



SPCSJ

**SCIENTIFIC AND PRACTICAL
CYBER SECURITY JOURNAL**

VOL4 No2
JUNE 2020

ISSN 2587-4667

RISK EVALUATION IN INFORMATION SYSTEMS USING PROBABILISTIC MODEL

Ajit Singh Department of Computer Science, Patna Women's College Bihar, INDIA

ABSTRACT: The paper constructs continuous and discrete distribution laws, used to assess risks in information systems. Generalized expressions for continuous distribution laws with maximum entropy are obtained. It is shown that in the general case the entropy depends also on the type of moments used to determine the numerical characteristics of the distribution law. Also, probabilistic models have been developed to analyze the sequence of independent trials with three outcomes. Expressions for their basic numerical characteristics are obtained, as well as for calculating the probabilities of occurrence of the corresponding events.

KEYWORDS: *information system, distribution, risk, random variable.*

1. INTRODUCTION

At the present stage of the development of society, which is characterized by the intensive introduction of information systems in virtually all areas of activity, issues related to the assessment of the risks that occur during their operation are of particular importance. When analyzing and assessing risks, issues related to the definition of distribution laws are of the greatest importance. The given work is devoted to questions of construction of distribution laws.

In the modeling of information systems, risk is a random variable and is described by a probability distribution on a given set [1-3]. In contrast to experiments conducted in physics, where there is a possibility of their multiple conduct, the conditions of the functioning of information systems are characterized by a constant impact of negative external influences and are constantly changing [4], and consequently the repetition of the experiment under the same conditions is practically impracticable. The laws of probability distribution of risk events, as a rule, do not correspond to the law of the normal Gaussian distribution [5-6].

2. CONSTRUCTION OF CONTINUOUS DISTRIBUTION LAWS WITH THE MAXIMUM ENTROPY

Entropy coefficient is often used [7-8] with the classification of distribution laws of random continuous value (RV) with number characteristics.

$$\delta_e = \frac{1}{2\sigma} \exp(H) \quad (1)$$

In the formula (1) $\sigma = \sqrt{\mu_2}$ is standard deviation, and μ_2 is the second central power moment for this distribution law; value H – entropy, which is defined by the definition:

$$H = - \int_{-\infty}^{\infty} p(x) \ln(p(x)) dx, \quad (2)$$

$p(x)$ – density of probability distribution (PDD) SV. Entropy coefficient has the maximum value for Gaussian law ($\delta_e = 2.066$), for uniform law - $\delta_e = 1.73$, for Koshi distribution - $\delta_e = 0$ etc.

The entropy value does not depend on shift parameter, to simple computation let's consider, that it is equal to zero. Firstly we need to find distribution law from unilateral laws of distribution of unlimited RV, for which entropy value H (2) reaches the maximum with the following limitations, imposed on probability density $p(x)$:

$$p(x) \geq 0, \int_0^{\infty} p(x) dx = 1, \int_0^{\infty} x^v p(x) dx = \beta^v / v, \quad (3)$$

where β – scale parameter; v – value of maximum existing primary direct moment. Here and next we'll consider positive power moment as a direct moment in accordance with (3), and negative power moment as a reverse moment.

To find the extremum we'll use the method of indefinite Lagrange multipliers [9]. We need to maximize:

$$\int_0^{\infty} [-p(x) \ln(p(x)) + \lambda_1 p(x) + \lambda_2 x^v p(x)] dx \quad (4)$$

inserting Lagrange multipliers λ_1 and λ_2 , considering the limitations (3) and must be defined. Equating the result of variation integrand expression in (4) when $p(x) = 0$, we'll take the equation relatively to $p(x)$:

$$-\ln(p(x)) - 1 + \lambda_1 + \lambda_2 x^v = 0. \quad (5)$$

So, the density $p(x)$, which satisfies (3) and maximizes H , can be found from the equation (5)

$$p(x) = \exp(\lambda_1 - 1 + \lambda_2 x^v). \quad (6)$$

Substituting (6) in (3) instead of $p(x)$, we'll take from integrating:

$$\begin{aligned} \exp(\lambda_1 - 1) \frac{\Gamma(1/v)}{v(-\lambda_2)^{1/v}} &= 1, \\ \exp(\lambda_1 - 1) \frac{\Gamma(1/v)}{v(-\lambda_2)^{1+1/v}} &= \beta^v / v. \end{aligned} \quad (7)$$

From (7) we find, that $\lambda_2 = -1/\beta^v$, $\exp(\lambda_1 - 1) = v/(\beta \Gamma(1/v))$. Consequently

$$p(x) = \frac{\nu}{\beta \Gamma(1/\nu)} \exp\left(-\frac{x^\nu}{\beta^\nu}\right), \quad 0 < x < \infty, \quad (8)$$

where $\tilde{A}(z)$ gamma function.

From (8) follows, that if exists only the first beginning direct moment ($\nu = 1$), then exponential law has the maximum entropy; if there are two moments ($\nu = 2$), then unilateral Gaussian law; and if all direct moments exist ($\nu \rightarrow \infty$), then unilateral uniform law. Indeed, the limiting moment (8) with ($\nu \rightarrow \infty$) is a unilateral uniform law $p(x) = \beta^{-1}$, $0 < x < \beta$. So, if all direct moments exist, then uniform law has the maximum entropy from unilateral distribution laws of RV.

Analogically for bilateral symmetry laws of distribution unlimited RV can be shown, that if the first ν of absolute central direct moments, then the probability density has the maximum entropy:

$$p(x) = \frac{0.5\nu}{\beta \Gamma(1/\nu)} \exp\left(-\frac{|x|^\nu}{\beta^\nu}\right), \quad -\infty < x < \infty. \quad (9)$$

From (9) follows, that if only first absolute central moment exists ($\nu = 1$), then Laplace distribution has the biggest entropy; if there are two moments ($\nu = 2$), then Gaussian law; and if all direct moments exist ($\nu \rightarrow \infty$), then uniform law. Indeed, the limiting case for (9) is a uniform law $p(x) = 0,5\beta^{-1}$, $-\beta < x < \beta$. So, if all direct moments exist, then uniform law has the biggest entropy from bilateral symmetry distribution laws of RV. Considered private cases of bilateral laws with the maximum entropy coincide with already known laws (Laplace and Gaussian), which have maximum entropy, that confirms the correctness of received results.

From analysis of received expressions (8) and (9) follows, that for increasing the amount of information about evaluating parameters of distribution laws with big length (with long tails) with the help of a method of moments is necessary to use direct moments of lesser order, including fractional order. If the parameters of distribution laws lesser length are used, then it is necessary to use direct moment of higher order.

Let's find from unilateral distribution laws of unlimited RV such distribution law, with which entropy value H reaches maximum with the following limitations, imposed on probability density $p(x)$:

$$\begin{aligned} p(0) &= 0, p(x) \geq 0, \\ \int_0^\infty p(x) dx &= 1, \int_0^\infty x^{-\nu} p(x) dx = \beta^\nu / \nu, \end{aligned} \quad (10)$$

where ν value of maximum existing beginning reverse moment. Considering this an entropy is defined by an expression:

$$H = - \int_0^{\infty} y^{-2} p(1/y) \ln(y^{-2} p(1/y)) dy = - \int_0^{\infty} p(x) \ln(x^2 p(x)) dx, \quad (11)$$

where $y^{-2} p(1/y)$ - a probability density RV η , which is reverse to ξ , which has the probability density $p(x)$. As a result of using the method of indefinite Lagrange numerators we will receive following expression for distribution law with the maximum entropy

$$p(x) = \frac{\nu \exp(x)}{\beta \Gamma(1/\nu)} \exp\left(-\frac{\exp(\nu x)}{\beta^\nu}\right), \quad (12)$$

$$-\infty < x < \infty.$$

The limiting case for (12) with $\nu \rightarrow \infty$ (all reverse moments exist) is a unilateral distribution law of limitations down from RV $p(x) = 1/\beta x^2$, $1/\beta < x < \infty$.

Let us define from bilateral distribution laws of RV such distribution law, for which entropy value H reaches the maximum with the following limitations, imposed on probability density $p(x)$

$$p(x) \geq 0, \quad \int_{-\infty}^{\infty} p(x) dx = 1, \quad (13)$$

$$\int_{-\infty}^{\infty} \exp(\nu x) p(x) dx = \beta^\nu / \nu,$$

where ν - a value of maximum existing primary direct exponential moment. Considering this an entropy H is defined by the expression

$$H = - \int_{-\infty}^{\infty} p(x) \ln(\exp(-x)p(x)) dx. \quad (14)$$

As a result of using the method of indefinite Lagrange numerators we will receive the following expression for distribution law with the maximum entropy.

$$p(x) = \frac{\nu \exp(x)}{\beta \Gamma(1/\nu)} \exp\left(-\frac{\exp(\nu x)}{\beta^\nu}\right), \quad -\infty < x < \infty. \quad (15)$$

The limiting case for (15) when $\nu \rightarrow \infty$ (all direct exponential moments exist) is a distribution law of bordered above RV $p(x) = \exp(x)/\beta$, $-\infty < x < \ln(\beta)$.

Now let us find from bilateral distribution laws of unlimited RV such distribution law, for which the value of entropy H reaches maximum with the following limitations, imposed on probability density $p(x)$:

$$p(x) \geq 0, \quad \int_{-\infty}^{\infty} p(x) dx = 1, \quad (16)$$

$$\int_{-\infty}^{\infty} \exp(-vx) p(x) dx = \beta^v / v,$$

where v a value of maximum existing primary reverse exponential moment. Considering this an entropy H is defined by the expression

$$H = - \int_{-\infty}^{\infty} p(x) \ln(\exp(x) p(x)) dx. \quad (17)$$

As a result of using the method of indefinite Lagrange numerators we will receive the following expression for distribution law with the maximum entropy.

$$p(x) = \frac{v \exp(-x)}{\beta \Gamma(1/v)} \exp\left(-\frac{\exp(-vx)}{\beta^v}\right), \quad -\infty < x < \infty. \quad (18)$$

The limiting case for (18) when $v \rightarrow \infty$ (all direct exponential moments exist) is a distribution law of bordered above RV $p(x) = \exp(-x)/\beta$, $-\ln(\beta) < x < \infty$.

From the analysis of expressions (15) and (18) follows, that exponential transformation of RV leads to transformation of form parameter v in scale parameter, and β parameter in shift parameter.

