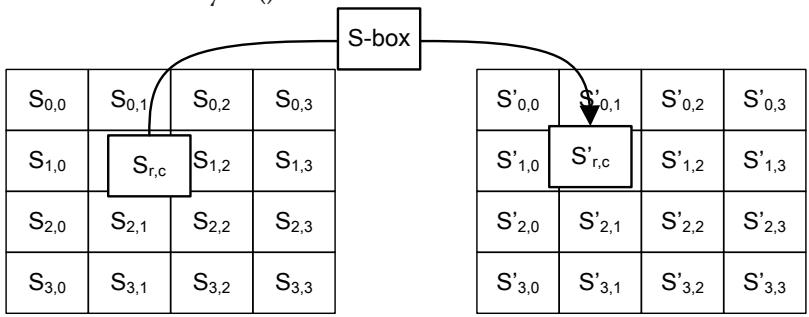


Figure 5: Applying SubBytes on single State element

Shiftrows transformation

As stated in [7], in the ShiftRows() transformation, the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets). The first row, r = 0, is not shifted.

$$S'_{r,c} = S_{r,\,(c + shift(r, Nb))\ mod\ Nb}$$
$$za\ 0 < r < 4\ i \qquad (23)$$
$$0 \le c < Nb,$$

Figure 6 illustrates the ShiftRows() transformation.

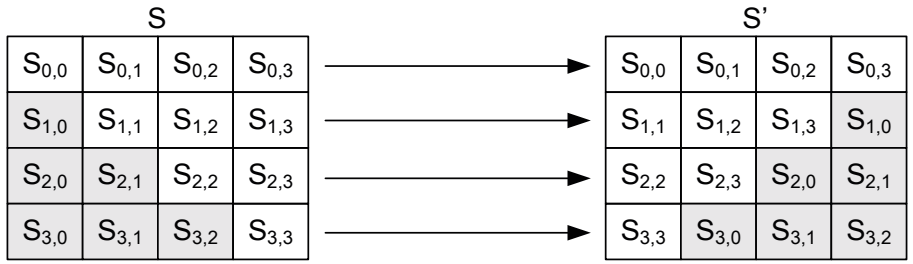


Figure 6: Applying SubBytes on single State element

Mixcolumns transformation

The MixColumns() transformation operates on the State column-by--column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo $x^4 + 1$ with a fixed polynomial a(x), given by [1, 7]

$$a(x) = \{03\}x\mathbf{3} + \{01\}x\mathbf{2} + \{01\}x + \{02\} \quad (24)$$

this can be written as a matrix multiplication. Let

$$s'(x) = a(x) \otimes s(x) \quad (25)$$

$$\begin{bmatrix} b_{0,c} \\ b_{1,c} \\ b_{2,c} \\ b_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} c_{0,c} \\ c_{1,c} \\ c_{2,c} \\ c_{3,c} \end{bmatrix}$$

Figure 7: MixColumns transformation as matrix

The four bytes in a column are replaced by the following

$$\begin{aligned} S'_{0,c} &= (\{02\} \bullet s_{0,c}) \otimes (\{03\} \bullet s_{1,c}) \otimes (\{01\} \bullet s_{2,c}) \otimes (\{01\} \bullet s_{3,c}) \\ S'_{1,c} &= (\{01\} \bullet s_{0,c}) \otimes (\{02\} \bullet s_{1,c}) \otimes (\{03\} \bullet s_{2,c}) \otimes (\{01\} \bullet s_{3,c}) \\ S'_{2,c} &= (\{01\} \bullet s_{0,c}) \otimes (\{01\} \bullet s_{1,c}) \otimes (\{02\} \bullet s_{2,c}) \otimes (\{03\} \bullet s_{3,c}) \\ S'_{3,c} &= (\{03\} \bullet s_{0,c}) \otimes (\{01\} \bullet s_{1,c}) \otimes (\{01\} \bullet s_{2,c}) \otimes (\{02\} \bullet s_{3,c}) \end{aligned} \quad (26)$$

Addroundkey transformation

In this transformation , the state is modified by combining it with a round key with the bitwise XOR operation [2]. Nb words from the key schedule are each added (XOR'd) into the columns of the state so that [1, 7]:

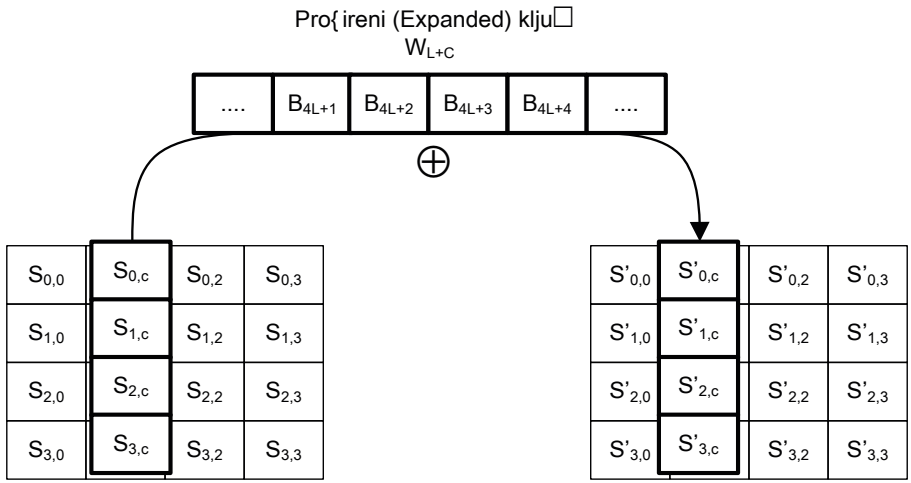


Figure 8: AddRoundKey transformation

The key schedule

As in [11] the round keys are derived from the cipher key by means of a key schedule with each round requiring Nb words of key data with an extra initial set making Nb(Nr + 1) words in total. The resulting key schedule consists of a linear array of 4-byte words, denoted [wi], with i in the range

0 <= i < Nb(Nr + 1).

The function RotWord(x) takes a word $[b_0 , b_1 , b_2 , b_3]$ as input and returns the word

$[b_1 , b_2 , b_3 , b_0]$.

The word array Rcon[i] contains the values given by $[x^{i-1}, 0, 0, 0]$ with x^{i-1} being powers of x in the field GF(256) (note that i starts at 1, not 0).

```
KeyExpansion( byte key[4*Nk], word w[Nb*(Nr + 1)], Nk)
begin
word temp
i = 0
while (i < Nk)
w[i] = word( key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
i = i + 1
end while
i = Nk
while ( i < Nb*(Nr + 1) )
temp = w[i-1]
if ((i mod Nk) = 0)
temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
else if ( (Nk > 6) and ((i mod Nk) = 4)
temp = SubWord(temp)
end if
w[i] = w[i - Nk] xor temp
i = i + 1
end while
end
```

Listing 2: Pseudo code for KeyExpansion

INVERSE CIPHER

AES Decryption computes the original plaintext of an encrypted ciphertext. During the decryption, the AES algorithm reverses encryption by executing inverse round transformations in reverse order. The round transformation of decryption uses the functions AddRoundKey, InvMixColumns, InvShiftRows, and InvSubBytes [12]. The Inverse Cipher is described in following pseudo code [1]:

```
InvCipher (byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4, Nb]
state = in
AddRoundKey( state, w[Nr*Nb, (Nr+1)*Nb-1])

For round = Nr-1 step -1 downto 1
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
InvMixColumns(state)
End for

InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[0, Nb-1])

Out = state
End
```

Listing 3: Pseudo code for InvCipher() function

PERFORMANCE IMPROVEMENT

Today's cryptographic algorithms are designed in a way that they combine mathematical theory and practice of computer science in order to improve resistance to cryptanalysis. Complexity of cryptographic algorithms caused the respective requirements in terms of processing power.

In order to increase performance, hardware manufacturers today are using multiprocessor systems or hardware accelerators. The first request requires a special way of code writing from the manufacturers of the system as well as cryptographic software. The second request from the software manufacturer imposes an obligation to adapt to the specific drivers or special instruction sets. A special kind of improvements is represented by the research of potential acceleration of modes of operations by using parallelization.

When it comes to performance of this algorithm, there is the potential use of specific solutions, such as eg. assembler language or C / C ++ for the AES-NI instruction set. There are a number of works that examine the possibility of algorithm AES acceleration [9, 13, 14, 15, 16] on different platforms and programming languages.

Recently, there have been emerged three programming paradigm connected with AES algorithm acceleration. There are a number of studies [17, 18, 19] that have focused on the performance improvement of this algorithm by using parallelization of its execution.

In terms of performance improvements, there are solutions that use the GPU parallelization and performance improvement as [1, 20, 21, 22].

In his study Manavski [22] discusses the possibility of the implementation of the algorithm AES using at that time traditional approach, that is based on the OpenGL library as well as the implementation using the NVIDIA CUDA platform and determine the benefits that are achieved using the new architecture.

The existence of different modes of operations has already served as an idea for parallelization of execution of some algorithms. According to Lipmaa et al. [23] blocks C1, C2, ... can also be encrypted at the same time and therefore CTR mode can be paralelized.

The rapid development of GPU (Graphic Processing Unit) units and user environments such as NVidia CUDA or OpenCL has led to various attempts AES algorithm parallelization using CTR mode. Thus, according to Tran et al. [24] the authors first increase the size of the block in relation to the standards defined by AES algorithm, and then use the coarse grained granularity for algorithm parallelization. Authors in the solution shown in (Di Biagio et al. 2009) using a fine (fine grained) and internal granularity parallelism of each round by independently manipulating with 4 32-bit words (T-word) that occur in each AES-this round. Authors in [21] are using a fine grained granularity and internal parallelism of each round by independently manipulating with 4 32-bit words (T-word) that occur in each AES-this round.

In an Intel document [25] author present the source code of programs that are generated keys and 128-bit, 192-bit and 256-bit encryption and decryption in ECB, CBC and CTR cryptographic modes. This text presents the source code for the simultaneous (parallel) processing of 4 blocks of data in the ECB, and the CTR mode and decryption in CBC mode. All examples can be compiled using Intel C/C ++ compiler v11 or later.

Hoban et al. [26] in exploring the possibility of improving the method for encryption within the operating system Linux provide a solution for the performance of this algorithm parallelization using XTS encryption mode. In [27] authors examine possibilities of achieving performance improvement by using new parallel tweakable OFB modes of operation. In creation of these new modes, XEX and XE constructions and XTS-AES multiplication are used.

As stated in [1], research has shown that the greatest acceleration in the execution of the algorithm can be achieved using aes-ni instruction set. In addition, use of GPU units for AES algorithm parallelization has enormous potential for the performance acceleration of this algorithm. Use of the GPU units in programs have shown almost equal performance with programs using Ni-AES instruction set.

CONCLUSION

In this paper gives an overview of the algorithm AES with its transformations and basic directions and methods used to accelerate its execution. A characteristic of today's conventional computer system is slowing the growth rate of single-processor systems and focusing hardware manufacturers on multi-processor systems and hardware accelerators. In order to increase AES algorithm performance, programmers and hardware manufacturers today are using parallel programming or hardware accelerators. There are great number of researches that have been focused on the performance improvement of this algorithm by using parallelization of its execution. A substantial part of this research is devoted to parallelization using GPU devices, where they achieved very significant results. Exploration of the possibilities for parallelization of individual modes of operation is another direction in which they move numerous studies. However, hardware acceleration, such as AES-NI acceleration is currently unmatched when it comes to speeding up AES algorithm.

Sažetak

Moderna kriptografija se u velikoj mjeri oslanja na kompleksne algoritme koji su zasnovani na matematičkoj teoriji i na praksi računarskih nauka. Današnji kriptografski algoritmi se dizajniraju oko binarnog formata podataka imajući pri tome u vidu i pretpostavku težine izračunavanja da bi što više otežali mogućnost njihovog razbijanja. Jedan od algoritama čija je otpornost na kriptoanalizu tokom prethodnih 16 godina intenzivno testirana je algoritam AES.

Advanced Encryption Standard (AES) je prvi kriptografski algoritam koji je nastao kao rezultat javno objavljenog i održanog takmičenja od strane NIST instituta (National Institute of Standards and Technology) 1997. godine da bi se pronašao algoritam koji će postati slijedeći standard američke vlade. AES je nastao restrikcijom pobjednika ovog takmičenja, algoritma pod nazivom Rijndael, na blok veličine 128 bita. Od momenta njegovog prihvatanja za standard 2001. godine traju neprekidna testiranja i istraživanja njegove otpornosti na kriptoanalizu ali i testiranja i istraživanja skoncentrisana na poboljšanje njegovih performansi. Ovaj rad predstavlja detaljan pregled algoritma AES zajedno sa svim njegovim transformacijama u i sa idejama za ubrzanje njegovog rada.