Finally let us define from unilateral distribution laws of unlimited RV such distribution law, for which the value of entropy H reaches maximum with the following limitations, imposed on probability density $p(x)$:

$$p(0) = 0, \quad p(x) \geq 0,$$

$$\int_0^{\infty} p(x) dx = 1, \quad \int_0^{\infty} |\ln(x)|^v p(x) dx = \beta^v / v, \quad (19)$$

where v a value of maximum existing primary direct logarithmic moment. Considering this an entropy H is defined by the expression

$$H = - \int_0^{\infty} p(x) \ln(x \cdot p(x)) dx. \quad (20)$$

As a result of using the method of indefinite Lagrange numerators we will receive the following expression for distribution law with the maximum entropy.

$$p(x) = \frac{v}{2\beta \Gamma(1/v)x} \exp\left(-\frac{|\ln(x)|^v}{\beta^v}\right), \quad 0 < x < \infty. \quad (21)$$

From (21) it follows, that if only two absolute logarithmic moments exist ($\nu = 2$), then logarithmic normal law has the biggest entropy. If $\nu \rightarrow \infty$ (all absolute primary moments exist), then (21) is transforming in Shannon law for limitations from above and down of RV $p(x) = 0,5/\beta x$, $\exp(-\beta) < x < \exp(\beta)$. It is necessary to notice, that with logarithmic transformation of RV scale parameter β transforms in form parameter and shift parameter transforms in scale parameter.

In general case, if RV η connected with RV ξ by a ratio $y = f(x)$ and known PDD $p(y)$ of continuous RV ξ , then PDD $p(x)$ can be found by a method of functional transformation with the help of expression

$$p(x) = p(y) \cdot \left| \frac{dy}{dx} \right|. \quad (22)$$

At this an entropy H , considering (22) and ratio

$$H = - \int_{\Theta} p(y) \ln(p(y)) dy$$

will be defined by an expression

$$H = - \int_{\Omega} p(x) \ln(q(x) \cdot p(x)) dx, \quad (23)$$

where $q(x) = |dy/dx|^{-1}$; Θ and Ω areas of existence RV η and ξ respectively.

3. DISTRIBUTIONS ARISING IN THE ANALYSIS OF THE SEQUENCE OF INDEPENDENT TESTS WITH THREE OUTPUTS

Next, consider the development of a probabilistic model of a sequence of independent trials with three outcomes, which becomes particularly important in the formation of estimates of the information security of information processing systems [10].

Most often during the test, it is taken into account that its result is either event A or the opposite event C. The probability of event A in any test is independent of the outcomes of all other tests (the tests are independent) and equal to the probability (this is ensured by the same set of conditions for each test). This scheme of tests was first considered by J. Bernoulli and bears his name [11-14].

The probability $P_A(k)$ of the fact, that event A in N tests will come precisely k times ($k = 1, 2, \dots, N$) is defined by Bernoulli's formula [13-15]

$$P_A(k) = \frac{N!}{(N-k)!k!} p^k (1-p)^{N-k}, \quad (24)$$

which represents binomial distribution. In $N = 1$ it transforms in Bernoulli's distribution.

$$P_A(k) = p^k(1-p)^{1-k}. \quad (25)$$

The limiting case of binomial distribution, when $p \rightarrow 0$ and $N \rightarrow \infty$, and product Np aims to some positive constant value λ (i.e. $Np \rightarrow \lambda$), is Poisson's distribution [13-15]

$$P(k) = \frac{\lambda^k}{k!} \exp(-\lambda), \quad 0 \leq k < \infty. \quad (26)$$

If sequence of tests with Bernoulli's scheme continues to appear m failures, then the number of successes k obeys to negative binomial distribution

$$P(k) = \frac{\Gamma(m+k)}{\Gamma(m)k!} p^k(1-p)^m, \quad 0 \leq k < \infty, \quad (27)$$

where $\Gamma(m)$ gamma function.

Main purpose of this work to invent sequence probability model of independent tests with three outputs and with its help receive formulas, analogic to (24), (26) and (27), for defining the probabilities of coming coinciding events.

Let it be produced N of independent tests. Every test can end with three outputs: either event A with the probability p_1 will come, or event B with the probability p_2 will come, or event C with the probability $(1-p_1-p_2)$ will come. Let's match random discrete value to random output of every test, which takes three values: -1, if event A happened; 0, if event C happened and 1 if event B happened. Positive or negative output of every test we'll consider as a success, and zero output failure. In this the probability $P(k)$ of coming events A , C and B in every test can be found by an expression

$$P(k) = \begin{cases} p_1, & k = -1; \\ 1 - p_1 - p_2, & k = 0; \\ p_2, & k = 1, \end{cases} \quad (28)$$

where $0 < p_1 < 1$, $0 < p_2 < 1$, $p_1 + p_2 < 1$.

This distribution of probabilities, analogically to Bernoulli's distribution (25), can be called bilateral Bernoulli's distribution. Let's find characteristic function for distribution (28), using ratio [15]

$$\theta(j\mathcal{G}) = \sum_{k=-1}^1 \exp(j\mathcal{G}k)P(k). \quad (29)$$

Substituting in it (28), we'll get

$$\theta(j\mathcal{G}) = p_1 \exp(-j\mathcal{G}) + (1 - p_1 - p_2) + p_2 \exp(j\mathcal{G}). \quad (30)$$

Since ongoing tests are independent, then characteristic function $\theta_N(j\mathcal{G})$ of distribution laws $P(k)$ in N tests will be equal to expression:

$$\theta_N(j\mathcal{G}) = \theta(j\mathcal{G})^N = [p_1 \exp(-j\mathcal{G}) + (1-p_1-p_2) + p_2 \exp(j\mathcal{G})]^N. \quad (31)$$

In this probability distribution $P(k)$ in N tests can be found by a formula:

$$P(k) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \theta(j\mathcal{G})^N \exp(-j\mathcal{G}k) d\mathcal{G}, \quad k = -N, -(N-1), \dots, N. \quad (32)$$

Substituting (31) in (32) and integrating, let's find obvious expression for probability distribution $P(k)$ in N tests

$$P(k) = (1-p_1-p_2)^N \times \left(\sqrt{\frac{p_2}{p_1}} \right)^k \sum_{i=|k|}^N \frac{N!}{(N-i)!} \times B(i, k) \left(\frac{\sqrt{p_1 p_2}}{1-p_1-p_2} \right)^i, \quad (33)$$

where $B(i, k) = \frac{0,5(1+(-1)^{i+|k|})}{\Gamma(0,5(i-k)+1)\Gamma(0,5(i+k)+1)}$.

Expression (10) can be simplified for five private cases:

1. If $p_1 = p_2 = p < 0.5$, then

$$P(k) = (1-2p)^N \times \sum_{i=|k|}^N \left(\frac{N!}{(N-i)!} \times \left(\frac{p}{1-2p} \right)^i \times \frac{0,5[1+(-1)^{i+|k|}]}{\Gamma[0,5(i+k)+1]\Gamma[0,5(i-k)+1]} \right). \quad (34)$$

2. If $p_1 = (1-p)^2$, $p_2 = p^2$, then

$$P(k) = \frac{(2N)!}{(N-k)!(N+k)!} \times p^{N+k} (1-p)^{N-k}, \quad k = -N, -(N-1), \dots, N. \quad (35)$$

Probability distribution (35), just like distribution (24) is a binomial distribution with not-zero shift parameter.

3. Let's view limiting case for distribution (33), when probability of coming value C is aims to zero, i.e. $(p_1 + p_2) \rightarrow 1$. In this case every test will end in two outputs: either coming of event A with the probability $(1-p)$, or event B with the probability p . To those outputs can be matched discrete random value, which takes two values: -1, if event A happened and 1, if event B happened. In this probability distribution (33) in result can be transformed in distribution:

$$P(k) = (0,5N![1+(-1)^{N+|k|}]) \times (\Gamma[0,5(N+k)+1]\Gamma[0,5(N-k)+1])^{-1} \times \left(\frac{p}{1-p} \right)^{0,5k} (p(1-p))^{0,5N}. \quad (36)$$

4. Let's view the second limiting case for distribution (33), when probability of coming event A aims to zero, i.e. $p_1 \rightarrow 0$. In this case every test will end in two outputs: either coming of event C with a probability $(1-p)$, or event B with a probability p . To those outputs can be matched

random discrete value, which takes two values: 0, if event C happened and 1, if event B happened. In this probability distribution (33) as a result of limiting transition transforms in binomial distribution (24). That's why received probability distribution (33) can be called generalized Bernoulli's formula, or bilateral binomial distribution.

5. Let's view the third limiting case for distribution (33), when $p_1 \rightarrow 0$, $p_2 \rightarrow 0$, $N \rightarrow \infty$, and products Np_1 , Np_2 aim to some positive constant values λ_1 , λ_2 (i.e. $Np_1 \rightarrow \lambda_1$, $Np_2 \rightarrow \lambda_2$). In this probability distribution (33) in result of limiting transition transforms in probability distribution

either

$$P(k) = \exp(-\lambda_1 - \lambda_2) \left(\sqrt{\frac{\lambda_2}{\lambda_1}} \right)^k \times \sum_{i=|k|}^{\infty} \frac{0,5 [1 + (-1)^{i+|k|}] \left(\sqrt{\lambda_1 \lambda_2} \right)^i}{\Gamma[0,5(i+k)+1] \Gamma[0,5(i-k)+1]} \quad (37)$$

or

$$P(k) = \exp(-\lambda_1 - \lambda_2) \times \left(\sqrt{\lambda_2 / \lambda_1} \right)^k I_{|k|} \left(2 \sqrt{\lambda_1 \lambda_2} \right), -\infty < k < \infty \quad (38)$$

where $I_\nu(z)$ modified Bessel's function.