Ključne riječi: *kriptografija, algoritam AES, performanse*

REFERENCES

1. Damjanović B. (2016) Adaptive implementation of the AES algorithm in modern operating systems, Ph.D. thesis, University of Belgrade, Faculty of Organizational Sciences
2. Daemen J., Rijmen V., (2002). The Design of Rijndael, Springer-Verlag, Inc.
3. KONHEIM A. G., Computer Security And Cryptography, John Wiley & Sons, Inc., Hoboken, New Jersey, 2007
4. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1999). Performance comparison of the AES submissions.
5. Biham, E. (1999, March). A note on comparing the AES candidates. In *Second AES Candidate Conference* (Vol. 266, pp. 22-23).
6. Bassham, L. E. (1999). *Efficiency testing of ANSI C implementations of round 1 candidate algorithms for the advanced encryption standard*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.
7. Specification for the ADVANCED ENCRYPTION STANDARD (AES), (2001) Federal Information Processing Standards Publication 197, Available at: http://csrc.nist.gov/publications/.
8. Satoh, A., Morioka, S., Takano, K., & Munetoh, S. (2001, December). A compact Rijndael hardware architecture with S-box optimization. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 239-254). Springer Berlin Heidelberg.
9. DAMJANOVIĆ, B., & SIMIĆ, D. (2013). Performance evaluation of AES algorithm under Linux operating system. *Proceedings of the Romanian Academy Series A–Mathematics Physics Technical Sciences Information Science*, *14*(2).
10. Daemen J., Rijmen V., (1998) The Rijndael Block Cipher Proposal, NIST, Available at: csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
11. Gladman, B., (2007), A Specification for Rijndael, the AES Algorithm, Available at: http://gladman.plushost.co.uk/oldsite/cryptography_technology/rijnda
12. Hyubgun Lee, Kyounghwa Lee, Yongtae Shin, AES Implementation and Performance Evaluation on 8-bit Microcontrollers, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009
13. Elbirt, A. J., Yip, W., Chetwynd, B., & Paar, C. (2001). An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *9*(4), 545-557.
14. Mandal, A. K., Parakash, C., & Tiwari, A. (2012, March). Performance evaluation of cryptographic algorithms: DES and AES. In *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on* (pp. 1-5). IEEE.
15. Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2008). Performance evaluation of symmetric encryption algorithms. *IJCSNS International Journal of Computer Science and Network Security*, *8*(12), 280-286.
16. Singhal, N., & Raina, J. P. S. (2011). Comparative analysis of AES and RC4 algorithms for better utilization. *International Journal of Computer Trends and Technology*, *2*(6), 177-181.
17. Saggese, G. P., Mazzeo, A., Mazzocca, N., & Strollo, A. G. (2003, September). An FPGA--based performance analysis of the unrolling, tiling, and pipelining of the AES algorithm. In *International Conference on Field Programmable Logic and Applications* (pp. 292-302). Springer Berlin Heidelberg.
18. Yoo, S. M., Kotturi, D., Pan, D. W., & Blizzard, J. (2005). An AES crypto chip using a high--speed parallel pipelined architecture. *Microprocessors and Microsystems*, *29*(7), 317-326.

19. Granado-Criado, J. M., Vega-Rodríguez, M. A., Sánchez-Pérez, J. M., & Gómez-Pulido, J. A. (2010). A new methodology to implement the AES algorithm using partial and dynamic reconfiguration. *INTEGRATION, the VLSI journal*, *43*(1), 72-80.
20. Iwai, K., Kurokawa, T. and Nisikawa, N. (2010), AES Encryption Implementation on CUDA GPU and Its Analysis, First International Conference on Networking and Computing (ICNC)
21. Di Biagio, A., Barenghi, A., Agosta and G. and Pelosi, G. (2009), Design of a Parallel AES for Graphics Hardware using the CUDA framework, IEEE International Symposium onParallel & Distributed Processing
22. Manavski, S.A. (2007), CUDA Compatible GPU as an Efficient Hardware Accelerator for AES Cryptography, IEEE International Conference on Signal Processing and Communications,
23. Lipmaa H., Rogaway P and Wagner D., (2000), Comments to NIST Concerning AES--modes of Operations: CTR-mode Encryption. In Symmetric Key Block Cipher Modes of Operation Workshop, Baltimore, Maryland, USA
24. Tran, N. P., Lee, M., Hong, S., & Lee, S. J. (2011, August). Parallel execution of AES-CTR algorithm using extended block size. In *Computational Science and Engineering (CSE), 2011 IEEE 14th International Conference on* (pp. 191-198). IEEE.
25. Gueron, S. (2012), Intel Corporation, White Paper, Intel Advanced Encryption Standard (AES) New Instructions Set
26. Hoban, A., Laurent, P., Betts, I. and Tahhan, M. (2013), Unleashing Linux*- Based Secure Storage Performance with Intel AES New Instructions, Intel Corporation, White Paper,
27. Damjanović, B. and Simić, D. (2015), Tweakable parallel OFB mode of operation with delayed thread synchronization, Wiley, Security and Communication Networks, Security Comm. Networks (2015), Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1404.

ISSN 0354-9852
Pregledni rad
Overview paper

UDK 821.111.09-31 Lorens D. H.
DOI 10.7251/AKT1636002DJ
COBISS.RS-ID 6277912

BODY OBJECTIFICATION AS ILLUSTRATION OF SOCIAL RELATIONSHIPS IN THE NOVEL 'LADY CHATTERLEY'S LOVER' BY DAVID HERBERT LAWRENCE

Vesna Đurović

Abstract

Lady Chatterley's Lover is one of Lawrence's novel that caused the most controversy in the English society back then. This is one of the few books which was prosecuted for obscene and immoral scenes and the use of inappropriate words, as members of aristocratic English society formulated it. The fact is that Lawrence through this novel in a different way of description and presentation of the body describes all the shortcomings and contradictions of the English society then. What makes this novel contemporary even nowadays is that unfortunately these relations are still present, with the only difference is that ruling class present those who are the owners of capital and the working class remained the same, only the means of labour and the ways of working have changed.

Key words: *social relations, working class, aristocracy, body, moral, object*
JEL classification:Y3

THE PAPER

When analysing this novel moral and objectification should be seen in a wider context. If the literature is one of the elements of social control, then Lawrence's illustration of the body and sexuality is the contrast to overall social and sociological control of the society back then. Lawrence through illustration of the gamekeeper's and Connie's body, as representatives of two different social classes, politesse the problem of socially contrasted classes. By that act he makes enormous distance from morally accepted norms. When the social reaction on the publishing the novel *Lady Chatterley's Lover* is analysed it is clear how much this novel was contrasting with socially accep-

ted norms of the society back then. It is not only up to certain words the things that cause attention of the censors, but the fact that Lawrence with the use of those words illustrates neutral relationship of the members of different classes, thus criticizing the relation of superior and subordinate class. Lawrence points out that 'culture and civilization have taught us to differentiate word from the act, thought from the action or physical reaction.'[1]

Seen from this perspective, it is clear that D. H. Lawrence's novel is not at least obscene, nor filled with 'shameful' words or acts. Lawrence thinks that his book is necessary and useful to society and illustrates that with several examples, putting in contrast an aged puritan man who ends up at the court because he raped an underage girl, and a young man from the jazz generation who his life and body sees as a cocktail which he takes and rushes forward, not looking back.[2]

Lady Chatterlåó's Lover is a story that celebrates a healthy physical relationship between members of the two different classes. What is interesting in this novel is the fact that in almost all Lawrence's novels a female body is the object of observation, description and analyse. In *Lady Chatterley's Lover,* the two male bodies is what Lawrence puts in contrast: a healthy, potent body of the gamekeeper Melrose and sick, disabled body of Sir Clifford.

The novel itself is filled with specific relationship among the characters. From the very beginning through the description of the sisters' development, Constance and Hilda, Lawrence emphasises that there is the change in the generations and that the new generation is wild, playful, curious in its great wish to change relationships in society around them. Sisters are the members of intellectual social classes. Their interlocutors are students, members of certain young intelligence of cosmopolitan spirit. They passionately discuss on various spiritual, social, intellectual and emotional issues with young men they socialise with. Physical relationship is unsatisfactory because it represents just a bare result of intellectual struggles. Connie finds unsatisfactory that and first uncomplete contact. She simply does not understand the point of such a relationship, when she feels more excitement during some discussion with an interesting topic where she can show completely all the sharpness of her intellect and orator capability. At the beginning, Connie is a girl of sensual body, ruddy cheeks, soft face and sharp intellect who indulges in the beauties of art, good, qualitative and constituent conversation on topics connected to the whole society, because she is the society. Connie is, a typical representative of young, wild conscious middle intellectual class. The relationship between genders represents a kind of mini arena for the proving of scientific theses, that is physical relationship of man and woman is a re-

1 Лоренс, Д. Х., *Љубавник леди Четерли,* Отокар Крешовани, Ријека, 1963. стр. 6.
2 Ibid, стр. 9.

lationship of different social classes of the English society, as it is described at the beginning of the novel. Physically more capable, in this case men, or ruling class in wider perspective, take like a predator what they believe belongs to them by the right of birth. The only weird thing in this relationship is the fact, they take and use what does not belong to them, the ruling class, well almost everything, the right on work, vacation, food, even life itself. The joyful socialising lasts until the beginning of The World War I. In the moment of disturbance of global scale, the border between the members of different social classes starts to disappear. The cosmopolitan gang falls apart because it is made of the members of different nations. Connie's boyfriend gets killed, and Connie returns in England where she joins to intellectual elite of Cambridge students. There is a real patriotic euphoria in England at the beginning of the war. Intellectual youth of England observes everything with a mild irony. In this environment we meet Clifford and his brother who laughs on the news of killing of English young men on front line. This laughter, so horrible and sarcastic is heard until the moment when Clifford faces the loss of his brother and his own wounding.

The contrast in the feelings which Lawrence shows in only several pages is extraordinary. The playful youth from the beginning of the book is suddenly very serious and one might say even overtaken with the state in the world. The personal loss certainly hurts more and are not funny as it was the case with somebody else's losses. The whole society is now in the function of government's war plans, and personal faiths are pushed aside. Connie and Clifford start their life together, which is done for general good sake, because Clifford, as the only living heir of Chetterley's has the obligation to provide the next heir. The first days of life together pass in introduction and the beauties of honey moon. The martial happiness of the Chatterleyes and physical fulfilment unfortunately last for a very short period of time because Clifford must return to the front line and gets terrible wounded. Clifford returns home after the front line in a very serious condition. Thanks to capability of doctors and medical achievements Clifford will survive, but his life will never be the same. Here we can see that Clifford from the very beginning of the novel represents new, technically improved English society without emotions. The new society, as Lawrence describes in this novel, is on the good way to become inhuman, automated and sick. The lack of healthy physical relationship and physical closeness with another human being makes Clifford an emotional cripple. Clifford is incapable to live along with the people of Tevershall, although he was born and raised in this environment, he can less understand the miners, villagers and his staff then Connie who is, to be honest, somewhat closer to them by her class. Connie, contrary to Clifford, tries to understand what kind of problems troubles the citizens of

Tevershall and what are difficulties of dissatisfied miners. She defends the miners and tries to explain Clifford, who is freshly awaken industrialist, that he cannot accomplish the respect and obedience of the miners otherwise, but through the conversation. Unfortunately, Clifford will prove her contrary. In the new, industrial world, which looks more like a slavery society, the mine owner is in a way the owner of the miners' lives, as well as the whole social class which depends on the owner's attitude. Bodies and strength of the miners represent for Clifford only a bare instrument that works, earns and provides for him. In this case, the minors' bodies are the objects, but not a sexual one, as this is the case with the bodies of Melrose or Connie, but the object which represents an instrument of class division. It is the clear contrast between the Clifford's physically incapable body which represents industrial and intellectual class, and the minors' bodies, which are battered and exhausted with hard work but still persistent and at the end adjusted to hard life and new industrial society. It can be concluded that in the new society intellectual automatism will rule, not natural selection.

In the preface Lover Lady Chatterley's Lover Archibald MacLeish states that sometimes characters are more symbols than human beings and sometimes through text propaganda purpose appears. It can be clearly concluded against which is Lawrence in the modern, industrialized world but also it is not entirely clear what he stands for.[3]

Lawrence attitudes regarding class differences are clear, he represents the working class, but it is not completely clear the goal nor what is the future of this class. The characters really are a kind of symbol of class affiliation, Clifford ownership class, Connie middle, game keeper working and every one of them in many ways illustrates all the problems, all the differences and all the intransigence of the class. At the beginning of the novel Connie is a typical representative of the curious middle class who tends to climb over on the social scale. In the beginning of married life Clifford and Connie through their physical contact and interaction, we can guess that this is just a perfect combination. The young couple understand each other perfectly and together they survive the cruel world at the beginning of the First World War. However, as time passes and Clifford is more accustomed to his handicap. Connie, who was initially a perfect support and comfort, is gradually becoming distant. Because of the remoteness, Connie is able to look at things from another angle. She realizes that she is involved in a vicious cycle of physical, mental and emotional discontent. At a different perspective of observation Connie is encouraged by the new acquaintance with the local game keeper, who by his birth belongs to the working class, but thro-

3 Lawrence, D. H., *Lady Chatterley's Lover,* Grove Press, New York, 1959. VI, (предговор написао: Archibald Macleish).

ugh his education and military service was on his way to also climb the social ladder. At the beginning of this combination works well. All classes are intertwined, and complement each other, and they are dependent on each other. In contrast to such a beginning, the end is quite different. All the characters are somehow returning to a class backward: Connie binds to gamekeeper, Melrose gives up the standard language and moves to the dialect, and Clifford experience some kind of spiritual, class and emotional collapse. He will bind his life to Mrs. Bolton, a nurse and a new member of staff, who eventually grows into something more important than just a member of the staff and thus climbs up the social ladder. Lawrence through a physical description of the characters illustrates the class where characters belong to. Connie's core young woman typical female attributes. Its appearance is by no means appropriate for the times in which he lives, when women are thin and built more like boys, but as a future mother. The moment you begin to suffer as a result of physical inactivity Connie weak physically, her emotional strength also decreases. Her salvation found in relation to the gamekeeper, whose healthy body just represents the class to which it belongs, the working class. Lawrence through a physical description of the characters illustrates the class where characters belong. Connie is a healthy young woman with typical female attributes. With her appearance she is by no means appropriate for the times in which she lives, when women are thin and built more like boys, but as a future mother. In the moment she begins to suffer as a result of her physical inactivity Connie starts to weak physically, her emotional strength also decreases. She finds her salvation in relation with the gamekeeper, whose healthy body also represents the class to which he belongs, the working class. His body is a body built to withstand a variety of efforts. In some descriptions in moments of absolute physical and emotional nakedness Lawrence places the body of game keeper in a sort of contrast to himself. More broadly it is described the contrast of fragility and extraordinary physical strength of the new working class, which with the development of technology and machines become just an instrument for launching industrial machinery, in some way, a screw which drives, but unfortunately a necessary one. The question is whether the new people in the modern world will become uniformed figures moving in a predetermined protocol, without thoughts and feelings? Clifford's body represents the ruling class. Strong intellect and body damaged in the war represents what to Lawrence's predictions will happen to the ruling class. Clifford's emotional breakdown at the end of the novel, and his total surrender to Mrs. Bolton represents only a simple illustration of the future, and it is clear, according to Lawrence, it will not be at all fabulous. High class due to alienation from

simple and natural relations would be brought to collapse and eventually set partly in a precarious position.