If parameter $\lambda_1 \rightarrow 0$, and parameter $\lambda_2 \rightarrow \lambda$, then distribution (37) or (38) transforms in Poisson's distribution (26). That's why probability distribution (37) or (38) can be called bilateral Poisson's distribution. Characteristic function for it is presented lower

$$\theta(j\vartheta) = \exp[-(\lambda_1 + \lambda_2) + \lambda_1 \exp(-j\vartheta) + \lambda_2 \exp(j\vartheta)]. \quad (39)$$

Primary moment of first order and central moments of second order. Third and fourth order for distribution (33) can be found from the expressions

$$\begin{aligned} m_1 &= N(p_2 - p_1); \\ M_2 &= N \left[p_2 + p_1 - (p_2 - p_1)^2 \right] \end{aligned} \quad (40)$$

$$M_3 = (p_2 - p_1) \times \left[N - N(p_2 - p_1)^2 - 3M_2 \right] \quad (41)$$

$$M_4 = M_2 \left[1 + 6(p_2 - p_1)^2 \right] + 3(1 - 1/N)M_2^2 + 3N(p_2 - p_1)^2 \left[(p_2 - p_1)^2 - 1 \right] \quad (42)$$

Instead of central moments of the third and the fourth orders usually use asymmetry coefficient K_a and excess coefficient K_e , which can be found from ratios

$$\begin{aligned} K_a &= \frac{M_3}{M_2^{1,5}}; \\ K_e &= \frac{M_4}{M_2^2} - 3. \end{aligned} \quad (43)$$

Expressions (40)–(42) for moments are significantly simplified for private distribution cases (33). So, for distribution (34), for mentioned moments the fair expression is:

$$\begin{aligned}
 m_1 &= 0; \\
 M_2 &= 2N p; \\
 M_3 &= 0; \\
 M_4 &= M_2 + 3(1 - 1/N)M_2^2.
 \end{aligned} \tag{44}$$

In this

$$K_a = 0; K_e = \frac{0,5 - 3p}{pN}. \tag{45}$$

For distribution (45) fair expressions are:

$$\begin{aligned}
 m_1 &= N(2p - 1); \\
 M_2 &= 2N p(1 - p);
 \end{aligned} \tag{46}$$

$$\begin{aligned}
 M_3 &= 2N p(1 - p)(1 - 2p); \\
 M_4 &= 2N p(1 - p) \times [1 + 6p(1 - p)(N - 1)]
 \end{aligned} \tag{47}$$

$$K_a = \frac{1 - 2p}{\sqrt{2N p(1 - p)}}, \tag{48}$$

$$K_e = \frac{1 - 6p(1 - p)}{2N p(1 - p)}.$$

For distribution (36) fair expressions are:

$$\begin{aligned}
 m_1 &= N(2p - 1); \\
 M_2 &= 4N p(1 - p);
 \end{aligned} \tag{49}$$

$$M_3 = 8N p(1 - p)(1 - 2p);$$

$$M_4 = 3M_2^2 + 4M_2 [1 + 6p(1 - p)], \tag{50}$$

$$K_a = \frac{1 - 2p}{\sqrt{N p(1 - p)}}, \tag{51}$$

$$K_e = \frac{1 + 6p(1 - p)}{N p(1 - p)}.$$

From this follows, that for expression (37) or (38) we have

$$\begin{aligned}
 m_1 &= \lambda_2 - \lambda_1, \\
 M_2 &= \lambda_1 + \lambda_2, \\
 M_3 &= \lambda_2 - \lambda_1,
 \end{aligned} \tag{52}$$

$$M_4 = \lambda_1 + \lambda_2 + 3M_2^2,$$

$$K_a = \frac{\lambda_2 - \lambda_1}{(\lambda_1 + \lambda_2)^{1,5}}, \tag{53}$$

$$K_e = \frac{1}{\lambda_1 + \lambda_2}.$$

Probability $P_B(k)$ of fact, that event B in N tests will come k times can be found from formula (33), or from it's private cases (34), (35), (36), (37) or (38). In this we suppose, that $P_B(k) = P(k)$, $k = 1, 2, \dots, N$.

Probability $P_A(k)$ of fact, that event A in N tests will come k times can be also found from formula (33), or it's private cases (34), (35), (38), (37) or (38). In this we suppose, that $P_A(k) = P(k)$, $k = -1, -2, \dots, -N$.

Probability P_C of coming event C in N tests can be found using formula (33), or it's private cases (34), (35), (36), (37) or (38). In that we suppose, that $P_C = P(0)$. Probability P_C matches to probability of fact, that in N cases events A and B won't come.

Let's view the example. Two symmetric coins are being thrown for ten times. In every throw three outputs are possible: two eagles with probability 0,25; two tails of coin with probability 0,25 and eagle and tail of coin with probability 0,5. It's necessary to find: 1) probability P_{ee} of fact, that precisely five times two eagles drop; 2) probability P_{tt} of fact, that precisely three times two tails of coin drop; 3) probability P_{et} of fact, that precisely five times two eagles and three tails of coin drop.

Solution: In the match with example's condition we have

$$\begin{aligned} p_1 &= p_2 = p = 0.25, \\ N &= 10; P_{ee} = P_A(-5), \\ P_{tt} &= P_B(3); P_{et} = P_A(-5)P_B(3). \end{aligned}$$

I.e. $p_1 = p_2$, then we use expression (9) as a counting formula. With it's help we find, that either

$$\begin{aligned} P_{ee} &\approx 0,015; \\ P_{tt} &\approx 0,074; \\ P_{et} &\approx 1,093 \cdot 10^{-3}; \end{aligned} \tag{54}$$

or

$$F(k) = (1 - p_1 - p_2)^m \left(\sqrt{\frac{p_2}{p_1}} \right)^k \times \left(\sqrt{p_1 p_2} \right)^{|k|} \frac{\Gamma(m + |k|)}{\Gamma(m)} F(k), -\infty < k < \infty, \tag{55}$$

where $F(k) = {}_2F_1(0,5(m + |k|), 0,5(m + |k| + 1), 1 + |k|, 4p_1 p_2)$ - Hypergeometric Gaussian function.

Characteristic function of distribution (54) or (55) has the view

$$\theta(j\mathcal{G}) = [(1 - p_1 - p_2) \times (1 - p_1 \exp(-j\mathcal{G}) - p_2 \exp(j\mathcal{G}))^{-1}]^m. \tag{56}$$

Primary moment of the first order and central moments of the second, the third and the fourth orders for expressions (54) or (55) are defined by expressions

$$m_1 = \frac{m(p_2 - p_1)}{1 - p_1 - p_2};$$

$$M_2 = \frac{m(p_2 + p_1 - 4p_1p_2)}{(1 - p_1 - p_2)^2};$$
(57)

$$M_3 = \frac{m(p_2 - p_1)}{(1 - p_1 - p_2)^3} \times (1 + p_2 + p_1 - 8p_1p_2);$$
(58)

$$M_4 = m \left[\frac{6(p_2 - p_1)^4}{(1 - p_1 - p_2)^4} + \left(\frac{4(p_2 - p_1)^2}{(1 - p_1 - p_2)^3} + \frac{(p_1 + p_2)}{(1 - p_1 - p_2)^2} \right) \times (2p_1 + 2p_2 + 1) \right] + 3M_2^2.$$
(59)

Let's view limiting case for distribution (31) or (32), when probability $p_1 \rightarrow 0$, and probability $p_2 = p$. In this probability distribution (31) or (32) as a result of limiting transaction transforms in negative binomial distribution (4). That's why received probability distribution (31) or (32) can be called bilateral negative binomial distribution.

Choosing from bilateral binomial, Poisson's and negative binomial distributions we can use following properties of those distributions: Binomial $K_d M_2 < 1$, Poisson's $K_e M_2 = 1$, Negative binomial - $K_e M_2 > 1$.

So, there was developed probability model for sequence of independent tests with three outputs, were received expressions for its general number characteristics, and also for calculating the probabilities of coming matched events precisely k times. Was shown, that limiting cases of received bilateral distributions are binomial, negative binomial and Poisson's distributions.

4. CONCLUSION

In this way, the following results are obtained.

- Generalized expressions for one-way and two-way continuous distribution laws with maximum entropy depending on the number of existing power, exponential or logarithmic moments. With their help, one can more reasonably choose the a priori distribution under the conditions of a priori uncertainty in the analysis of the risks of information systems. From the analysis of expression (23) and its particular cases (2), (11), (14), (17), (20) at the appropriate values $q(x)$ it follows that in the general case the entropy depends also on the type of moments used to determine the numerical characteristics of the distribution law.

- Probabilistic model for a sequence of independent trials with three outcomes, which acquire special significance in the formation of information security assessments of information systems. Expressions for its basic numerical characteristics are obtained. It is shown that the limiting cases of the obtained two-way distributions are the binomial, negative binomial and Poisson distributions.

REFERENCES

1. Burkov V., Novikov D., Shchepkin A. Control Mechanisms for Ecological-Economic Systems. - Berlin: Springer, 2015. 174 p.
2. Kuznecov N.A., Kul'ba V.V., Mikrin E.A., Kovalevskij S.S., Pavlov B.V., Kosjachenko S.A., Malineckij G.G., Arhipova N.I., Kul'ba A.V., Volkov A.E., Shelkov A.B., Vlasov S.A., Kononov D.A., Shubin A.N., Chernov I.V., Gladkov Ju.M. Informacionnaja bezopasnost' sistem organizacionnogo upravljenja. Teoreticheskie osnovy [Information security of organizational management systems. Theoretical basis]. V 2-h tomah. Tom 1. M.: Nauka, 2006. 495 p.
3. Kuznecov N.A., Kul'ba V.V., Mikrin E.A., Kovalevskij S.S., Pavlov B.V., Kosjachenko S.A., Malineckij G.G., Arhipova N.I., Kul'ba A.V., Volkov A.E., Shelkov A.B., Vlasov S.A., Kononov D.A., Shubin A.N., Chernov I.V., Gladkov Ju.M. Informacionnaja bezopasnost' sistem organizacionnogo upravljenja. Teoreticheskie osnovy [Information security of organizational management systems. Theoretical basis]. V 2-h tomah. Tom 2. M.: Nauka, 2006. 437 p.
4. Gromov Yu.Yu., Ivanovskiy M.A., Ivanova O.G., Yakovlev A.V. Analiz i sintez struktur informatsionnykh tselenapravlennykh sistem [Analysis and synthesis of structures of information-oriented systems] - Saarbrücken (Germaniya): LAP LAMBERT Academic Publishing. 2015. 164 p.
5. Shul'c V.L., Kul'ba V.V., Shelkov A.B., Chernov I.V., Somov D.S. Upravlenie tehnogennoj bezopasnost'ju na osnove scenarnogo i indikatornogo podhodov [Managing technogenic safety based on scenario and indicator approaches]. M.: IPU RAN, 2013. 116 p.
6. Shul'c V.L., Kul'ba V.V., Shelkov A.B., Chernov I.V. Metody scenarnogo analiza ugroz jeffektivnomu funkcionirovaniju system organizacionnogo upravljenja [Methods of scenario analysis of threats to the effective functioning of organizational management systems] // Trendy i upravlenie. - 2013. No 1. - P. 6-30. DOI: 10.7256/2307-9118.2013.01.2.
7. Gromov Yu.Yu., Ivanovskiy M.A., Didrikh V.E., Ivanova O.G., Martem'yanov Yu.F. Metody analiza informatsionnykh sistem [Methods of analysis of information systems]. Tambov; M.; SPb.; Baku; Vena; Gamburg: Izd-vo MINTS «Nobelistika», 2012. 220p.
8. Gromov Yu.Yu., Karpov I.G. Dal'nejshee razvitie sushhestvujushchih predstavlenij ob osnovnyh formah zakonov raspredelenij i chislovyh karakteristik sluchajnyh velichin dlja reshenija zadach informacionnoj bezopasnosti [Further development of existing representations on main forms of laws of distribution and numerical characteristics of random values for solving the problems of information security] // Informacija i bezopasnost'. - 2010. - T. 13. - No 3. - P. 459-462.
9. Teoriya informatsionnykh protsessov i sistem [Theory of information processes and systems] / Yu. Yu. Gromov, V. E. Didrikh, O. G. Ivanova, V. G. Odnol'ko. Tambov : Izd-vo FGBOU VPO «TGTU», 2014. 172 p.