Mrs. Bolton is a strong woman. She has all the features one caring woman who is accustomed to nurture patients. A sufficient amount of tenderness and bitterness due to premature loss of her husband, who is in fact characterized as a coward, have made Mrs. Bolton perfect expert on social conditions and wise counselor and observer of The Chetterley's home. Mrs. Bolton monitors the situation between spouses at all times. She is a friend in long sleepless nights to Clifford and, in some ways, an ally of Constanca in her secret relationship with a game keeper. At one moment she tries to create a positive climate in case Constance gets pregnant creating illusory story of incredible possibilities. Mrs. Bolton actually tries to keep the existing emotional and social state. She is aware of the new conditions in which Mrs. Chatterley's is, and according to that, she tries to keep the temporary state.

Yajing Li in her paper *Love Accounts in D. H. Lawrence's Novels* points out that Lawrence believed that industrialized western culture is inhuman because it emphasises the intellectual characteristics versus the natural ones or physical, which leads to complete alienation. Li points out further that this culture, as such, is fainting and that humankind will soon evaluate into a new state of consciousness, that is the state that it belongs to the nature. One of the aspects of this 'blood consciousness' would be the acceptance of the need for sexual fulfilment.[4]

The proof of this claim just could be Lawrence's description of Constanta, which due to physical emptiness and dissatisfaction gradually veins, and from the beginning of an affair with a game keeper, an affair that completely absorbs her and fulfills physically, her body gets again healthy and vibrant segments. The primeval human need is bonding with another human being. Only a full understanding of himself and the people around us can lead to progress of individuals and society as a whole. An iconic is the human need to get close to another human being. Only complete understanding of oneself, and people surrounding us can lead to progress of individual and complete society.

Li further states that the novel *Lady Chatterley's Lover* proved that Lawrence explicit scenes of nudity and sex does not use for the sake of sex. There is no doubt that the book is moral one. Lawrence leads to the conclusion that in fact the old doctrine makes mistake, the one that says that sexuality and moral are separate units.[5]

This segment of human relations, since it is inherently natural as such is moral. As well as the relations in which the human body appears. If the re-

4 Li,Yajing, *Love Accounts in D.H. Lawrence's Novels,* US-China Foreign Language, USA, 2006, 31.
5 Ibid, 30-31.

lationship was created out of pure desire and need to express affection of two human beings, this relationship cannot be immoral. Seen in this light, Lawrence was right when he argues that sexuality and morality should not be seen as separate entities. In a healthy relationship between two people there should come to a råapprochement and deepening of relations. The consequences of a lack of understanding and coexistence by force are obvious if we look at the relationship of Connie and Clifford. That artificial relationship, without complete physical and psychological understanding is empty and unsatisfactory. Put in the words of one of Lawrence's characters the relationship between to people is nothing but the exchange of feelings, rather than the exchange of ideas.[6] This notion exactly describes Lawrence's attitude on human interaction. Eventually this interaction between Clifford and Constanca is lost and become everything, but the exchange of emotions. Clifford and Connie fulfil their life with the exchange of ideas, attitudes on different social issues. The Chaterrley's are surrounded by people who have empty attitudes and endlessly lot of time to discuss about them. An excellent illustration of this claim is the scene when Clifford and Connie are visited by Clifford's Cambridge friends who endlessly discuss on various issues. The whole time, Connie sits calmly in the corner with her broidery. She does not include in the conversation for a moment, but she is also well aware that without her presence, this conversation would not be as lively, and participants would not be so eloquent. At the end, the topic of discussion itself is pointless and meaningless.

It can be stated that in the book there is a kind of contrast in manifestation of love. Love or similar sentiment between Connie and Clifford is a high-ranking socially acceptable behavior. Often there are pictures in various journals of Clifford sitting in a wheelchair in an intellectual pose and Connie, a silent, young woman, the perfect companion and shadow. Connie represents many English women after World War I. However, the '' soft '' sentiment and that sad, lost gaze, as presented in the photos, only present essentially the despair in which Connie is currently in and the contrast by its exuberant youth feels to the absence of physical fulfillment. Clifford his disability tries to replace with intensive writing of popular works, and later with full commitment to the mine, its modernization, as well as innovations that are related to the production of secondary products from the ore. How much Clifford is infatuated with technical achievements and his faith in the new, technical world, illustrates the scene when Connie and Clifford go for a walk and when his motor wheelchair brakes. His helplessness and despair are clearly displayed when he shouts at gamekeeper not to help him if the help is not sought. What Lawrence underscores here is a victory for the

6 Лоренс, Д. Х., *Љубавник леди Четерли,* "Отокар Крешовани", Ријека, 1963., 45.

natural over the technical. What Lawrence points out here is a certain victory of natural over technical. Joint Connie's and the gamekeeper's strength will push Clifford and his machine to the house. In a brief illustration of this scene we can see the segments of Lawrence's attitudes, and that is return to the nature, simple relationship of the human being to oneself and two human beings will provide humankind the continuity of existence. The disposal of our own bodies and orientation towards new, technical achievements, as illustrated in the character of Clifford, will make us incapable of automated machines, which cannot function if it breaks the smallest screw or quite a bit overheats. Even worse, it will make of us semi-automatic products that do not work in the natural environment.

The question is whether humanity moves away from the body's own need for moral reasons or moral reasons are you just stumbling block of the whole social system. Does the ruling class, nurturing '' moral principles '' descends away individuals from each other and from themselves or simply imposes a certain code of conduct that would subordinate the working class to their own needs and ideas? Lawrence through numerous descriptions of love scenes between Connie and gamekeeper tries to describe this. He describes the act of union, which complement each other giving the story fullness and meaning. This attitude is exactly the attitude that Lawrence considers natural.

1. The body represents the only form that is the driving force of a strong desire, natural and complete. Although Connie and Melrose are from different social classes and speak different dialects, their bodies recognize each other in the primal desire to complement each other and make them happy. Here social attitudes and social codes do not play any role in the primordial relationship that they establish with each other. Melrose is a man, and Connie is a woman who has needs and whose needs just a body, primordial and potent, can fulfill. The social codes and norms of behavior that are imposed by a small number of people who rule fall into the water, simply because the body seeks its satisfaction, which is natural and logical in itself enough.
2. The theme of social turmoil and mutual misunderstanding due to various social affiliation is extremely close to Lawrence from his own life. England in which Lawrence was writing was England of great turmoil and change. In the English society then was important to nurture socially acceptable relationship although such relationships is often a torture for one of the characters. A great example are Connie and Clifford. Connie had with Clifford socially acceptable relationship, but due to the lack of a healthy physical relationship gradually begins to fade, and the Lawrence very vividly demonstrated in numerous descriptions of the vigorous

body of the heroine of the novel and her essential contrast presented in the form of Clifford. Interestingly, Clifford's character is presented as morally correct in that society, and Connie is the one who has left home and family for the gamekeeper. We could say that Lawrence's had a little different sense of moral from the morality of his society. Lawrence to some extent justifies the Connie to leave Clifford and her new life makes with Melrose and the future child. For him is quite natural and morally justified to respect our own wishes.

3. Lawrence's use sexual act in his works was very shocking for the time in which he wrote, and later. But when we look at total of his work, just that scenes seem as natural part of his novels and stories. If we delete them or change, his work would lose meaning and compatibility. The value of these scenes is even greater because Lawrence was not interested in human touch as mere physical gratification. Lawrence in a physical relationship and intimacy of the body and touch, saw a way to restore the human being itself and its primordial essence, which is in harmony with nature and from nature arises. Li also points that the importance of highlighting the sexual act is not to increase the functions of sex in our lives, but to defend the feelings and sexuality that are based on morality. According to Li, this is a unity of body and soul. Lawrence puts in contrast the pure sexual act without feeling that in part will lead to a complete separation of humanity. Although sexual desire requires the unification of men and women, this unification is not only a result of this kind of desire, but the union of sentiments. Otherwise there would be no harmony between body and soul, it would be mere fornication.[7]

Lawrence emphasizes the extent to which basic social norms and moral principles in society diminish. Through the illustration of the human body and placing that same body in different situations of physical relationships Lawrence points to the fact that the human individual is always in a kind of shackles, mental or physical in relation to the ruling class. That is precisely the ruling class is trying to ornament their own parameters authorities through various management methods. In this way, the ruling class by the various moral norms and attitudes is trying to build a larger gap between members of different classes. An excellent example to illustrate this thesis is the scene where Clifford writes Connie about the events on the estate and the scenes that take place with a gamekeeper who was '' visited '' by ex-wife. Through an ironic and mocking tone, making use of the ornate literary style Clifford describes how '' mad '' wife visited the '' poor '' gamekeeper and tried to force restore and reconstruct the marital relationship. In anger

7 Li,Yajing, *Love Accounts in D.H. Lawrence's Novels,* US-China Foreign Language, USA, 2006, 30.

Melrose's wife displays all the details of married life of the divorced spouse without sparing words nor descriptions. What Clifford does not mention in his letter it is announced that Connie is also part of the martial triangle. It is clear that Connie is protected as a member of the ruling class, a gamekeeper must leave the estate, while his wife is under the threat of imprisonment. It is clear that different criteria are present when it comes to morally judgement to the members of different classes, although all of them are participants in the same event. The question is whether this is the outcome of the high moral of English society. This makes Constanca's to her life with Melrose so devastating not only for Clifford, but also for the entire English high society. It is devastating that despite all the differences and different habits, one member of high society is ready to give up all the benefits that high class offers for small joys of life and physical satisfaction. With this act Connie humiliated not only herself, but all members of the upper class. Despites that, she allowed the mixing and breaking the unbreakable social bonds and norms.

In this case, Lawrence represents characters bodies only as mere objects. Putting them for the first time in such a direct connection, Lawrence's characters are real social puppets. Each of these puppet has perfectly prepared role that at one moment should be played. The problem arises when puppets confuse texts and quotations. There is a strange mixture and strange turnover. But if one think about it more deeply, perhaps these turnovers are not so unexpected. There is no doubt that in some strict boundaries between different social units came to saturation. Further social progress is possible only if members of different classes mix. In this way, one could avoid the terrible saturation in social circles, and the human race would again could be healthy and free.

Lawrence is a man rich in spirit and extraordinary standpoints. Lawrence's beliefs are different from the beliefs of his contemporaries. In his latest novel, Lady Chatterley's Lover he described English society as he saw and experienced it. Of course, individual units of *Lady Chatterley's Lover* can be viewed globally and as a general remark on the social situation in the early twentieth century. The moral aspects of society in relation to Lawrence's standpoints are somewhat different and inappropriate.

REFERENCES

1. Adelman, Gary, *Reclaiming D. H. Lawrence,* Bucknell University Press, Lewisburg, 2002.
2. Бекер, Мирослав, *Модерна критика у Енглеској и Америци,* Младост, Загреб, 1973.
3. Ellis, David, *D. H. Lawrence's Women in Love,* Oxford University Press, Inc., New York, 2006.

4. George, Stephan K., *Ethics, Literature &Theory,* Rowman & Littelfield Publishers, Inc., Oxford, 2005.
5. Кољевић, Светозар, *Тријумф интелигенције,* Просвета, Београд, 1963.
6. Лоренс, Д. Х., *Тајне феникса,* Издавачко предузеће „Рад", Београд, 1977.
7. Lawrence, D. H., *Sex Literature and Censorship,* Twayane Publishers, New York, 1953.
8. Lawrence, D. H., *Fantasia of the Unconscious,* Thomas Seltzer, New York, 1922.
9. Марковић, Вида Е, *Енглески роман XX вијека,* Научна књига, Београд, 1982.
10. Пелеш, Гајо, *Тумачење романа,* АрТрессор наклада, Загреб,1999.
11. Пухало, Душан, *Енглеска књижевност XIX – XX вијека (1832 – 1950),* Научна књига, Београд, 1976.

ISSN 0354-9852
Pregledni rad
Overview paper

UDK 004.738.5:351.083.8
DOI 10.7251/AKT1636003K
COBISS.RS-ID 6278168

ZAŠTITA PODATAKA U GLOBALNOM LANCU SNABDEVANJA - PRIMENA SMART CM PLATFORME

DATA PROTECTION IN THE GLOBAL SUPPLY CHAIN - SMART CM PLATFORM APPLICATION

Tanja Kaurin[1], Milorad Kilibarda[2]

Sažetak

Globalni lanac snabdevanja obuhvata veliki broj učesnika, kao što su proizvođači, distributeri, logističke i transportne kompanije, brodari, granični terminali, carina i sl. Uspešno povezivanje svih učesnika u jedan sinhronizovan lanac nije moguće bez informacionih tokova, koji obezbeđuju efikasan protok informacija na različitim nivoima. Učesnici uglavnom imaju sopstvene informacione sisteme, a istovremeno su sastavni delovi različitih infomracionih i komunikacionih mreža na globalnom nivou. U takvim uslovima poslovanja od ključnog značaja je bezbednost informacija. Ovaj rad se upravo bavi problematikom zaštite podataka u globalnom lancu otpreme i isporuke kontejnera. Prvo su sagledani zahtevi kao što su: transparetnost, bezbednost, pouzdanost, pravovremenost, ekonomičnost, i efikasnost u lancu snabdevanja, a zatim je predloženo rešenje koje se zasniva na SMART CM platformi. Predstavljena je funkcionalna arhitektura platforme, ključni scenariji za uspešnu primenu i modeli funkcionisanja kroz određene blokove i slojeve. Definisani su formati poruka i izvori informacija. Na kraju su predstavljene mogućnosti i ograničenja primene platforme sa stanoviša najvažnijih učesnika u lancu otpreme i isporuke kontejnera.

Ključne reči*: Zaštita podataka, bezbednost informacija, lanac snabdevanja, SMART CM platforma*
JEL klasifikacija:L91

1 *Fakultet za pravne i poslovne studije dr Lazar Vrkatić, Novi Sad, tanja.kaurin@useens.net*
2 *Saobraćajni fakultet Univerziteta u Beogradu, miloradkilibarda@gmail.com*

UVOD

Globalni lanac snabdevanja je izuzetno složen, dinamičan i ranjiv na mnoštvo pretnji, rizika i opasnosti. Broj učesnika u lancu se svakodnevno povećava i od suštinske je važnosti obezbediti nesmetano i pouzdano snabdevanje privrede i krajnjih potrošača. Bezbednost globalnog lanca snabdevanja je preduslov za efikasno povezivanje tržišta i olakšanu međunarodnu trgovinu. Međutim, često se u lancima snabdevanja velika pažnja usmerava na brzinu izvršavanja operacija, što može otežati praćenje bezbednosti. Teško je osigurati isti nivo bezbednosti u svakom njegovom segmentu. Sistem za upravljanje bezbednošću lanca snabdevanja kombinuje tradicionalne načine upravljanja lancem snabdevanja sa merama bezbednosti, što omogućava kompanijama da zaštite svoje poslovanje od pretnji kao što su piraterija, terorizam i krađe. Antagonističke pretnje, drugi rizici i neizvesnosti mogu biti namerno izazvane, nezakonite i neprijateljske. Neophodno je uložiti značajne napore za uspostavljanje bezbednog lanca, kako bi se pretnje, rizici i opasnosti sveli na najmanju moguću meru. Svi uključeni u procese isporuke moraju biti dosledni i veoma ozbiljno shvatiti problem sigurnosti, dok pokušavaju da robu isporuče na vreme. Neophodan je interdisciplinarni pristup bezbednosti, koji uključuje dobro definisane protokole, razumevanje svetskih propisa, obuku zaposlenih, mere fizičkog obezbeđenja, temeljnu proveru različitih učesnika, video nadzor skladišta, utovara i istovara tereta, kao i korišćenje sigurnih objekata. Za one koji se bave ovim problemima postoje dva cilja: prvi je da se promoviše efikasno i bezbedno kretanje robe, a drugi je da se podstakne globalni lanac snabdevanja koji je pripremljen, može da izdrži sve veće pretnje, opasnosti i brzo se oporavi od poremećaja. Potrebno je razumeti i rešiti pretnje na početku procesa i ojačati bezbednost fizičke infrastrukture, prevoznih sredstava i informacija, uz maksimiziranje trgovine kroz modernizaciju infrastrukture u procesima.

U prošlosti su logističke kompanije i drugi učesnici u lancu snabdevanja uglavnom bili usmereni na povećavanje sigurnosti obavljanja logističkih operacija u fizičkom okruženju, ali poslednja istraživanja nesumnjivo ukazuju na sve veće opasnosti u virtuelnom okruženju. Neophodno je više pažnje posvetiti rizicima i pretnjama u informacionim tokovima i sistemima. Opravdano se očekuje da sigurnost informacija i podataka, postane ključna za bezbednost lanaca snabdevanja[3].

To je i bio osnovni motiv pisanja ovog rada, gde su autori pokušali da sagledaju različite aspekte vezane za vidljivost lanca snabdevanja, bezbednost informacija i zaštitu podataka u lancu snabdevanja. Nakon sporvedene

3 R. Banomyong. 2005. *"The Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management*". Pra Chan Road, Thammasat Business School, Thammasat University, Bangkok 10200, Thailand. Marit.Pol.MGMT, January-March 2005, Vol 32, No1, 3-13

analize, u radu je prestavljena SMART CM platforma za protok i zaštitu podatka u globalnom kontejnerskom lancu snabdevanja.

VIDLJIVOST LANCA SNABDEVANJA

Vidljivost lanca snabdevanja je sposobnost da se proizvodi u toku isporuke prate od proizvođača do krajnjeg odredišta. Cilj je poboljšati i ojačati lanac snabdevanja tako da podaci budu dostupni svim zainteresovanim stranama, uključujući i kupca. Može se reći da vidljivost lanca snabdevanja predstavlja snimanje i integraciju podataka, kreiranje inteligencije i donošenje odluka baziranih na promenama tri funkcionalna toka (materijal, kapital i informacije) u lancu snabdevanja zajedno sa relevantnim zahtevima za očuvanje životne sredine[45]. Međutim, kompanije se često suočavaju sa problemima kao što su: gubljenje vremena zbog ručnog zakazivanja isporuka i praćenja proizvoda od kanala do kanala; propuštene prilike jer se ne zna količina robe u tranzitu i raspoloživost zaliha; poremećeni odnosi nakon isporuke jer pošiljka ne stiže na vreme. Zajednički element svih ovih problema je nedostatak vidljivosti, odnosno sposobnosti da se vide podaci o proizvodima u realnom vremenu. Mnoge kompanije brzo su reagovale i u proteklih nekoliko godina, shvatajući da vidljivost nije samo želja već nesto što se mora obezbediti. Unapređenjem vidljivosti u lancu snabdevanja postižu se konkretni ciljevi, kao što su: smanjenje broja operacija i rizika, poboljšanje vremena isporuke i pravovremena identifikacija nedostataka ili lošeg kvaliteta duž lanca snabdevanja[6].

U većini organizacija informacije su projektovane tako da služe svrsi pojedinih odeljenja u organizaciji umesto da se koriste u celom lancu snabdevanja. Tako na primer, odeljenje prodaje ima svoje projekcije i budžet, proizvodnja ima svoj raspored proizvodnje, a kupci i dobavljači imaju svoje baze podataka, koje obično ne dele sa drugim učesnicima u lancu. Cilj poboljšanja vidljivosti lanca snabdevanja jeste obezbediti kontrolisan pristup i transparentnost kako bi se osigurali tačni i blagovremeni podaci i relevantne informacije duž celog lanca[7].

Vidljvost informacija je proces deljenja kritičnih podataka koji su potrebni za upravljanje protokom proizvoda, usluga i informacija u realnom vremenu između dobavljača i kupaca. Ako je informacija dostupna, ali joj ne mogu pristupiti učesnici koji treba da reaguju na datu situaciju njena vrednost se eksponencijalno smanjuje. Povećanje informacione vidljivosti u lancu snabdevanja omogućava rast prihoda, iskorišćenost sredstava i smanjenje

4 ttp://searchmanufacturingerp.techtarget.com/definition/supply-chain-visibility-
5 http://www.gtnexus.com/solutions/supply-chain-visibility
6 http://www.mepsupplychain.org/supply-chain-visibility/
7 Handfield R., *Creating Information Visibility in the Chain*, 2002.

troškova. Kako bi se povećala odgovornost u lancima snabdevanja kompanije razmatraju upotrebu zajedničkih modela koji dele informacije na različitim nivoima svih učesnika – od dobavljača svojih dobavljača do kupaca svojih kupaca. Ovi trgovinski partneri treba da dele prognoze, upravljanje zalihama, rasporede rada, optimiziraju isporuke i na taj način smanje troškove, povećaju produktivnost i stvore veću vrednost za krajnjeg kupca u lancu. Tradicionalni lanci snabdevanja se brzo razvijaju u „dinamičke poslovne mreže" koje se sastoje od grupe nezavisnih poslovnih jedinica koje dele informacije o planiranju i izvršenju logističkih operacija, kako bi se zadovoljili zahtevi korisnika[8].

Neki od razloga koji moraju biti uzeti u obzir prilikom implementacije informacionog sistema uključuju veličinu baze podataka o dobavljačima i kupcima sa kojima se razmenjuju informacije, kriterijume za unapređenje vidljivosti, strukturu podataka koji se dele i tehnologiju koja se koristi, što omogućava svim učesnicima da imaju pristup informacijama neophodnim za efikasno kontrolisanje protoka materijala, upravljanje zalihama, da ispune uslove iz ugovora i ispoštuju potrebne standarde kvaliteta.

Jedan od koncepata koji se često pominje u poslednje vreme jeste koncept „kontrolnog tornja lanca snabdevanja". Kontrolni toranj daje ključne podatke na raspolaganje partnerima u lancu snabdevanja kako bi se olakšala koordinacija zahteva kupaca i odgovora dobavljača. Kako bi se dostupni podaci transformisali u korisne informacije neophodan je razvoj u tri oblasti:

- Procesi – Procesi treba da postanu zajednički, sa razmenom podataka i saradnjom između odeljenja ali i između organizacija. Koordinacija projekcija prodaje i lanca snabdevanja može da pomogne dobavljačima da predvide buduće potrebe. Kompanije treba da razviju podatke koji mogu da se dele između partnera da bi bilo moguće planiranje potražnje. Takođe treba realizovati upravljanje rizicima kako bi se smanjila mogućnost prekida lanca snabdevanja.
- Povezanost (veze) – Informacije se moraju deliti između procesa, različitih poslovnih funkcija i izvan kompanije pružajući svim učesnicima realan uvid u procese. Saradnja je neophodna i za povećanje nivoa poverenja između partnera.
- Tehnologija – Glavni izazov u razmeni informacija jeste problem prenosa podataka između različitih informacionih sistema. Inovacije kao što su cloud computing, baze podataka i različiti softveri danas čine kontrolni toranj mogućim. Jednom kada se podaci dizajniraju tako da pruže učesnicima sve potrebne informacije kasnije se mogu koristiti za različi-

8 Kaurin T., Kilibarda M., *Informacione i komunikacione tehnologije u globalnim lancima snabdevanja,* Treća međunarodna naučna konferencija Evropska unija – izazovi proširenja i Zapadni Balkan, Banja Luka 2016.

te analize i planiranja. Kontrolni toranj omogućava kompanijama da precizinije upravljaju tražnjom kako bi smanjile nivo zaliha i odgovorile na zahteve kupaca brže i precizinije[9].

BEZBEDNOST INFORMACIJA I RIZICI U LANCU SNABDEVANJA

Vidljivost lanaca snabdevanja je moguće obezbediti preko različiti komunikacionih mreža, sistema, servisa i platformi. Internet ima najveći potencijal da obezbedi potrebnu informacionu vidljivost i olakša saradnju i donošenje odluka između različitih učesnika u lancu snabdevanja. Internet i novi komunikacioni servisi obezbeđuju izuzetne uslove za razmenu informacija, praćenje pošiljki i vidljivosti u realnom vremenu na globalnom tržištu. Međutim, internet kao jedna velika, globalna, otvorena i javna mreža koja, pored velikih mogućnosti za poslovanje sa partnerima i klijentima širom sveta, otvara i mogućnost za brojne prevare, malverzacije, zloupotrebe i online terorističke napade. Sve to predstavlja značajne rizike koje treba izbeći ili smanjiti njihove posledice.

Smanjivanje rizika u internet logistici predstavlja kompleksan postupak, koji obuhvata uvođenje novih tehnologija, organizacionih politika i procedura, novih zakona i industrijskih standarda, na osnovu kojih će se dati ovlašćenja nadležnim organima da gone i kažnjavaju počinioce cyber- kriminalnih radnji i time obezbede i očuvaju sigurnost u logistici koja se ugovara i prati preko interneta. Naime, konkurentske kompanije mogu „provaliti" u sistem određene logističke kompanije, sa ciljem da preuzmu informacije, preusmere porudžbine ili čak u potpunosti unište njen informacioni sistem kako bi zaustavili poslovanje i naneli štetu tom preduzeću i njegovim klijentima, a na taj način se može trajno uništiti reputacija napadnute kompanije. Zbog sve učestalijih online napada, logističke kompanije bi morale posebno da vode računa o sigurnosti svojih informacionih sistema. Međutim, potpuna sigurnost ne postoji, jer svaki sigurnosni sistem može biti ugrožen ukoliko se u ostvarenje takve namere ulože dovoljna sredstva. Ali trajna sigurnost u informacionoj eri nije ni potrebna. Informacije obično imaju vrednost u određenom vremenskom periodu, tako da je podatke moguće zaštititi prema potrebi na jedan dan, mesec ili godinu.