10. Gromov Yu. Yu. Generalized probabilistic description of homogeneous flows of events for solving informational security problems / Y.Y. Gromov, I.G. Karpov, Y.V. Minin, O.G. Ivanova // Journal of Theoretical and Applied Information Technology. 2016. - T. 87. - № 2. - P. 250-254.
11. Gnedenko B.V. Kurs teorii veroyatnostey [Course of probability theory]. - M.: Nauka, 1988. - 448 p.
12. Levin B.R. Teoreticheskiye osnovy statisticheskoy radiotekhniki [Theoretical bases of statistical radio engineering]. M.: Radio i svyaz', 1989.
13. Veroyatnost' i matematicheskaya statistika: entsiklopediya [Probability and mathematical statistics: encyclopedia] / Gl. red. YU.V. Prokhorov. M.: Bol'shaya Rossiyskaya entsiklopediya, 1999. 910 p.
14. Odnomernyye diskretnyye raspredeleniya [One-dimensional discrete distributions] / N.L. Dzhonson, S. Kots, A. Kemp. M.: BINOM. Laboratoriya znaniy, 2010. 559p.
15. Vadzinskiy R.N. Spravochnik po veroyatnostnym raspredeleniyam [Handbook of probability distributions]. SPb.: Nauka, 2001. 296 p.

IMPLEMENTATION OF CHATBOT USING AWS AND GUPSHUP API

Pramod K.¹, Akash Hegde², Sandhya S.³, Dr. Shobha G.⁴

¹⁻⁴Department of Computer Science and Engineering, R. V. College of Engineering, Bengaluru, India

ABSTRACT: A chatbot can be defined as a program developed to carry out conversations with a human using either audio or text. There exist numerous chatbots which are used for various purposes such as e-commerce, customer support, design, communication, finance, education, analytics, and so on. Furthermore, many companies use chatbots for their internal operations, for human resources, for customer support and more recently, support for Internet-of-Things (IoT) operations has also been added. Bearing in mind the existing chatbot applications with respect to productivity, the aim is to develop a chatbot for various operations related to productivity and project analysis within an organization, such that it can be integrated with CA Technologies Rally (Agile Central). It can be used for checking tasks and defects, generating reports and obtaining notifications. In the proposed work, the chatbot is built using Gupshup Bot Builder API which deploys it on to Amazon Web Services (AWS) Cloud, and then, it is integrated with Rally. Natural language processing (NLP) is used by the chatbot in general command interactions with the user, thereby eliminating the need for a fixed database of interaction commands.

KEYWORDS: *chatbot; cloud computing; natural language processing; project analysis; project management.*

I. INTRODUCTION

A chatbot is known by many names in the current world. It can be called as a smartbot, chatterbot, talkbot, interactive agent, conversation agent, conversational interface, artificial conversational entity, or simply a bot. A chatbot can be described as a developed program or a human-created artificial intelligence (AI) that uses various technologies to mimic a conversation that a human would have with another human. It can carry out the conversation either by audio or by text.

Chatbots are designed and developed such that they can simulate the way in which a human behaves in a regular conversation. This allows the chatbots to pass the Turing test, such that they are indistinguishable from a human. Chatbots are commonly used in dialog systems, such as customer service or information acquisition, which are two of the most practical applications in today's world. Recently, more chatbots are being developed that use complex NLP systems for their processing, as compared to traditional chatbot systems, which scan for keywords when the input is provided, then check for the reply which contains the most matching keywords, or a pattern of words, from an existing database on a server.

The term chatterbot was first introduced to the world by Michael Mauldin in 1994; he used this term to describe conversational programs. He is the creator of the first Verbot known as "Julia." The first chatbot was "ELIZA," developed by Joseph Weizenbaum in 1966.

A. Accessibility and Usage

Virtual assistants are usually used to access chatbots; they can also be accessed using messaging apps or messengers such as Facebook Messenger, or also using apps and internal websites of individual organizations.

Chatbots are generally classified into many categories based on their usage. Conversational commerce, also known as "e-commerce via chat" is one of the major categories. It can also be observed that they are used for communication purposes, for financial purposes and design purposes. Some people use chatbots for their personal tasks. They can also be used in education sector, marketing campaigns, sports events organization, entertainment industry, data analytics, multiplayer

games where text-based chat is needed, customer support over the internet, health care, Human Resources (HR) and management, news discussions, productivity analysis, developer tools, social media networking, travelling navigation and many other utilities. Some chatbots are used for Business-to-Consumer (B2C) customer service, marketing and also, sales of business products. The chatbots of many companies run on messaging apps such as Messenger for Facebook, WhatsApp Messenger, Slack app, WeChat messenger, Telegram, LiveChat, and Line messenger. The bots are generally present in the contacts of the user in the app, but they can also participate in a group chat, catering to a large number of people. They have become increasingly popular these days. Banks and insurance agents, media companies, e-commerce websites, airline companies, hotel management and restaurants, shop retailers and owners, government agencies and health care providers use chatbots on a daily basis to do limited tasks such as answering simple questions raised by the customers, increasing customer services engagement, promotional purposes, and also, by offering additional ways with which the users can order from them.

Furthermore, many companies use chatbots for their internal operations, for human resources, for customer support and more recently, support for Internet-of-Things (IoT) operations has also been added. For example, Overstock.com, which specializes in e-commerce, has launched a chatbot recently, which is named "Mila"; it is primarily used to automate simple processes which are extremely time-consuming, for example, when an employee posts a request for a sick leave.

Fig. 1. shows different chatbots available in different domains. These chatbots provide services to the users based on the domain to which they are applied. The user would be able to provide voice commands to the bot available on the device, which interacts with the applications and provides service back to the user.

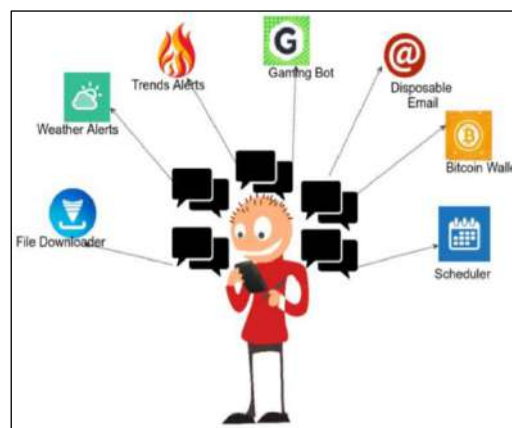


Fig.1. Chatbots in different domains

B. Organization of the Paper

This paper focuses on implementation of a chatbot using AWS cloud and Gupshup API. This chatbot is then integrated with CA Technologies Rally to be used for productivity and project analysis. Section II describes the related work that has taken place so far in terms of chatbots. Section III gives the methodology used to build the chatbot and the approach employed to integrate it with CA Technologies Rally. Section IV describes the implementation of the chatbot using the Gupshup Bot Builder API and CA Technologies Rally. Section V describes the results obtained from this implementation and is followed by Section VI, which concludes by giving the overview of the paper.

II. RELATED WORK

The topic of chatbots has drawn the attention of many researchers and thinkers. There are a number of review papers that describe the increasing use of chatbots in modern times. It has drawn many researchers to develop newer and better technology to incorporate chatbots to do menial tasks, provide customer care, give mental and emotional support, among others. There has also been an increased demand for Internet-of-Things (IoT) in recent days, and this has further alleviated the usage of chatbots for this purpose.

A novel proposal to develop a chatbot that takes in to account the context of how a conversation occurs is discussed. TensorFlow library with neural network [1] is used for developing the model and Natural Language Processing (NLP) techniques are used to determine the context, before giving a response. The chatbot thus developed can be used in small industries, it can also be used for automating customer care in businesses, wherein the chatbot handles user queries and thus, reduces the need of human labour and extra investment and expenditure.

A novel system architecture that tries to overcome the problem of solving grievances of a huge volume of users of any particular social media platform is proposed. This method analyses the messages [2] of each jabberd user to check for its actionability, where jabberd is a XMPP application server that is written in Erlang. If the messages are actionable, then the chatbot starts the conversation automatically with that particular user and helps the user to resolve any issues, by using Language Understanding Intelligent Service (LUIS) to interact with the user like a human. Their proposed system is implemented on AWS cloud publicly. This is done to provide an extremely robust, highly scalable and architecture that is extensible.

A review paper that discusses the overview of cloud-based chatbot technologies, programming of chatbots and challenges of programming in the current and future generations of chatbots is studied. The working of a chatbot using machine learning [3] in the Python programming language is described. Information about the challenges faced by the chatbots and their working is given, mainly the proper implementation and maintenance of natural language processing and machine learning techniques in chatbots. It is further stated that handling complex queries needs a lot of attention in the current scenario of chatbot development and also recommend the use of sentiment analysis as much as possible, in upcoming chatbots.

The past research done on chatbots or conversational agents using quantitative bibliometric analysis [4] is presented. The goal is to help future researchers identify the gaps for future development and research in the field of chatbots. The findings are presented and it is stated that there exists a potential research opportunity in the field of deep learning chatbots. The paper also gives several recommendations for future research based on the results.

A paper is presented that provides a review study of integrated applications which use chatbots that run on Artificial Intelligence Markup Language (AIML) [5]. These applications are prevalent in various fields such as cultural programmes and national heritage, e-learning courses, online functioning of the government, web-based and dialog models, framework for semantic analysis, framework for interaction, management of networks and modular architecture that can be adapted to any other architecture easily. The chatbots provide services, as well as interact with the users frequently and propose and determine solutions to problems through AIML-based intelligence. It is also stated that it is extremely popular with entrepreneurs these days, which employ these chatbots to help grow their business.

A comparison between Google Analytics and Adobe Analytics is made. An AIML-driven chatbot [6] is proposed that takes in raw data of the analytics as the input and enables bot users to receive business insights as the output by querying the bot.