U tradicionalnoj i internet logistici postoji sličan rizik za snabdevača, logističku kompaniju i kupca. Tako na primer, u digitalnom okruženju za sve postoji rizik vezan za naplatu robe ili usluga, ukoliko se plaćanje odvija preko interneta. S druge strane, rizik za kupca proizvoda ili naručioca logističke usluge vezuje se za situaciju da plati robu ili uslugu, a da je uopšte ne

9 Handfield R., *Creating Information Visibility in the Chain*, 2002.

dobije, ili da dobije ono što nije poručio i platio. Osim toga, postoje i rizici vezani za aktivnosti trećih lica, koja svojim delovanjem direktno ugrožavaju bezbednost transakcija na internetu. U suštini lanci snabdevanja i pojedinačni učesnici izloženi su različitim kriminalnim rizicima veznim za poslovanje u virtuelno okruženje[10]. Internet kriminal ili kako se još popularno naziva „cyber" kriminal, predstavlja bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemima i mrežama, u kompjuterskim sistemima i mrežama i protiv kompjuterskih sistema i mreža[11]. Počinioci vrše napad na funkcije, servise i sadržaje koji se nalaze na internetu. Kradu se podaci, informacije, usluge i identitet, i oštećuju se ili čak uništavaju delovi ili cela mreža i računarski sistemi ili se ometa njihovo normalno funkcionisanje. U internet kriminal spadaju sve prevare koje se izvode uz pomoć računara i preko interneta. Generalno, internet prevara je bilo koja prevara, pri čijem izvršenju se koristi jedna ili više komponenti interneta, kao što su „chat rooms", web stranice, elektronska pošta i slično. Cilj je da se pribavi protivpravna imovinska korist ili da se stvore uslovi za lažno prikazivanje ili prikrivanje činjenica, kojim bi se neki učesnik u lancu snabdevanja doveo u zabludu ili u njoj održao. Takvo stanje omogućava da se učini nešto na štetu svoje ili tuđe imovine u lancu snabdevanja. Svakako je potrebno posebnu pažnju posvetiti najčešćim oblicima pretnji i narušavanja sigurnosti u onlinе okruženju, kao što su: zlonameran kod (eng. malicious code), hakeri, sajbervandalizam, lažno predstavljanje, prisluškivanje, špijuniranje, DDoS napadi, napadi iznutra i sl.

Generalno gledano, pri obezbeđenju vidljivosti lanca snabdevanja mogu se izdvojiti dve velike grupe rizika:

- Rizici u poslovnoj komunikaciji između velikog broja učesnika u lancu snabdevanja, putem interneta ili nekih drugih komunikacionih servisa, gde podaci u poslovnim porukama mogu biti kompromitovani ili razotkriveni;
- Rizici za informacioni sistem učesnika u lancu snabdevanja, kada informacije dolaze izvan sistema preko određenih komunikacionih kanala i servisa.

Kako bi se obezbedila zaštita podataka i informacionih sistema u lancu snabdevanja koriste se različite kombinacije zaštitnih mehanizama, aplikacija, protokola i internih kontrola, sa ciljem da se osiguraju integritet, privatnost i pouzdanost podataka.

10 Kaurin, T., Skakavac, Z., *Značaj digitalne forenzike mobilnih uređaja u otkrivanju i dokazivanju krivičnih dela organizovanog kriminala*, Peta Međunarodna znanstveno-stručna konferencija, Zagreb 2016, str. 58
11 http://www.uncjin.org/Documents/congr10/10e.pdf,

ZAŠTITA PODATAKA U LANCU SNABDEVANJA

Kada je reč o bezbednosti obavljanja logističkih aktivnosti u virtuelnom okruženju, tj. na internetu, najosetljivije tačke na kojima treba postaviti zaštitne mehanizme, sa tehnološkog aspekta, jesu sledeći nivoi zaštite: zaštita na nivou telekomunikacione mreže; zaštita na aplikativnom nivou; zaštita na nivou poruke.

Sistem zaštite na nivou telekomunikacione mreže obuhvata zaštitne mehanizme pristupa određenoj prenosnoj mreži, kako bi se u mrežu mogli uključiti samo autorizovani korisnici i to na osnovu korisničkih identifikacionih kodova i lozinki. Zaštita na ovom nivou obezbeđuje se identifikacijom uključenih strana u procesu razmene, odnosno pošiljaoca i primaoca poruke. Pouzdana i nedvosmislena identifikacija se obavlja pomoću sertifikata, koji dostavlja sertifikaciono telo – treća strana u razmeni u koju sve strane imaju poverenje i koja vodi registar svih partnera u razmeni. Sertifikaciono telo garantuje identitet partnera dostavom sertifikata sa svojim digitalnim potpisom.

Sistem zaštite na aplikativnom nivou podrazumeva davanje dozvola ili uvođenje dodatnih restrikcija, vezanih za korišćenje raspoloživih podataka, koje se uvode za korisnike koji su zadovoljili uslove bezbednosnog sistema na nivou mreže. Naime, određeni podaci ili aplikacije mogu biti zabranjeni ili dostupni za korišćenje određenim korisnicima, pa tako različiti korisnici mogu imati različita prava (pravo samo na čitanje sa internet stranice, pravo samo na unošenje podataka, pravo na čitanje i izmenu podataka, pravo na slanje podataka drugim stranama u razmeni i dr.).

Sistem zaštite na nivou poruka je izuzetno važan. U globalnom lancu snabdevanja poruka prolazi kroz veliki broj rutera i servera, pa se smatra da odatle vrebaju najveće sigurnosne pretnje. Zbog toga je visok nivo zaštite na nivou poruka izuzetno značajan za digitalnu logistiku. Pretnje mogu da budu izazvane namerno, kao posledica neovlašćene manipulacije sadržajem poruka ili nenamerno, kao rezultat grešaka u komunikacionom prenosu, kojima se menja sadržaj poruka. U svakom slučaju, razvijeni su brojni bezbedonosni mehanizmi za koje se koriste jedna ili više metodologija zaštite. Opšte pretnje bezbednosti poruka, mogu se najbolje sagledati analizom pet dimenzija sigurnosti obavljanja logističkog procesa[12]:

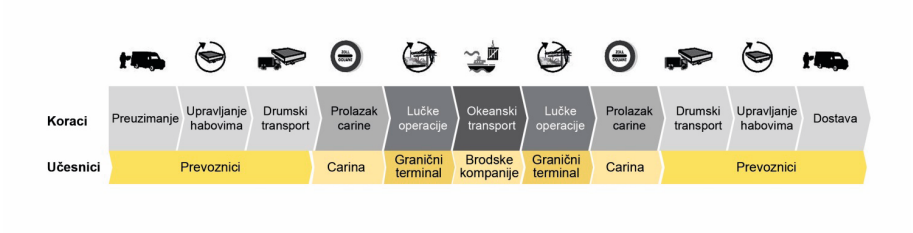
- *Poverljivost* – sposobnost da se obezbedi da informacije i podatke, koji su poslati preko interneta, može da vidi samo ovlašćeni subjekt, odnosno razmenjivani podaci treba da budu zaštićeni od neovlašćenog uvida, kopiranja ili otkrivanja;

12 K. Rethmann 2009. Logistics PEOPLE – The Rhenus Group customer magazine, *„How Does the Supply Chain Become Secure?"* No 2. Str. 11.

- *Integritet* – sposobnost da se obezbedi da informaciju koja je postavljena na internet mrežu, ili je poslata i primljena preko interneta, niko ne može ni na koji način da izmeni neovlašćeno. Integritet znači da su podaci tačni, potpuni, pouzdani i pravovremeni;
- *Autentičnost* – sposobnost utvrđivanja individualnog i poslovnog identiteta učesnika u lancu snabdevanja. Autentičnost znači da informacija zaista potiče iz navedenog izvora;
- *Dostupnost* – znači da su podaci raspoloživi, tj.dostupni u vreme i na mestu na kome su potrebni ovlašćenim licima;
- *Pravna usklađenost* – odnosi se na potrebu da interno razvijeni propisi u kompaniji, kojima se reguliše sigurnost podataka, budu unutar zakonskih okvira.

Mehanizmi zaštite podataka u lancima snabdevanja i logistici, u kompjuterskom i internet okruženju, treba da spreče narušavanje bilo kojeg od navedenih nivoa sigurnosti.

PRIMENA SMART CM PLATFORME U LANCU SNABDEVANJA



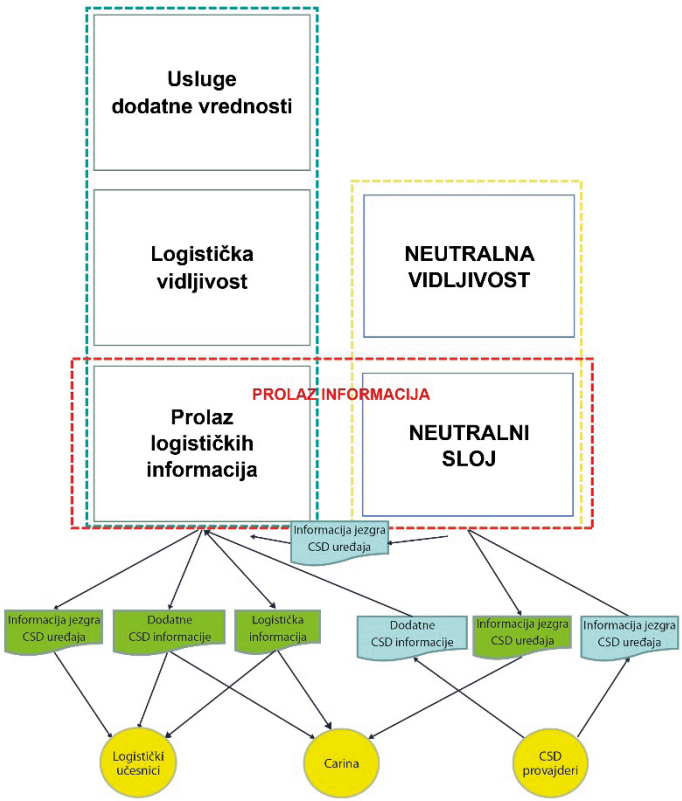
U globalnom lancu snabdevanja prisutan je veliki broj različitih učesnika, kao što su: pošiljalac, prevoznici, carina, granični terminali, brodske kompanije, logistički provajderi, inspekcije, primaoci robe i dr. (slika 1). Svi ovi učesnici realizuju različitet proce, koji su uređeni i povezani u lanac od mesta otpreme do mesta isporuke robe.

Slika 1. Učesnici u globalnom lancu snabdevanja

Učesnici obavljaju različite upravljačke aktivnosti i neophodan im je čitav niz informacija i podataka, kako bi efikasno upravljali lancem snabdevanja. Informacije imaju različite izvore, nastaju i završavaju na različitim mestima i od presudnog značaja je njihov efikasan protok i razmena između učesnika. Učesnici u lancu snabdevanja imaju različite zahteve vezane za protok informacija i podatka, kao što su: vidljivost, bezbednost, kompletnost, pouzdanost, tačnost, pravovremenost, efikasnost i dr. Navedene zahteve učesnika nije moguće uspešno realizovati, ukoliko ne postoji odgovarajuća informaciona i komunikaciona podrška. Potrebno je imati odgovarajuću platformu koja će omogućiti efikasan i siguran protok informacija i podata-

ka između učesnika u lancu. U skladu sa tim, u narednim izlganjima predstavljena je SMART CM platforma koja se koristi za razmenu informacija i praćenje kontejnera u globalnom lancu snabdevanja. Na bazi zahteva učesnika u lancu, definisana je funkcionalna struktura i arhitektura SMART-CM platforme, koja obuhvata dva polja delovanja. Prvo polje treba da zadovolji korisničke zahteve i upravljačke procedure u lancu snabdevanja, a drugo polje carinske i bezbednosne zahteve i procedure.

Platforma ima zadataka da obezbedi vidljivost i praćenje kontejnera kroz sve faze i procese lanca snabdevanja i da obezbedi bezbedan protok informacija između različitih učesnika u lancu. Informacije o kretanju i statusu kontejnera se prate preko „pametnog" sigurnosnog uređaja koji je postavljen na kontejner (CSD - Container Security Device). SMART-CM platforma je podeljena na informacioni prolaz, čija je osnovna namena prikupljanje podataka od različitih izvora i logistički sloj, gde se realizuju usluge praćenja i upravljanja procesima u lancu snabdevanja (slika 2)[13].



Slika 2. Strutkura i izgled funkcionisanja platforme

13 SMART-CM Implementation framework for global container surveillance and control, 2009.

Izvori podataka se generalno dele na tri osnovne kategorije: CSD informacije jezgra; CSD dodatne informacije i logističke informacije. U suštini se razlikuju sledeći formati poruka:

- Poruke sigurnosnog uređaja: poruke primljene direktno od CSD jedinica, a mogu biti brojevi kontejnera, CSD identifikacioni brojevi, informacije o statusu kontejnera.
- Poruke lanca snabdevanja: poruke koje su vezane za izvršavanje operacija u lancu snabdevanja ali se ne prenose putem CSD uređaja, kao što je identifikacija potrebnih dokumenata, izveštaji o prispeću kontejnera ili informacija o promeni vremena, i dr.
- Poruke i informacije dostupne u spoljnim bazama podataka, kao što su: detaljniji izveštaji o prispeću kontejnera, carinske procedure, komercijalne informacije (liste cena, liste pakovanja, fakture, tovarni listovi...).

Model protoka i razmene podataka odvija se kroz pet osnovnih blokova: blok sigurnosnih poruka, blok poruka lanca snabdevanja, blok obrade poruka, blok distribucije poruka i blok saradnje i dostupnosti. Blok sigurnosnih poruka i blok poruka lanca snabdevanja imaju mogućnost da rukuju sa „guranim" i „vučenim" porukama zbog većeg broja ulaznih kanala. Još jedna mogućnost je da se poruke učitavaju sa sigurnosnog servera. Čak i sa toliko različitih ulaznih kanala i protokola, blok poruka sigurnosnog uređaja ih sve podržava. Moraju biti dostupni najprostiji kanali i protokoli, ali mora biti moguća nadogradnja novih komunikacionih kanala unutar platforme, kao i podržana integracija različitih scenarija. Ulazni kanali sigurnosnog uređaja su odgovorni za upravljanje raznim scenarijima od nadolazećih poruka, kao i za transfer ovih poruka do bloka za dekodiranje poruka. Dekodiranje poruka sigurnosnog uređaja se primenjuje kada poruke ispune sigurnosne zahteve. Određene poruke mogu biti poslate šifrovane pa ih treba dekodirati, ili su određene poruke digitalno obrađene pa strana koja ih šalje treba samo da ih potvrdi. Kada se bezbednost i poreklo dolazeće poruke provere, poruka se dalje transformiše u poruku koja odgovara internim formatima, nakon čega se struktura i sadržaj proveravaju. Specifična pravila transformacije i provere za različite strane uglavnom su dostupne programu platforme, omogućavajući više verzija formata poruka koje se primaju u slučaju dodatnih informacija uz poruke. Nakon transformacije i provere, poruke se priključuju informaciji o kontejneru, gde je osnovna stvar odabrati pravi kontejner. Ovo obavlja blok identifikacije sigurnosnog uređaja na kontejneru. U zavisnosti od tipa poruke i količine dostavljenih informacija u sigurnosnoj poruci, ova združena informacija se može koristiti za određivanje tačnog kontejnerskog statusa i puta.

Nakon što se prime poruke lanca snabdevanja i sigurnosnog uređaja, njihov sadržaj se obrađuje u bloku za obradu poruka. To podrazumeva da se u porukama moraju poštovati poslovna pravila, sadržaj poruke se uparuje sa drugim informacijama o statusu kontejnera, te se pažljivo konstruišu poruke koje se šalju kao odgovor uključenim stranama. Svim odlaznim porukama upravlja blok za distribuciju poruka. Preko odgovarjuće matrice distribucije vrši se dostava odgovarajućim korisnicima. U slučaju da podaci koji se razmenjuju treba da budu zaštićeni, poruka će biti šifrovana zavisno od strane kojoj je namenjena. Blok za saradnju i dostupnost potrebno je da obezbedi konsolidovan pregled svih dobijenih statusa i detalja o kontejnerskom statusu, a podaci se dobijeni od sigurnosnog uređaja postavljenog na kontejner. Blok pretrage informacija o kontejneru pruža mogućnost da se preko pametnog uređaja postavljenog na sam kontejner traži određeni kontejnerski put. Potrebno je samo imati njegov identifikacioni broj. Ostali kriterijumi pretrage mogu biti definisani po određenim vrstama putovanja: identifikacija pošiljke, poslednja luka javljanja, logistički operator, itd.

ZAKLJUČAK

Internet i različiti komunikacioni servisi imaju izuzetno značajan potencijal za unapređenje globalnog poslovanja. Međutim, virtuelno okruženje prate i značajni bezbednosni rizici, koju mogu ugroziti globalni lanac snabdevanja i isporuku robe. Neophodno je da logističke kompanije i drugi učesnici u lancu snabdevanja preduzmu značajne mere i rešenja u pogledu zaštite podataka i informacionih sistema, a time i samog poslovanja. Mere i rešenja zaštite mogu da idu u više pravaca. Prvo je potrebno razvijati korporativnu bezbednosnu kulturu i politiku, uzimajući u obzir prirodu svih rizika na različitim nivoima. Drugo, potrebno je utvrditi koju vrstu podataka je potrebno zaštiti i na koji način. Treće, potrebno je odabrati odgovarajuće tehnologije i softverska rešenja, odnosno razviti procedure i protokle, kako bi se uspešno suprostavili realnim pretnjama i rizicima. U svakoj logističkoj kompaniji koja posluje na internetu i uz pomoć interneta, trebalo bi da postoji odeljenje koje sprovodi sigurnosnu politiku, obučava zaposlene, održava alate protiv sigurnosnih rizika i ukazuje menadžmentu na sigurnosne pretnje. Potrebno je sprovoditi kontrolu pristupa interentu i komunikacionim servisima, koja podrazumeva uvid u to koji spoljašnji i unutrašnji učesnici mogu da imaju pristup mreži.

Pored toga, potrebno je razvijati odgovarajuće platforme koje će obezbediti efikasno i bezbedno odvijanje tokova informacija između učesnika u lancu snabdevanja. SMART CM platforma koja je razmatrana u ovom radu pruža značajne prednosti u tom pogledu, koje se ogledaju kroz: smanje

troškova (operativnih i investicionih); skraćenje vremena obrade podataka, čekanja i isporuke; poboljšanje produktivnosti, pouzdanosti i fleksibilnosti; povećanje otpornosti lanca snabdevanja; veća zaštita i bezbednost podataka; veća zaštita robe od krađe i krijumčarenja, itd. Da bi platforma bila operativna i njena primena uspešna, mora postojati održivi poslovni model, koji bi obezbedio usluge, koje su od značaja i idu u korak sa tržištem. Potrebno je obezbediti neutralnost platforme, kroz neutralnu organizaciju koja bi je vodila.

Summary

The global supply chain comprises a large number of participants, such as manufacturers, distributors, logistics and transport companies, shippers, border terminals, customs, and the like. A successful connection of all participants in a synchronized chain is not possible without information flows, which provide an efficient flow of information at different levels. The participants generally have their own information systems and, at the same time, they are components of different information and communications networks at the global level. In such business environment, information safety is crucial. This paper discusses the issues of data protection in the global chain of container shipping and delivery. First, requirements such as: transparency, safety, reliability, timeliness, effectiveness and efficiency in the supply chain are analyzed, and then a solution based on the SMART CM platform is proposed. The functional architecture of the platform, the key scenarios to successful implementation and models of functioning through certain blocks and layers are proposed. Message formats and sources of information are defined. Finally, the possibilities and limitations of the platform application from the viewpoint of the most important participants in the chain of container shipping and delivery are presented.

Key words: *Data protection, information safety, supply chain, SMART CM platform*

LITERATURA

1. Banomyong, R., *"The Impact of Port and Trade Security Initiatives on Maritime Supply--Chain Management"*. Pra Chan Road, Thammasat Business School, Thammasat University, Bangkok 10200, Thailand. Marit.Pol.MGMT, January-March 2005, Vol 32, No1, 3-13
2. Bichou K., Bell, M., *Internationalisation and Consolidation of the Container Port*
3. *Industry: Assessment of Channel Structure and Relationships,* Maritime Economics &
4. Logistics, 2007, 9, (35–51
5. Ekwall, D. , *"On analyzing the official statistics for antagonistic threats against transports in EU: a supply chain risk perspective"*. Journal of Transportation Security, Vol. 3, No. 4, pp 213-230, 2010.

6. Handfield, R., Barnhardt, R., & Powell, N.," *Mapping the Automotive Textile Supply Chain: the Importance of Information Visibility",J*ournal of textile and apparel technology and management, 3(4), 1- 19. 2004
7. Kaurin, T., Skakavac, Z., *Značaj digitalne forenzike mobilnih uređaja u otkrivanju i dokazivanju krivičnih dela organizovanog kriminala*, Peta Međunarodna znanstveno-stručna konferencija, Zagreb 2016, str. 58
8. Kaurin T., Kilibarda M., *Informacione i komunikacione tehnologije u globalnim lancima snabdevanja,* Treća međunarodna naučna konferencija Evropska unija – izazovi proširenja i Zapadni Balkan, Banja Luka 2016.
9. Rethmann 2009. Logistics PEOPLE – The Rhenus Group customer magazine, *„How Does the Supply Chain Become Secure?"* No 2. Str. 11.
10. SMART-CM Implementation framework for global container surveillance and control, 2009.
11. http://searchmanufacturingerp.techtarget.com/definition/supply-chain-visibility-
12. http://www.gtnexus.com/solutions/supply-chain-visibility
13. http://www.mepsupplychain.org/supply-chain-visibility/
14. http://www.uncjin.org/Documents/congr10/10e.pdf,

ISSN 0354-9852
Pregledni rad
Overview paper

UDK 534.831(497.6Banja Luka)
DOI 10.7251/AKT1636004S
COBISS.RS-ID 6278424

ODREĐIVANJE INTENZITETA BUKE NA TERITORIJI GRADA BANJA LUKA

DETERMINATION OF NOISE INTENSITY AT THE BANJA LUKA TERITORRY

Ljiljana Stojanović Bjelić[1], Momčilo Bobić, Dragana Nešković, Bogoljub Antonić[2]

Sažetak

Buka u životnoj sredini, ili kako se veoma često zove komunalna buka, definiše se kao buka koju stvaraju svi izvori buke koji se javljaju u čovjekovom okruženju. Glavni izvori komunalne buke su izvore buke na otvorenom prostoru i izvori buke u zatvorenom prostoru. Kontrola buke, odnosno zvuka se mjeri raznim veličinama i jedinicama, ali najčešći je intezitet koji se definiše kao protok energije u jedinici i vremenu i kroz jedinicu površine. Cilj rada je da se na osnovu izvršenih mjerenja nivoa buke na području grada Banja Luka za petomjesečni period analizira odnos ekvivalentnog i vršnog nivoa buke u životnoj sredini i izvrši poređenje intenziteta buke prema zakonskoj regulativi.

Ključne riječi: *grad Banja Luka, buka, intenzitetet*
JEL klasifikacija: K32

UVOD

Prisutna buka negativno utiče na psihološko stanje, a može biti i uzrok ostećenja sluha. Najizraženija je u velikim gradovima gdje je gust intenzivni saobraćaj. Buka nastaje i u radnoj sredini, poslovnim i stambenim zgradama pa podjednako ugrožava na otvorenom i u zatvorenom prostoru. Ugradnjom savremenih zvučnoizolacionih materijala buku u objektima možemo bitno smanjiti ili potpuno prigušiti, s time se postiže viši komfor, bolji radni uslovi i zdravije okruženje. Na mjestu prijemnika buka se doživljava kao problem

1 Doc. dr Ljiljana Stojanović Bijelić, Panevropski univerzitet "Apeiron" Banja Luka
2 Prof. dr Bogoljub Antonić, Fakultet zdravstvenih nauka

ukoliko su nivoi buke visoki ili ukoliko remeti osnovne ljudske aktivnosti: rad, odmor i spavanje.

METOD RADA

Na osnovu izvršenih mjerenja nivoa buke na području grada Banja Luka za period: 02, 03, 08, 11. i 12.02.2016. godine izvršena je analiza odnosa ekvivalentnog i vršnih nivoa buke u životnoj sredini za dnevni period 6-22h (8 h mjerenja po mjernom mjestu u 15 minutnim intervalima) na 5 lokacija (mjerna mjesta 1-5) i noćni period 22-06h (8 h mjerenja po mjernom mjestu u 15 minutnim intervalima) na 5 lokacija (mjerna mjesta 1-5). Na osnovu dobijenih rezultata prema zakonskoj regulativi i akustičnom opterećenju grada Banjaluka tj. Pravilnikom o dozvoljenim granicama intenziteta zvuka i šuma („Službeni list SRBiH" br. 46/89 definisani su dominantni izvori buke u životnoj sredini i tačke čije mjerne vrijednosti najviše odstupaju od propisanih dozvoljenih vrijednosti u analiziranom periodu mjerenja. Lokacije na kojima je mjeren nivo komunalne buke na području Grada Banja Luka su:

1. Mjerno mjesto 1. - raskrsnica Ul. Trive Amelice i Ul. Krajiških brigada (Rosulje),
2. Mjerno mjesto 2. - raskrsnica Ul. Gundulićeva i Bulevar Vojvode Radomira Putnika (Borik),
3. Mjerno mjesto 3. - raskrsnica Ul. Cara Lazara i Ul. Stepe Stepanovića (Obilićevo),
4. Mjerno mjesto 4. - „kružna" raskrsnica (Lauš),
5. Mjerno mjesto 5. - „parking" površina na raskršću Bulevara cara Dušana i Kralja Petra I Karađorđevića ("Centar").

Slika 1 Lokacije mjerenja komunalne buke na području grada Banja Luke

Mjerno mjesto br. 1 (GPS 44°47'8.60"N 17°11'46.48"E) nalazi se u naselju Rosulje, u blizini ukrštanja saobraćajnica (Ul. Trive Amelice i brzog puta E661). Mjerenje je izvršeno na otvorenoj površini na udaljenosti cca 10 m od ivice najbliže saobraćajnice.

Slika 2 Uža lokacja mjernog mjesta br. 1.

Tabela 1 Rezultati mjerenja buke na mjernom mjestu br. 1.

Mjerno mjesto	Rosulje (raskrsnica ul. Trive Amelice i ul. Krajiških brigada)
Datum mjerenja	02/03.02.2016. god.

Analizirani period (15 min.)	Mjerni interval	Mjerna veličina	Izmjerena vrijednost dB(A)	Najviši dozvoljeni nivo dB(A)	Područje (zona)	Meteorološki Parametri
Dan (06-22 h)	0914-0929h	Leq	60.4	60	IV*	T=70C rH=77% Vv=4.5m/s
		L10	79.9	70		
		L1	83.6	75		
Dan (06-22 h)	1529-1544h	Leq	66.1	60	IV*	T=310C rH=31% Vv=2.6m/s
		L10	96.8	70		
		L1	105.4	75		
Dan (06-22 h)	1829-1844h	Leq	59.4	60	IV*	T=310C rH=31% Vv=2.6m/s
		L10	78.2	70		
		L1	81.8	75		
Noć (22-06 h)	0115-0130h	Leq	49.2	50	IV*	T=110C rH=70% Vv=6.5m/s
		L10	70.4	70		
		L1	78.2	75		
Noć (22-06 h)	0430-0445h	Leq	54.7	50		T=190C rH=68% Vv=1.0m/s
		L10	88.0	70		
		L1	95.2	75		

Leq - ekvivalentni nivo buke

L10 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 10% vremena mjerenja

L1 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 1% vremena mjerenja

* - područje grada nije akustički zonirano

Mjerno mjesto br. 2 (GPS 44°46'16.08"N 17°11'56.48"E) nalazi se u naselju Borik, u blizini ukrštanja saobraćajnica (Ul. Gundulićeva i Bulevar Vojvode Radomira Putnika). Mjerenje je izvršeno na otvorenoj površini na udaljenosti cca 10 m od ivice najbliže saobraćajnice.