A chatbot is used to control functions of electrical appliances over the Internet, employing IoT techniques [7]. The messages sent to the bot are processed using NLP techniques. The application is also embedded with security features that only allows access to the authorized users and also informs the users whenever an intruder is detected using motion sensors within the house.

A chatbot is built based on Recurrent Neural Network (RNN) principles [8]. Sequence-to-sequence Long Short-Term Memory (LSTM) cell neural network is used on Google's neural net word2vec. It is stated that model training times and its language model quality that is used for training affects the prediction output quality of the chatbot.

A. Existing Chatbots in India

This section describes the famous chatbot applications that currently exist in India. These can be categorized into two, based on the services or assistance provided to the public.

1. General Services

These types of chatbots are used to provide general services to the public, such as information about offers and coupons, interactive chat with the users and electronic bill payments. They usually consist of multiple services that help the public with many day-to-day activities. Some of the chatbots that fall under this category are as follows.

- "Sonia" provides information about coupons and offers from top online shops. It is deployed by developer Jiss Jose.
- "TOI Personal Assistant" chatbot represents Times of India. It is deployed by Haptik and integrated into the TOI mobile app. Apart from providing news, it also allows users to book cab services such as Ola and Uber, pay monthly bills such as TV and electricity. It accepts payment using either credit or debit card, net banking and e-wallets.
- "Ziman" is a chatbot representing Zicom. It is deployed by Haptik. The main aim of Ziman is to mimic a human conversation for people who do not feel safe and comfortable when travelling. It also aims at being available all the time to the users.
- "Rembo" is a chatbot deployed by Haptik, used to set reminders and task to-do's. It also shares jokes and motivational quotes.
- "Fun Bot" is a chatbot representing Maruti TechLabs. It is deployed by Maruti TechLabs. It asks some questions to understand the user's personality. Based on the answers provided, it recommends holiday destinations.
- "Brev" is a chatbot representing Brevity. It is deployed by Artificial Industry. It provides life hacks, how-to's, latest stories and information in categories like health, food, work, relationships, and technology.
- "Haptik Assistant" is a chatbot representing Haptik. It is deployed by Haptik. It is an assistant used to do many things such as setting reminders, booking cab services, trains, airlines, paying bills and finding nearby locations of interest.
- "Amy" is a chatbot used to talk to freely and ask for information like stock prices. It is deployed by Abhishek Bhattacharya.

2. Specific Assistance

These type of chatbots are used only for certain specific applications and/or services. The interaction between the user and the chatbot is usually limited to only the particular topic with which it is associated. Some of the chatbots that fall under this category are as follows.

- "Pathology Lab Chatbot" represents Dr. Lal PathLabs. It is deployed by Haptik on the Dr. Lal PathLabs website. Any visitor can login and check the status of his/her reports. It also guides the user through every step, thus enabling quicker resolution of queries. It is also helpful in finding nearby medical centres, for booking a check-up or a test or just browsing the catalog for information about the tests, check-ups and their respective prices.
- "Akancha" chatbot is used to represent Akancha Against Harassment. It is deployed by Haptik. It serves users who are seeking help, by using a chat-based interface that is personalised to their needs, and is extremely approachable. The bot can answer various queries regarding cyber security and safety, methods to contact the police, outlining of each person's rights, laws provided by the Indian Constitution. This bot is trained to accept requests

for help and has been designed in such a way that it mimics human behaviour with a personality that is comforting and empathetic towards the users.

- "Home Services Bot" is a chatbot representing Housejoy. It is deployed by Haptik. It provides booking for online home services like personal care, home needs and appliances.
- "Coke India" is a chatbot representing Coca Cola. It is deployed by Haptik. It allows users to ask questions about Coca Cola's quality standards, community campaigns, water usage and helps raise awareness among consumers.
- "Ask Me" is a chatbot representing Citibank India. It is deployed by Creative Virtual on the Customer Service Center of Citibank's website. It is designed to provide information to customer queries about Citibank products and services.
- "Rickfare" is a chatbot representing Rickfare Inc. It is deployed by Rickfare Inc. It calculates autorickshaw and taxi fares for Delhi, Pune, Mumbai and Ahmedabad.

III. PROPOSED METHODOLOGY

This section describes the methodology used in this paper to build the chatbot. It also gives some insights into the concepts used and the use cases that are implemented.

A. Objectives

This paper aims to develop a chatbot that can be used to implement work flow monitoring and project analytics, which can then be easily integrated with CA Technologies Rally (Agile Central). Proper authentication procedures have to be provided so that it is secure and does not leak information to the outside world. Deployment has to be done in a secure environment and only the authenticated users should be able to interact with the chatbot, or change its code or inherent functionalities and features. Three use cases are specified, which are given as follows.

- Use Case 1 – Each chatbot is usually assigned a particular "room," which is a pre-defined space in which the chatbot can interact with the users. A user should be able to add the chatbot to the room using the ID or name. The user should be able to interact with the chatbot using a set of commands as defined by the developer. The chatbot is expected to be utmost available and any outage should alert all the users about the unavailability. The chatbot is also expected to generate and preserve logs of the places it has been integrated onto.
- Use Case 2 – All users in a particular room should be able to interact with Rally. The actions of the users that are done on a day-to-day basis for internal operations, such as update tasks, discussions, defect/story status, are to be made available to all the users using the chatbot. Update tasks have to be reflected in Rally and the chatbot should confirm this updation. The chatbot should also be able to show the status of a particular field when requested for. If there is an invalid syntax used when chatting with the bot, an alert must be generated and a help file with the correct syntax must be shown to the users.
- Use Case 3 – A project manager must be able to generate various metrics such as iteration burndown, bugs for a developer in an iteration, developer points delivered, among others. This use case gets various metrics that will give insights into various metrics broadly based on productivity, efficiency and quality.

B. Chatbot Design

A chatbot is created similar to how a mobile application or a webpage is created. There are four stages in this process - designing the bot, building the bot, analyzing the bot and maintaining the bot.

- Designing the bot – The design process of a chatbot is done based on how a user interacts with the chatbot. The designer adds features to the chatbot based on the requirements specified and also the responses that have to be generated to the queries are outlined. Conversational design can be considered as a superset of this process. Chatbot designers use several design tools and software, which provide previews of how the chatbot is going to function. This helps in collaboration of the team that is designing the chatbot, thus speeding

up the design process. User testing is also a crucial aspect in chatbot design. It can be carried out in a similar fashion as that of user testing of a GUI, for example.

- Building the bot – In the chatbot building process, two tasks take place: the first task is to understand how the user is able to interact with the chatbot with some queries and the second task is to produce the right answer to the respective queries. In order to accomplish the first task, an NLP Engine is usually used, which uses NLP to understand how to adapt to different user queries. In order to accomplish the second task, the chatbot is programmed to generate different types of responses to various queries posed by the users. This allows the chatbot to select which response has to be provided whenever a query is input to the chatbot.
- Analyzing the bot – In the analysis stage, the usage of the chatbot is continuously checked for any existing problems or flaws. This is done in order to reduce the number of bugs that the users might experience during their interactions with the chatbot. Thus, the user experience is enhanced due to this process, which will aid in more number of users employing the chatbot for their tasks.
- Maintaining the bot – The requirements, services and products of any company keeps changing, due to the fast-paced scenario of the world. This means that the chatbots that are employed by these companies will have to be updated regularly to be able to provide uninterrupted service. The traditional platforms used to develop chatbots need constant maintenance. Either a service provider can take care of this or a chatbot training team within the organization can help in this maintenance. These procedures utilise a lot of company resources, incurring an increased cost to the company. In order to avoid these costs, small start-up companies now use artificial intelligence for maintenance, wherein the AI develops chatbots which are self-learning.

C. Natural Language Processing in Chatbots

NLP technology is basically used to empower chatbots. When a user inputs some text to the chatbots, they process the text in the form of parsing it, which is followed by a response generated after a complex series of algorithms which interpret the user input and determine the most appropriate inference as to what the user means or wants. Then, the chatbot determines an appropriate response which can be given back to the user. Some chatbots are extremely similar to a human in terms of their authentic conversation, which makes it difficult to determine if the agent that is on the other side of the conversation is a chatbot or a human.

Inherent chatbot technology is distinctly different from NLP technology, but this also means that the chatbot technology can improve as quickly as the NLP technology; if there are no continuous developments in NLP, chatbots will not be able to understand the nuances in spoken and written dialogue.

This is where many NLP-based applications perform poorly. Any application or system that depends upon the ability of a machine to process speech is fairly likely to falter when dealing with metaphors and similes in the elements of speech. Even though these limitations exist, chatbots are becoming complex, more responsive to commands and acting natural.

Fig.2. depicts the general working of chatbots. The user input provided at the front-end is understood by the NLP layer, which then checks for the existing data in the knowledge base or the Central Management Server (CMS). If the chatbot has already interacted with the user earlier, the history and analytics of the conversation would be stored in the data store.

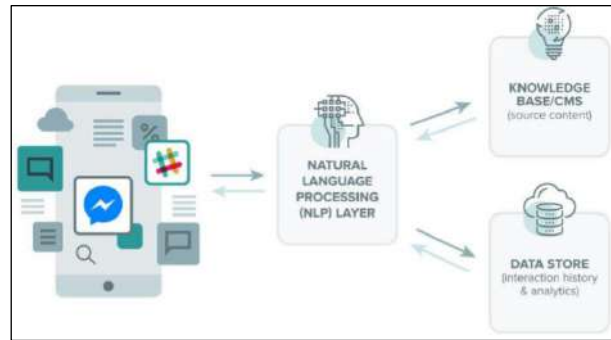


Fig.2. Working of chatbots

D. Methodology Involved in Creating the Chatbot

This subsection describes the main methodology involved in the establishment of a working chatbot that has been implemented in this paper.

Gupshup API is used to build the chatbot, which internally uses git and there is no presence of a package manager. Thus, the deployment process has to be done manually, as described in Section IV.

Once an account is created in Gupshup.io, a secure and unique API key is provided to the user in order to access the data necessary to deploy the chatbot. The access is only limited to the user's account and a git repository is already created in the back-end.

The deployment is done on AWS EC2 instances, where the replies from the chatbot are received as messages in AWS. These messages can be verified in the console logs that are generated whenever there is any interaction with the chatbot. There are multiple access points to this particular instance, which can be accessed via different messenger platforms. The chatbot will respond to that particular platform accordingly. There are a limited number of requests that can be sent. Rally offers a time-limited trial for this particular reason. It is also worth noting that AWS internally uses a read-only file system, thereby keeping the data and messages secure and not allowing the user to tamper with the existing files and repositories.

Node.js is mainly used because it comes with a default package manager and is easy to incorporate both server-side and client-side functionalities for the chatbot.

E. Importance of Chatbots

Chatbot applications are very important as they enhance customer experience by providing streamlined interactions between people and services. They also offer opportunities to companies to enhance customer service by engaging them with an automated bot that improves and aids their operations; this also results in reduced cost to the company. When a chatbot solution performs both of these tasks, it can be said that it is successfully operational. Human support is also crucial and essential because of their necessary intervention in building, configuring, constant training the chatbot to optimise and improve the system.

IV. IMPLEMENTATION

This section describes the tools used for implementation and also describes the process of building the chatbot and its integration with Rally.

A. About Gupshup Bot Builder

Gupshup.io is a web platform that offers a tool, which is known as the Bot Builder; this is primarily used to create and configure bots. This tool includes a code editor to write and edit code, a mechanism to publish the bot, analyse and diagnose the built bot employing the available tools, thus simplifying the overall process of building a chatbot.

1. Features of the Bot Builder

A usual process when a bot has to be built is to set up a developer environment, find and install necessary packages and libraries, set up space for the server, among many others. Gupshup reduces the burden on developers by taking care of all the above mentioned time-consuming processes. The IDE of the bot builder has a few features that make this possible. The pre-installed libraries such as a JavaScript async library and node-wit that is packaged with the code is very helpful.

The builder also provides a terminal to install new npm packages, to use git commands, to maintain the codebase and access bot logs for debugging and logging. The creation of a new bot comes with template code for common processes, which include helper methods. The IDE Bot Builder also provides single-click secure server deployment for the chatbot, thereby making it clear that the user need not set up his/her server.

The IDE Bot Builder is built on top of Amazon AWS Lambda and provides automated hosting. Gupshup Proxy Bot is used to test the chatbot, after deployment. The conversational aspects of the chatbot can be tested using the built-in chat widget given in the IDE Bot Builder.

B. About CA Technologies Rally

Agile methodology uses a concept called sprints – these are small, iterative periods of time, wherein the focus is on achieving small objectives such that the bigger and major objective is reached through these iterations. CA Technologies' Rally is an agile project management platform which aims at using this concept of agile, by delivering an early version of the product and then performing improvements on it.

CA Technologies Rally is now called CA Agile Central. The main idea of this software is to prioritize the tasks and complete these tasks following a plan given by the management of the company. Rally gives the option to a developer to set up a hierarchy for his/her project and portfolio. An overall roadmap can be set using Rally and continual monitoring of how well the teams are doing can be carried out.

Tracking of the releases and metrics are also present in Rally, which output an extensive report on user stories, tasks, defects, progress, dependencies, alignment and overall progress of a project.

C. Stages of Deployment

This paper aims at creating a chatbot used for project and performance analysis. It will also strive towards integrating it with the agile project management solution Rally to enable ease of use, single end point and enhanced analytics. There are mainly three stages in the development – building the bot, secure integration with Rally (CA Agile Central) and deploying it on AWS via Gupshup.

1. Building the Chatbot

The chatbot is built using the bot builder platform Gupshup.io. An index file is created to navigate to the respective modules. The bot is built to be efficient at taking input and providing output to the end user. Coding is done in Node.js to facilitate easier debugging for anyone with knowledge of Java and JavaScript concepts.

The general interactions with the bot are defined in a script that has a bit of NLP involved in it, to provide accurate answers to the end user's input. The application-specific interactions require the use of syntax to interact with the bot, which is specified in the documentation manual.

2. Secure Integration with Rally

The chatbot is then securely integrated with Rally (CA Agile Central) in order to facilitate easier access to projects, user stories, tasks and defects. Rally provides an agile project management solution that can be effectively used to make the work faster and more productive. An end user can chat with the bot and check the status of on-going projects, user stories, tasks and defects. Alternatively, the user can login to Rally to verify the same.

3. Deployment on AWS via Gupshup

Finally, the chatbot is deployed on AWS via Gupshup platform and can be accessed by any authenticated user to perform the specified tasks. It can also be used for testing purposes and raising defects, in order to be rectified by the project managers.

D. Authentication Procedures

Gupshup provides an API key with which an authenticated user can access the code built to create the chatbot. Once the code is completed, it can be deployed on AWS via Gupshup. Only the authenticated users must be able to access the project analytics information, metrics and charts. This is taken care of by AWS, wherein the user must input credentials in order to gain access to the chatbot services offered by the developers.

E. Interactions with the Chatbot

The chatbot is functional to a specific domain and cannot be interacted outside this domain. There are basically two types of interactions that can be done with the chatbot – general interactions and command-specific interactions.

1. General Interactions

These interactions with the chatbot need not have to follow a specific syntax. The queries for these interactions are usually about general topics and the chatbot responds to these queries without any need of technical information. For example, if "Hi!" or "Can you help me?" is sent to the chatbot by the user, the chatbot may respond with "Hi!" or "Yes please!" respectively.

Fig.3. shows an example of a general interaction between the chatbot and the user. It can be observed from the figure that the chatbot learns to respond with "Hi" even when two different inputs of the greeting are given to the chatbot.

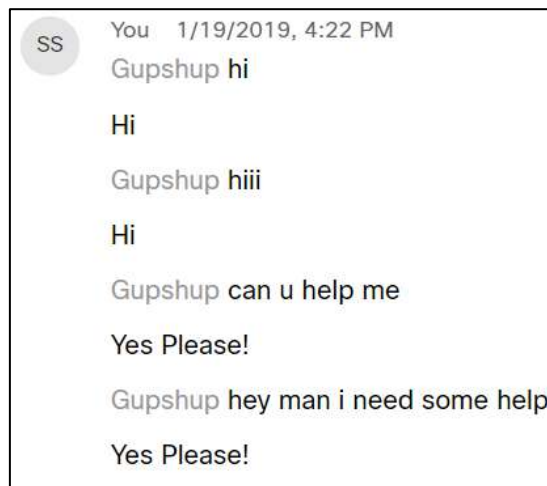


Fig.3. Example of a general interaction

2. Command-specific Interactions

These interactions with the chatbot are with respect to the project management aspect. The bot is programmed to respond to commands regarding creation, updation and deletion of projects, user stories, tasks and defects. For example, "create story Workspace". Fig.4. shows an example of a command-specific interaction. Here, it can be observed that the list of user stories is queried to the chatbot, which responds with a list of existing user stories. The status of the story "newworld" is then queried to the chatbot and it provides the necessary information as the output. Invalid queries to the chatbot are ignored and an alert message with a link to the help manual is generated.

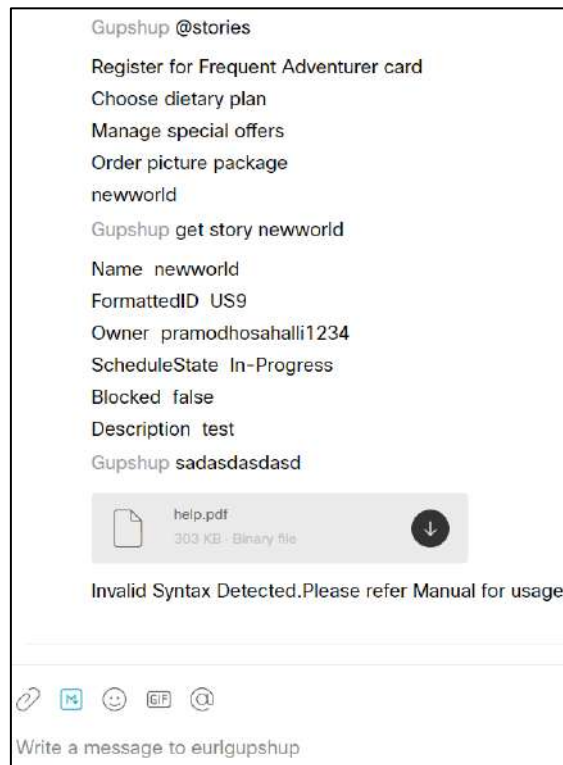


Fig.4. Example of a command-specific interaction

V. RESULTS

This section describes the results of deployment of the chatbot on AWS via Gupshup platform and its secure integration with CA Technologies Rally.

A. Deployment on AWS via Gupshup

The chatbot has been built using Gupshup Bot Builder platform, primarily using Node.js. It has been deployed on AWS via the Gupshup platform and is successfully able to interact with the user for general interactions and command-based interactions. The chatbot is functional within a specific domain and responds to messages given by the user.

B. Secure Integration with Rally

The chatbot has been successfully and securely integrated with CA Technologies Rally (Agile Central) platform which allows an authenticated user to perform the following commands - create, use, update, check for status, and delete. These commands are applicable to user stories, defects and tasks.

Furthermore, reports can be generated to check the output of the command-specific interactions. These are generated as a HTML file and can be downloaded to the local disk in the form of a JPEG or PNG image, XL sheet or CSV, among many other formats. *Fig.5.* and *Fig.6.* depict this scenario. Here, the report is generated for the defects that are present in a particular iteration. It is then visualized as a pie graph, which shows that the open defects are visualized with an orange colour, whereas the fixed defects are visualized with a green colour. *Fig.7.* also represents an example of a generated report, but with the presence of three stages of defects.