Slika 3 Uža lokacija mjernog mjesta br. 2

Tabela 2 Rezultati mjerenja buke na mjernom mjestu br. 2.

Mjerno mjesto	Borik (raskrsnica Ul. Gundulićeva i Bulevar Vojvode Radomira Putnika)					
Datum mjerenja	08/09.02.2016. god.					
Referentni period (15 min.)	Mjerni interval	Mjerna veličina	Izmjerena vrijednost dB(A)	Najviši dozvoljeni nivo dB(A)	Područje (zona)	Meteorološki Parametri
Dan (06-22 h)	0828-0843h	Leq	67.6	60	IV*	T=140C rH=52% Vv=18m/s
		L10	84.6	70		
		L1	94.5	75		
Dan (06-22 h)	1614-1629h	Leq	81.5	60	IV*	T=310C rH=31% Vv=2.6m/s
		L10	92.7	70		
		L1	93.6	75		
Dan (06-22 h)	2044-2059h	Leq	73.1	60	IV*	T=310C rH=31% Vv=2.6m/s
		L10	90.5	70		
		L1	94.1	75		
Noć (22-06 h)	0200-0215h	Leq	57.6	50	IV*	T=80C rH=80% Vv=7.0m/s
		L10	69.4	70		
		L1	77.4	75		

Noć						
(22-06 h)	0530-0545h	Leq	66.3	50		T=190C
rH=68%						
Vv=1.0m/s						
L10	76.2	70				
L1	85.1	75				

Leq- ekvivalentni nivo buke

L10 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 10% vremena mjerenja

L1 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 1% vremena mjerenja

* - područje grada nije akustički zonirano

Mjerno mjesto br. 3 (GPS 44°45'39.22"N 17°11'32.42"E) nalazi se u naselju Obilićevo, u blizini ukrštanja saobraćajnica (Ul. Cara Lazara i Ul. Stepe Stepanovića). Mjerenje je izvršeno na otvorenoj površini na udaljenosti cca 5 m od ivice najbliže saobraćajnice. Od važnijih objekta na užoj lokaciji, koji su ugroženi vanjskom bukom može se izdvojiti objekat Javne ustanove za predškolsko vaspitanje (vrtić „Buba-mara").

Slika 4 Uža lokacija mjernog mjesta br. 3

Tabela 3 Rezultati mjerenja buke na mjernom mjestu br. 3

Mjerno mjesto	Obilićevo (raskrsnica Ul. Cara Lazara i Ul. Stepe Stepanovića)					
Datum mjerenja	03/04.02.2016. god.					
Referentni period	Mjerni interval					
(15 min.)	Mjerna veličina	Izmjerena vrijednost dB(A)		Najviši dozvoljeni nivo dB(A)	Područje	
(zona)	Meteorološki					
Parametri						
Dan						
(06-22 h)	1044-1059h	Leq	75.0	60	IV*	T=100C
rH=88%						
Vv=4.5m/s						
L10	82.1	70				
L1	87.6	75				
Dan						
(06-22 h)	1700-1715h	Leq	76.3	60	IV*	T=310C
rH=31%						
Vv=2.6m/s						

L10 83.6	70					
L1 88.7	75					
Dan						
(06-22 h)	2129-2144h	Leq	82.9	60	IV*	T=310C
rH=31%						
Vv=2.6m/s						
L10 88.9	70					
L1 98.4	75					
Noć						
(22-06 h)	0145-0200h	Leq	75.9	50	IV*	T=30C
rH=93%						
Vv=8m/s						
L10 78.6	70					
L1 90.9	75					
Noć						
(22-06 h)	0415-0430h	Leq	69.7	50		T=190C
rH=68%						
Vv=1.0m/s						
L10 70.8	70					
L1 85.5	75					

Leq - ekvivalentni nivo buke

L10 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 10% vremena mjerenja

L1 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 1% vremena mjerenja

* - područje grada nije akustički zonirano

Mjerno mjesto br. 4 (GPS 44°46'17.65"N 17°10'52.48"E) nalazi se na ulazu u naselje Lauš, u blizini kružnog toka saobraćaja (Brzi put E661 i Bulevar Cara Dušana). Mjerenje je izvršeno na otvorenoj površini-parkingu na udaljenosti cca 10 m od navedenog kružnog toka saobraćaja. Od važnijih objekta na posmatranoj lokaciji nalazi se sportsko rekreativna površina (igralište), objekat „Banjalučke gimnazije" te objekat „Zavoda za transfuziju Banja Luka".

Slika 5 Uža lokacija mjernog mjesta br. 4.

Tabela 4 Rezultati mjerenja buke na mjernom mjestu br. 4.

Mjerno mjesto	Lauš (parking površina kod „kružne" raskrsnice)
Datum mjerenja	11/12.02.2016. god.
Referentni period	Mjerni interval

(15 min.) Mjerna veličina Izmjerena vrijednost dB(A) Najviši dozvoljeni nivo dB(A) Područje (zona) Meteorološki Parametri

Dan (06-22 h) rH=68% Vv=6.5m/s	0930-0945h	Leq	72.2	60	IV*	T=60C
		L10	83.7	70		
		L1	90.9	75		
Dan (06-22 h) rH=31% Vv=2.6m/s	0130-0145h	Leq	69.5	60	IV*	T=310C
		L10	83.5	70		
		L1	89.8	75		
Dan (06-22 h) rH=31% Vv=2.6m/s	2030-2045h	Leq	66.8	60	IV*	T=310C
		L10	80.2	70		
		L1	85.0	75		
Noć (22-06 h) rH=97% Vv=7m/s	0115-0130h	Leq	60.0	50		T=00C
		L10	71.4	70		
		L1	79.9	75		
Noć (22-06 h) rH=68% Vv=1.0m/s	0515-0530h	Leq	66.1	50		T=190C
		L10	79.1	70		
		L1	86.5	75		

Leq - ekvivalentni nivo buke

L10 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 10% vremena mjerenja

L1 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 1% vremena mjerenja

* - područje grada nije akustički zonirano

Mjerno mjesto br. 5 (GPS 44°46'5.34"N 17°11'16.37"E) nalazi se na ulazu u centru grada Banja Luka, u blizini ukrštanja saobraćajnica (Kralja Petra I Karađorđevića i Bulevar Cara Dušana). Mjerenje je izvršeno na otvorenoj površini-parkingu na udaljenosti cca 10 m od najbliže saobraćajnice. Na užoj lokaciji prisutni su većinom poslovni objekti: trgovačke i zanatske radnje, gradska „tržnica", stambene zgrade, zatim jedan vjerski objekat u izgradnji (džamija „Ferhadija").

Slika 6 Uža lokacija mjernog mjesta br. 5.

Tabela 5 Rezultati mjerenja buke na mjernom mjestu br. 5.

Mjerno mjesto	„Centar" - parking površina kod raskrsnice Bulevar cara Dušana i Kralja Petra I Karađorđevića					
Datum mjerenja	12/13.02.2016. god.					
Referentni period (15 min.)	Mjerni interval	Mjerna veličina	Izmjerena vrijednost dB(A)	Najviši dozvoljeni nivo dB(A)	Područje (zona)	Meteorološki Parametri
Dan (06-22 h)	0800-0815h	Leq	70.2	60	IV*	T=70C rH=80% Vv=7.5m/s
		L10	82.8	70		
		L1	85.0	75		
Dan (06-22 h)	1415-1430h	Leq	72.2	60	IV*	T=310C rH=31% Vv=2.6m/s
		L10	84.3	70		
		L1	90.0	75		
Dan (06-22 h)	2100-2115h	Leq	69.3	60	IV*	T=310C rH=31% Vv=2.6m/s
		L10	81.5	70		
		L1	85.7	75		
Noć (22-06 h)	0001-0016h	Leq	53.4	50	IV*	T=50C rH=95% Vv=7.0m/s

L10	76.2	70				
L1	79.1	75				
Noć						
(22-06 h)	0405-0420h	Leq	51.3	50		T=190C
rH=68%						
Vv=1.0m/s						
L10	70.4	70				
L1	78.6	75				

Leq - ekvivalentni nivo buke

L10 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 10% vremena mjerenja

L1 - nivo buke koji ilustruje prisustvo buke viših nivoa u trajanju od 1% vremena mjerenja

* - područje grada nije akustički zonirano

REZULTATI ISTRAŽIVANJA

Kao dominantani izvor buke na posmatranim lokacijama je saobraćajna buka. Pred buke od motornih vozila koja saobraćaju gradskim saobraćajnicama nemoguće je takođe bilo isključiti uticaj buke stvorene od ugostiteljskih i trgovački objekata, aktivnosti komunalnih službi i službi za održavanje zelenih površina kao i drugih aktivnosti u neposrednoj blizini mjernih mjesta (aktivnosti stanovništva koje boravi u stambenim objektima ili radi u poslovnim objektima). Na lokacijama mjerenja postoji veliki broj stambenih i poslovnih objekata u kojima ljudi borave. Okolni stambeni objekati su uglavnom veće spratnosti i čvrste građevinske konstrukcije. Na njima se nalazi veliki broj svijetlih otvora (prozori i vrata).

U cilju dobijanja pravog stanja nivoa komunalne buke koja djeluje na stambene jedinice dobijeni rezultati mjerenja buke su u skladu sa članom 4. stav 1. Pravilnika o dozvoljenim granicama intenziteta zvuka i šuma (Sl.list SRBiH broj 46/89).

1. Izmjerene vrijednosti ekvivalentnog nivoa buke na mjerno mjesto br. 1. u naselju Rosulje:

- za dnevne mjerne intervale iznosi 60.40 dB (A), 66.10 dB (A) i 59.40 dB (A),
- za noćne mjerne intervale iznosi 49.20 dB (A) i 54.70 dB (A).

2. Izmjerene vrijednosti ekvivalentnog nivoa buke na mjerno mjesto br. 2. u naselju Borik:

1. za dnevne mjerne intervale iznosi 67.60 dB (A), 81.50 dB (A) i 73.10 dB (A),

- za noćne mjerne intervale iznosi 57.60 dB (A) i 66.3 dB (A).

3. Izmjerene vrijednosti ekvivalentnog nivoa buke na mjerno mjesto br.3 u naselju Obilićevo:

- za dnevne mjerne intervale iznosi 75.00 dB (A), 76.30 dB (A) i 82.90 dB (A),
- za noćne mjerne intervale iznosi 75.90 dB (A) i 69.70 dB (A).

4. Izmjerene vrijednosti ekvivalentnog nivo buke na mjerno mjesto br.4 na početku naselja Lauš:

- za dnevne mjerne intervale iznosi 72.20 dB (A), 69.50 dB (A) i 66.80 dB (A),
- za noćne mjerne intervale iznosi 60.00 dB (A) i 66.1 dB (A).

5. Izmjerene vrijednosti ekvivalentnog nivoa buke na mjernom mjestu br. 5. u centru grada:

- za dnevne mjerne intervale iznosi 70.20 dB (A), 72.20 dB (A) i 69.30 dB (A),
- za noćne mjerne intervale iznosi 53.40 dB (A) i 51.30 dB (A).

Izmjerene vrijednosti ekvivalentnog nivoa buke na svim mjernim pozicijama u većem broju mjerenja prelaze najviši dozvoljeni nivo za IV akustičnu zonu određenu Pravilnikom o dozvoljenim granicama intenziteta zvuka i šuma („Službeni list SRBiH" br. 46/89). Jedino na mjernom mjestu broj 1. naselje Rosulje dva mjerenja su bila ispod dozvoljenih granicama intenziteta zvuka i šuma.