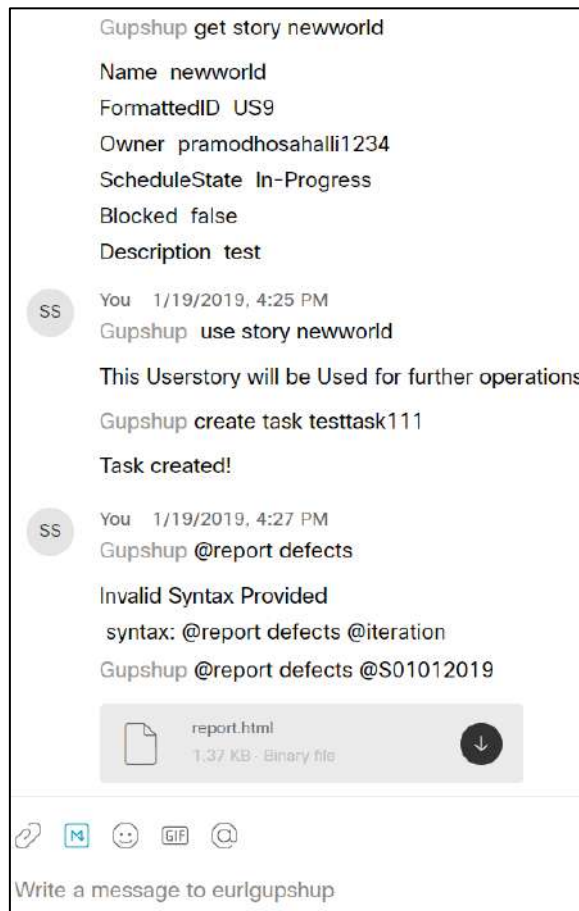


Fig.5. Command to generate report

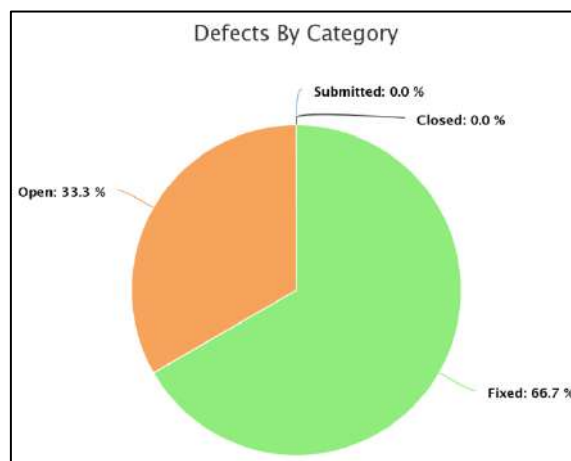


Fig.6. Example of a generated report

In the case of multiple users working on the same user story or task, the administrator account always receives notifications which specify the activity that is taking place in the system.

Fig.8. depicts the notifications. It can be observed here that whenever any changes have been made to a particular user story or a task, the chatbot immediately provides the notifications.

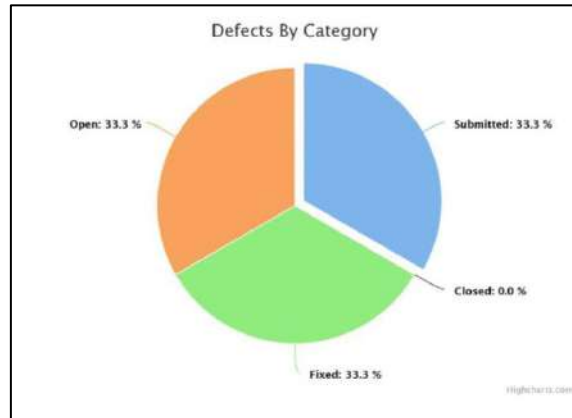


Fig.7. Another example of a generated report



Fig.8. Example of notifications

C. Analysis

The chatbot thus created has been observed to respond to user's commands within 2-3 seconds, depending on the strength of the internet connection. The deployment on AWS via Gupshup platform allows any authenticated user to securely interact with the bot and enter the set of commands. In the event of a wrong entry by a user, the chatbot provides the documentation manual which gives the correct syntax and example usage of the particular command.

Additionally, the chatbot provides reports of metrics as and when needed. This is helpful for productivity analysis. Notifications are important to the administrator to manage the projects that are going on simultaneously in the organization. They can also provide details regarding the changes that are made to the projects in real time. This helps in project analytics, productivity and management.

VI. CONCLUSION

Chatbots are conversational agents which allow humans to interact with them and obtain some useful information or perform some specific tasks or services. The advent of popular technologies such as natural language processing and deep learning has seen the incredible rise of the usage of chatbots in many applications over different domains.

A chatbot has been developed with respect to the requirements for productivity and project analytics. Node.js is primarily used to develop the code for the chatbot, which has been integrated with CA Technologies Rally and deployed on AWS via Gupshup platform. The code is kept secure via authentication procedures on Gupshup, as well as AWS. The deployment is made on AWS only after using the API key provided inherently by the Gupshup platform, which has capability of automated hosting to AWS.

The chatbot is capable of interacting casually as well as pertaining to the productivity aspects like creation and updation of user stories, tasks and defects, among other functionalities. Notification alerts are sent to the user whenever there is any update or if the user inputs an invalid command. A documentation manual is also provided, in case the user is unable to recollect the usage syntax of the commands. Future scope of this chatbot would be to include more features to help in the productivity analysis within the organization.

REFERENCES

1. R. Singh, M. Paste, N. Shinde, H. Patel and N. Mishra, "Chatbot using TensorFlow for small Businesses," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2018, pp. 1614-1619.
2. G. M. D'silva, S. Thakare, S. More and J. Kuriakose, "Real world smart chatbot for customer care using a software as a service (SaaS) architecture," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 658-664.
3. A. M. Rahman, A. A. Mamun and A. Islam, "Programming challenges of chatbot: Current and future prospective," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, 2017, pp. 75-78.
4. H. N. Io and C. B. Lee, "Chatbots and conversational agents: A bibliometric analysis," 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, 2017, pp. 215-219.
5. M. S. Satu, M. H. Parvez and Shamim-AI-Mamun, "Review of integrated applications with AIML based chatbot," 2015 International Conference on Computer and Information Engineering (ICCIE), Rajshahi, 2015, pp. 87-90
6. R. Ravi, "Intelligent Chatbot for Easy Web-Analytics Insights," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, pp. 2193-2195.
7. C. J. Baby, F. A. Khan and J. N. Swathi, "Home automation using IoT and a chatbot using natural language processing," 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, 2017, pp. 1-6.
8. M. T. Mutiwokuziva, M. W. Chanda, P. Kadebu, A. Mukwazvure and T. T. Gotora, "A neural-network based chat bot," 2017 2nd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2017, pp. 212-217.

IMPROVED MIRAI BOT SCANNER SUMMATION ALGORITHM

Faisal A. Garba Department of Computer Science Education Sa'adatu Rimi College of Education
Kano, Nigeria

ABSTRACT: Mirai is the most dangerous Distributed Denial of Service (DDoS)-capable IoT malware to date that is in the wild and yet very simple in nature. Mirai attack an array of Internet of Things (IoT) and embedded devices that ranges from Digital Video Recorders (DVRs), Internet Protocol (IP) cameras, routers and printers recruiting them to form a botnet. The biggest DDoS attack in history was executed using Mirai botnet. A recent study proposed the Mirai Bot Scanner Summation Prototype that analyzes the network traffic generated from Mirai bot host discovery. The Mirai Bot Scanner Summation Algorithm however, cannot recognize if a network traffic is truly Mirai bot host discovery traffic or not. Given any network traffic, the Mirai Bot Scanner Summation Prototype will proceed to summate and output number of bots, retransmission packets, number of packets and number of potential victim IoT devices using only the source Internet Protocol (IP) address and destination IP address of a packet without identifying if it is truly a Mirai bot host discovery packet or not. This paper present an Improved Mirai Bot Scanner Summation Algorithm that looks at the packet to determine whether it is a truly packet generated due to Mirai bot host discovery by looking at the TCP flag of the packet and the port number of the packet. To perform a host discovery Mirai bot sends out SYN packet over TELNET port 23 or 2323 to a randomly generated non-governmental IP addresses to establish a TCP 3-way handshake with a potentially vulnerable IoT device. The Improved Mirai Bot Scanner Summation Algorithm uses this condition to determine whether a packet is a Mirai bot host discovery packet or not. The Mirai Bot Scanner Summation Algorithm and the Improved Mirai Bot Scanner Summation Algorithm are evaluated using IoT Network Intrusion Dataset. The evaluation results have shown that the Improved Mirai Bot Scanner Summation Algorithm provides more accurate results than the Mirai Bot Scanner Summation Algorithm.

KEYWORDS: *Mirai, Internet of Things, botnet, Denial of Service Attack, cyber attack.*

INTRODUCTION

Internet of Things (IoTs) devices are a key targets for cyber attacks as a result of their fast growing number in smart cities, smart homes, smart hospitals etc and the quantity and sensitivity of the data they collected (Frank, 2019). Two issues highlighted by the IoT botnet are the reality that: a large number of IoT devices are easily reached over the Internet and most of the times security is a later addition to the design of most of the deployed IoT devices, that is if it has been given any consideration at all (Angrishi, 2017). One of the most predominant Distributed Denial of Service (DDoS) - capable IoT malware of the past few years is the Mirai malware which was discovered in the year 2016 and has changed the global view of IoT security since then (De-Donno et al., 2018). Mirai attack an array of IoT and embedded

devices that ranges from Digital Video Recorders (DVRs), Internet Protocol (IP) cameras, routers and printers (Antonakakis et al., 2017). The Mirai bot scanner generates a random non-governmental IP address and also creates a network socket and performs a TCP handshake (Frank, 2019). The biggest DDoS attack in history was executed using Mirai (York, 2016). This was achieved as a result of constructing a large Agent-Handler botnet that comprises of mini IoT devices taken over via a simple dictionary attack. Mirai malware is capable of carrying out a diverse number of attacks based on variety of protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Hypertext Transfer Protocol (HTTP) and can exploit devices that are based on different architectures. Mirai is the most dangerous DDoS-capable IoT malware to date that is in the wild and yet very simple in nature (De-Donno et al., 2018).

REVIEW OF RELATED WORKS

Kumar and Lim (2020) developed a network-based algorithm which can be used to detect IoT bots infected by Mirai and other malware in large-scale networks. They developed an algorithm that targets bots scanning the network for vulnerable devices to detect the bots before they launch an attack. They analyzed Mirai signatures to identify its presence in an IoT device. They lay their claim that uninfected IoT devices are not expected to open TELNET connections to any device. Kumar and Lim (2020) work is aimed at detecting Mirai Botnet attack in progress.

Frank (2019) developed Mirai Scanner Summation Prototype. With the use of Python scripts, the Mirai Bot Scanner Summation Prototype searches through the Bot scanner dataset to sum up bots, potential new bot victims and network packet types including TCP SYN and retransmission packets and save result in a database. The Mirai Scanner Summation Prototype however does not look at the packets to ensure that they are really Mirai bot scanner packets. The Mirai Scanner Summation Prototype only looks at the source and destination IP of the packets and whether they are unique or non-unique packets before proceeding to calculate the number of bots and potential bot victims from the packets. Therefore given

any network traffic that are not Mirai bot scanner packets, the Mirai Bot Scanner Summation Prototype will still proceed to calculate the number of bots and potential bots victims out of the packets.

Meidan et al., (2018) proposed N-Balot, A Network-Based Detection of IoT Botnet Attacks using Deep Autoencoders, proposed and empirically evaluated a novel network-based anomaly detection method which extracts behavior snapshots of the network and uses deep autoencoders to detect anomalous network traffic emanating from compromised IoT devices. The researchers claimed their work effectively detects attacks as they are being initiated from a compromised IoT device that are part of a botnet.