ZAKLJUČAK

U ovom radu prikazana su odstupanja na osnovu izmjerenih vrijednosti ekvivalentnog nivoa buke na mjernim mjestima od 1 do 5. U gore navedenim tabelama dobijene vrijednosti koje prelaze najviši dozvoljeni nivo za IV akustičnu zonu određenu Pravilnikom o dozvoljenim granicama intenziteta zvuka i šuma („Službeni list SRBiH" br. 46/89) su označene crvenom bojom, dok su ostale izmjerene vrijednosti u granicama intenziteta zvuka i šuma („Službeni list SRBiH" br. 46/89). Ustanovljena su odstupanjana na osnovu izvršenih mjerenja nivo buke na području grada Banja Luka. Ocjenjen je nivo buke prema zakonskoj regulativi i ustanovljeno akustično opterećenje grada Banjaluka, čime su utvrđene tačke čije mjerne vrijednosti najviše odstupaju od propisanih dozvoljenih vrijednosti u analiziranom periodu mjerenja. Potrebno je da grad Banja Luka obezbjedi 24-časovno mjerenje intenziteta buke pomoći

Grad Banja Luka je poslednjih decenija opterećen bukom, koja se povećava nekoliko decibela godišnje. Gradsku buku sačinjava haotični zbir zvuko-

va koji potiču od različitih i mnogobrojnih izvora, a koji se međusobno razlikuju po visini, intenzitetu i trajanju. Najveći uzročnik komunalne buke je saobraćaj sa oko 80%, a ostali izvori kao što su industrija, ugostiteljski objekti, ulična buka različitog porijekla i buka u domaćinstvima su zastupljeni u manjoj mjeri. Zaštita i unapređenje životne sredine, kao i strategijsko opredeljenje za zdravu životnu sredinu, podrazumijeva sprovođenje određenih aktivnosti za stvaranje lokalne strategije za zaštitu i unapređenje životne sredine. Lokalna strategija iskazana preko Lokalnog ekološkog akcionog plana treba da ukaže na sve aspekte životne sredine koji narušavaju zdravu životnu sredinu, kao i na neophodne korake koje treba preduzeti za eliminisanje negativnih efekata savremenog razvoja civilizacije na životnu sredinu, a samim tim i smanjenje buke. Mapiranje buke je suštinski dio kontinuiranog praćenja stanja i efektivnog upravljanja bukom u životnoj sredini. Cilj akustičkih mapa je da slikovito prikažu stanje buke vlastima i građanima, tako da mogu zajedno da utiču na smanjenje broja ljudi koji su izloženi prekomjernoj buci. Za postizanje kvalitetne zaštite od buke potrebno je u samom početnom projektovanju stambene zgrade odrediti najbolju poziciju i izgled zgrade kao i postaviti najbolju izolaciju od buke kojom će se smanjiti mogućnost prodora zvučnih talasa u stambenu zgradu. Povoljan položaj u odnosu na saobraćajnicu kao i ostale izvore buke koji se javljaju u okolini stambene zgrade, takođe, smanjuje mogućnost prodora zvučnih talasa u prostorije. U samom projektu stambene zgrade poželjno je sobe za odmor projektovati tako da budu pozicionirane što dalje od izvora buke. Potrebno je postaviti dobru izolaciju vrata i prozora tako da oko te izolacije ne postoje otvori kroz koje bi prolazili zvučni talasi.

Abstract

Noise in the environment, or how often called communal noise is defined as noise created by all sources of noise that occur in the human environment. The main sources of noise pollution are sources of noise in the open air and noise sources indoors. Control of noise and sound is measured and units of various sizes, but the most common is the intensity of which is defined as the energy flow per unit and time through unit area. The aim is that on the basis of measurements of noise levels in the city of Banja Luka for the five-month period to analyze the relationship equivalent and peak noise levels in the environment and a comparison to the intensity of the noise legislation.

***Key words**: city of Banja Luka, noise, intenzitetet*

LITERATURA

1. Ratko Uzunović,R.Albijanić.: Zaštita okoline od buke i vibracija, Beograd, 1981
2. Praščević,M. Cvetković, D.: Buka u životnoj sredini, Fakultet zaštite na radu u Nišu, Niš, 2005
3. Veličković, D.: Buka i Vibracije 2, Fakultet zaštite na radu u Nišu, Niš, 1990
4. D. Cvetković, M. Praščević: BUKA I VIBRACIJE „zbirka rješenih zadataka sa teorijskim osnovama", Niš, 1999. God.
5. Lokalni ekološki akcioni plan (LEAP) za Banja Luku, Banja Luka, 2009. God.
6. M. Jevtić: Buka i zdravlje, značaj akcionih planova, Ministarstvo zdravlja Republike Srbije, 2012. God.
7. Lj. Stojčić, M. Nikolić: Zdravstveni aspekt mjerenja komunalne buke i značaj za građevinarstvo,Niš, 2009. God.
8. M. Aranđelović, J. Jovanović: Medicina rada, Univerzitet u Nišu, 2009. God.
9. M. Rogač, M. Nikić: Uticaj buke železničkog saobraćaja na životnu sredinu, Podgorica, 2010. God
10. Probus GRUPA, http://www.pce-grupa.rs

ISSN 0354-9852
Prikaz časopisa
Journal overview

UDK 792:050AGON(049.32)
DOI 10.7251/AKT1636005C
COBISS.RS-ID 6278680

PRIKAZ ČASOPISA AGON

Ljiljana Čekić[1]

JEL klasifikacija: Y30

Једини часопис на босанско-херцеговачком, па самим тим и на простору Републике Српске, који се бави анализом и опсервацијом позоришног живота, али и визуелних комуникација, „Агон", у континуитету излази из штампе већ пет година у издању Народног позоришта Републике Српске и Академије умјетности Универзитета у Бањој Луци.

Структура часописа је чврсто и јасно постављена дкако би обухватила најразличитије области позоришног стваралаштва, па самим тим и истраживања. Временом, ово устројство доживљавало је извјесне модификације, као и сваки живи организам, али је основни образац часописа остао у оквирима првобитно дефинисаног.

Специфичност овог часописа није у његовој структури која у значајној мјери преузима модел старијих публикација сличног профила, него у његовој актуелности и ширини која је дефинисана и у самом поднаслову (позоришне и визуелне комуникације). Тематске цјелине које су диференцирале часопис представљају оквире унутар којих истраживачи и текстови проналазе свој простор. Базична поглавља („Из историје и теорије позоришта", „Филм", „Глума", „Медији", „Фестивали", „Прикази", „Драма" „Луткарство", и др.) у својој бројној комбинаторици, уз додавање специфичних тематикума стварају особеност естетског оквира сваког појединачног броја.

Посљедњи, осми број ове публикације, који је из штампе изишао у другој половини 2016. године, у значајном обиму упознаје читалачки аудиторијум са радовима који су излагани на стручно-научном скупу „Каква је будућност театра? – Продукција савременог театра", који је одржан 24. маја у оквиру XIX Театар феста Петар Кочић 2016. године у Бањој Луци, у организацији Народног позоришта Републике Српске, Академије умјетности Бања Лука и високошколске установе „Бањалука колец".

1 Др Љиљана Чекић, Народно позориште Републике Српске

Поводом стогодишњице смрти највећег крајишког писца Петра Кочића, др Лука Кецман, замјеник главног и одговорног уредника „Агона" је дао кратак осврт на значај Кочићевог дјела са становишта теорије књижевности акцентујући театарску димензију његове прозе, као и његову неисцрпну инспитаривност мотива и тема у поступцима транспоновања прозног текста у драму. Кецман антиципира и отвара нова тумачења Кочићевог опуса у свјетлу европске драмске литературе, али и филмске умјетности.

У тематском дијелу публикације, која доноси радове са претходно поменутог скупа објављено је девет текстова аутора који су из диспаратних театарских визура анализирали позоришну продукцију времена у коме живимо и оног које тек долази.

Небојша Брадић, позоришни редитељ се у својој језгровитој и емпиријски потврђеној анализи „Време је за културу" осврће на немогућност тржишногфункционисања културе иронизирајући „памет маса" и констатујући да су умјетност и хуманистичке науке области људског дјеловања на које није могуће примјењивати законе тржишног неолиберализма. Објашњавајући значај институција као незаобилазног ослонца у финансирању умјетничког стваралаштва он покушава да објасни важност балансирања између државе и идеологије са једне и умјетности и експертске анализе са друге стране у процесу валоризације умјетничких дјела која би требало да буду субвенционисана.

Полазећи од констатације да је позориште у кризи (а када није?) и дијагностикујући узроке таквог стања др Зоран Ђерић у тексту „Од кризе позоришта до позоришта кризе, ка позоришту нове драматургије" даје прецизну слику савременог театра и његовог урушавања јасно се реферишући на теоријске анализе значајних свјетских театролога (Патрис Павис, Дерек Пецет, Жан Бодријар и др.). Кратком ретроспективом доминантних позоришних естетика током вишемиленијумског развоја европског позоришта и концизним појашњењем драматургија које на различите начине егзистирају у савременом позоришном простору, од оних које се могу пронаћи само још у рецидивима до оних чији долазак на сцену тек предстоји, професор Ђерић покушава да иницира конзистентну систематизацију драматургије као научне дисциплине на српском језичком простору.

Др Наташа Глишић, у свом раду „Театрализација реалних искустава као изазов савременог (документарног) позоришта" покушава да пронађе одговор на питање који су коријени варбатим театра на нашим просторима и у чему је тајна његове распрострањености и популарности у свјетлу савремених друштвених и политичких догађања, бавећи се на тај начин актуелном социологијом позоришта. Полазећи од историјских почетака

документаристичког театра професор Глишић расвјетљава генезу развоја вербатим позоришта и врши реконструкцију процеса настанка овог облика театарског стваралаштва проналазећи упориште своје анализе у двјема београдским представама које је бањалучка публика имала прилику да види у свом граду.

Улазећи у највећи и најкомплекснији, али и највише проучаван позоришни простор, простор стваралаштва и живота Виљема Шекспира др Александар Саша Грандић је храбро закорачио у подручје на које готово сваки мислећи човјек полаже своје право на власништво, познавање и тумачење. Тежак и незахвалан задатак, али велики истраживачки изазов. Иако сам назив „Савременост Шекспирове комедије у контексту продукције савременог позоришта" аутору омеђава истраживачко поље, др

Грандић проширује област свог интересовања наводећи мноштво фактографских података из живота и професионалног рада Барда са Ејвона које наводи у самом раду.

„Избор продукционог тима у аудио-визуелном пројекту" др Милоша Бабића представља кратки туторијал за избор пројектног руководиоца и формирање пројектне екипе која би посједовала компетенције за реализацију сложених продукцијских задатака.

Ретроспективу најстаријег позоришног фестивала Републике Српске од његовог оснивања до данашњих дана изложио је др Раде Симовић у свом тексту „Продукција фестивала монодрама Српске – Фестивал малих сцена (1995 – 2015)". Као активни учесник у креирању организационе структуре, али и естетског идентитета фестивала који је свој животни вијек отпочео у ратном окружењу, др Симовић свједочи бурну историју ове културне манифестације. Уз мноштво података којима аутор располаже у тексту се цитирају и дијелови докумената који представљају ријетко сачувану архивску грађу.

Не губећи из вида основну мисао водиљу др Бранко Брђанин је, попут одличног ученика својим текстом "Праизвједба на репертоару, изазови и искушења продукције" одговорио на задану тему Научног скупа, дајући виђење театарске будућности из визуре позоришног драматурга, драмског писца, али и дугогодишњег умјетничког директора Народног позоришта Републике Српске. Убацујући у жрвањ своје анализе тему Скупа, др Брђанин даје историјски преглед значаја постављања националне драме на репертоар националног театра ослањајући се на латинску максиму Cuius panem edo, eius carmine cuneo (Чији хљеб једем, његову пјесму пјевам). Користећи методу студије случаја аутор анализира два драмска текста савремених српских писаца (Б. Шпањевић, Б. Чучак) и њихову сценску (не)реализацију.

Још један рад настао као резултат поменутог скупа „Прилагођавање институција културе условима рада у транзиционим друштвима“ др Ненада Новаковића пружа читаоцу слику тренутне организационе структуре институција културе Републике Српске и нуди једно од могућих рјешења њене квалитетне реорганизације.

Сандра Баришић својим радом „Значај индивидуалних слобода у савременој продукцији и естетици“ апострофира значај позоришне продукције приписујући јој најодговорнију позицију у позоришном стваралаштву дајући јој примат над умјетничким професијама, чиме је заокружено поглавље часописа у коме су публиковани радови са Научног скупа „Каква је будућност театра? – Продукција савременог театра“.

У цјелини која носи назив „Теорија“ објављена су два рада младих истраживача који на различите начине третирају драмски опус тројице најзначајнијих америчких драмских писаца.

Маска као сценски костим, али и као реквизита егзистира подједнако дуго као и само позориште и представља предмет истраживања мр Наташе Вученовић у тексту под називом „Употреба маски у модерном америчком позоришту у драмама Јуџина О’Нила“. Ауторка даје историјски преглед употребе позоришних маски компарирајући њихово значење у различитим историјским епохама. Као три главна временска и естетска упоришта своје анализе мр Вученовић одабира античку драму, средњевијековне моралитете и драме Јуџина О’Нила, студиозно се бавећи употребом маски у драмамаовог Нобеловца и најзначајнијег представника америчког психолошког реализма.

На фону претходног рада Зоран Тодоровић публикује свој текст „Драме Тенеси Вилијамса и Едварда Олбија на сцени Народног позоришта Републике Српске“. Враћајући се у прошлост најстаријег крајишког позоришта Тодоровић читаоцу пружа на увид присутност америчке драме на репертоару овог театра од његовог оснивања до данашњих дана. Информишући, али и доцирајући читалачку публику млади истраживач тежиште своје анализа ставља на двије представе „Ко се боји Вирџиније Вулф“ и „Трамвај звани жеља“ које су на бањолучкој сцени одигране прије десет, односно петнаест година.

Др Љиљана Чекић у тексту под називом „Сваштара кућног драматурга“ даје приказ књиге др Бранка Брђанина „Драма и позорница у Бањој Луци“ наглашавајући да велики број података уз прецизну мисао и јасну реченицу, уз неколицину духовитих синтагми са нескривеном енергијом и личним печатом аутора, ова књига може представљати занимљиво штиво за разнородан читалачки аудиторијум.

Према устаљеној структури часописа посљедње странице су намјењене драмама савремених писаца које до сада није публикована нити јавно

извођена. У осмом броју „Агона“ објављена је драма Синише Ковачевића „Учитељица“ коју је значајни српски драмски писац написао током 2014. године.

У мноштву текстова различитих по својој темеатици, обиму истраживања, али и квалитету „Агон“ представља часопис који лако проналази пут до својих читалаца, од оних којима је потребна подука о базичним питањима из теорије позоришне умјетности и визуелних комуникација до експерата који су заинтересовани за најновија истраживања својих колега.