IMPROVED MIRAI BOT SCANNER SUMMATION ALGORITHM:

The Summation Algorithm used in the Mirai Bot Scanner Summation Prototype proposed by Frank (2019) cannot differentiate if the network traffic in the form of pcap files passed on to it is truly Mirai Bot Scanner network traffic. Looking at the Mirai Bot Summation Algorithm in Figure 1, the algorithm expects to have network traffic generated due to Mirai bot scanning activity. As pointed out by Frank (2019), the Mirai Scanner network traffic dataset (Internet Addresses Census dataset, IMPACT ID: USC-LANDER/Mirai-Bscanning-20160601/rev5870, 2016), consists of only SYN packets sent by a Mirai Bot over TELNET port 23 or 2323 to initiate a connection with an IoT device. The Summation Algorithm only looks out for the source IP address and the destination IP address of a packet (any packet) and if the packet is unique, the algorithm concludes that it is a Mirai Bot and if the packet is not unique, then the summation algorithms concludes the destination IP represents a non-vulnerable IoT device (Frank, 2019).

```

01. //Initialization
02. Total_Bots = 0, Total_Potential_New_Bot_Victims = 0, Total_SYN = 0
03. Total_Retransmission = 0, Total_Packets = 0, Starting_Time = 0, Ending_Time = 0
04. Packet_date = 0, L = [], S = [], SUBNETS = []
05. Starting_Time = now
06. Packet_date = date_from_filename(PCAP)
07. // Read the network packets of the PCAP file
08. Insert into list L the source and destination IP of each network packet
09. // Go thru each element of L
10. For i in L
11.     // Summate total packets
12.     Total_Packets = Total_Packets + 1
13.
14.     // Determine subnet of destination IP
15.     Add Subnet(L[i].destination_IP) to SUBNETS
16.     // Unique source IP represents a Bot
17.     If the count(L[i].source_IP in L) == 1
18.         Total_Bots = Total_Bots + 1
19.     // Unique SYN packet
20.     If the count (L[i] in L) == 1
21.         Insert L[i].destination_IP into S
22.         Total_SYN = Total_SYN + 1
23.     // Retransmission packet
24.     If the count (L[i]) > 1
25.         Total_Retransmission = Total_Retransmission + 1
26.
27. // Go thru each destination IP in S
28. For j in S
29.     // a unique destination IP in S represent a potential New Bot Victim
30.     If the count(L[j] in S) == 1
31.         Total_Potential_New_Bot_Vicitms = Total_Potential_New_Bot_Vicitms + 1
32.
33. Ending_Time = now
34.
35. //Insert summation results into the database
36. Insert Total_Bots, Total_Potential_New_Bot_Victims, SUBNETS
37.     Total_SYN, Total_Retransmission, Total_Packets,
38.     Starting_Time, Ending_Time, Packet_date
39. Into
40. Persistent Storage

```

Figure 1: Mirai Bot Summation Algorithm

There is a need to improve the Summation Algorithm to check a packet to determine whether it is actually a SYN packet and sent over port 23 or 2323 before assuming it is a SYN packet sent out by a Mirai Bot.

To validate this fact we ran the Mirai Bot Scanner Summation Prototype over mirai-ackflooding-n(1~4)-dec.pcap files from the IoT Network Intrusion Dataset made available by Kang et al., (2019). This file contains Mirai Bot ACK flood packets and benign packets (Kang et al., 2019). A description of the dataset is provided in Table 1 and the contents of the IoT Network Intrusion Dataset is shown in Figure 2.

Table 1: Description of the IoT Network Intrusion Dataset

Packet File Name	Description
------------------	-------------

benign-dec.pcap	Benign-only traffic
mitm-arpspoofing-n(1~6)-dec.pcap	Traffic containing benign and MITM(arp spoofing)
dos-synflooding-n(1~6)-dec.pcap	Traffic containing benign and DoS(SYN flooding) attack
scan-hostport-n(1~6)-dec.pcap	Traffic containing benign and Scan(host & port scan) attack
scan-portos-n(1~6)-dec.pcap	Traffic containing benign and Scan(port & os scan) attack
mirai-udpflooding-n(1~4)-dec.pcap	Traffic containing benign and UDP flooding of zombie pc compromised by mirai malware
mirai-ackflooding-n(1~4)-dec.pcap	Traffic containing benign and ACK flooding attack of zombie pc compromised by mirai malware
mirai-httpflooding-n(1~4)-dec.pcap	Traffic containing benign and HTTP Flooding attack of zombie pc compromised by mirai malware
mirai-hostbruteforce-n(1~5)-dec.pcap	Traffic containing benign and initial phase of Mirai malware including host discovery and Telnet brute-force attack

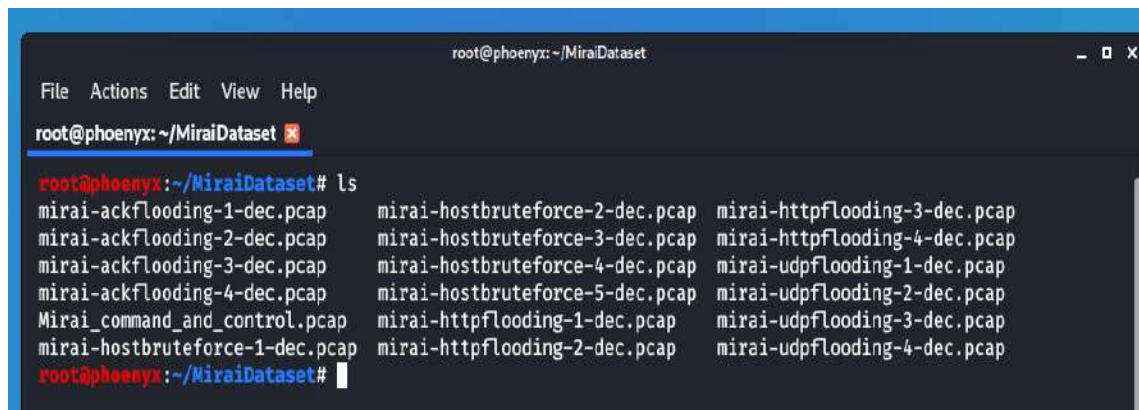


Figure 2: Contents of the IoT Network Intrusion Dataset

In Figure 3, we opened the mirai-ackflooding-1-dec.pcap using Wireshark. Next we apply the filter "tcp.flags.syn==1 and tcp.flags.ack==0 and (tcp.port==23 or tcp.port==2323)" to see if there are Mirai Bot Scanning packets in Figure 3.

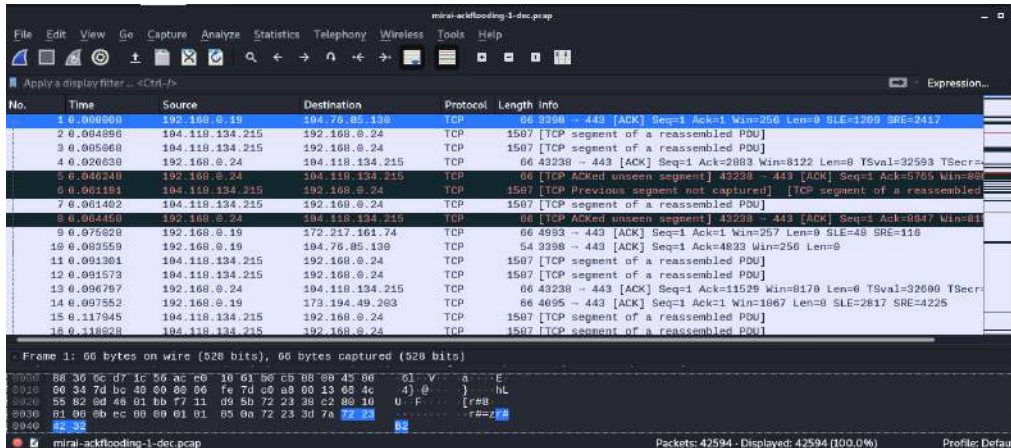


Figure 3: : Viewing mirai-ackflooding-1-dec.pcap File using Wireshark

As we can see in Figure 4, the filter returns no results. This shows that the mirai-ackflooding-1-dec.pcap contains no SYN packets sent over Telnet port 23 or 2323. However, running the Mirai Bot Scanner Summation Prototype over the mirai-ackflooding-1-dec.pcap, it couldn't identify that it is not a Mirai Bot Scanner packets, it went on straight ahead to summate the packets as if they were packets generated due to Mirai Bot scanning activity as seen in Figure 5.

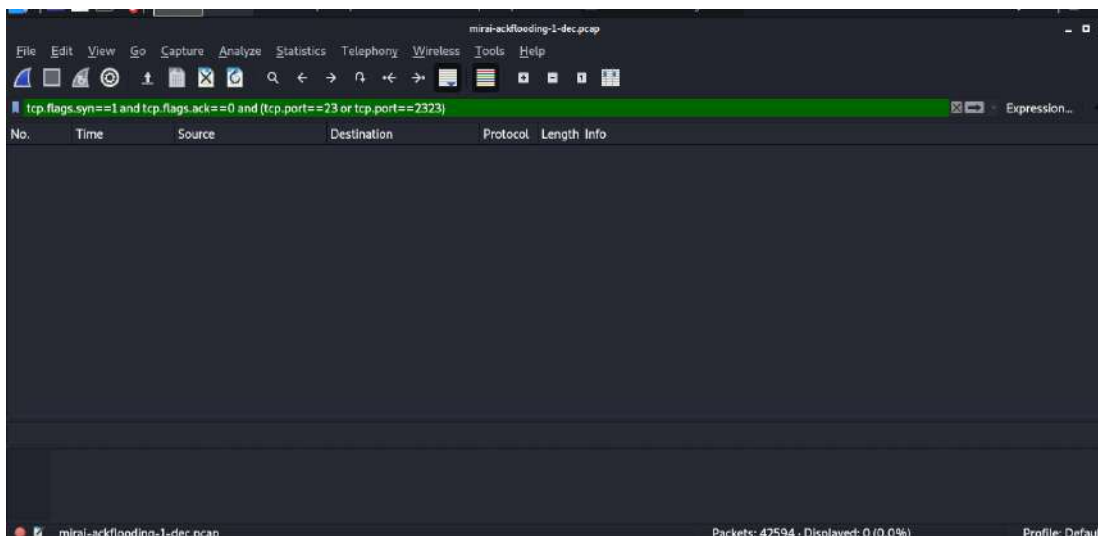
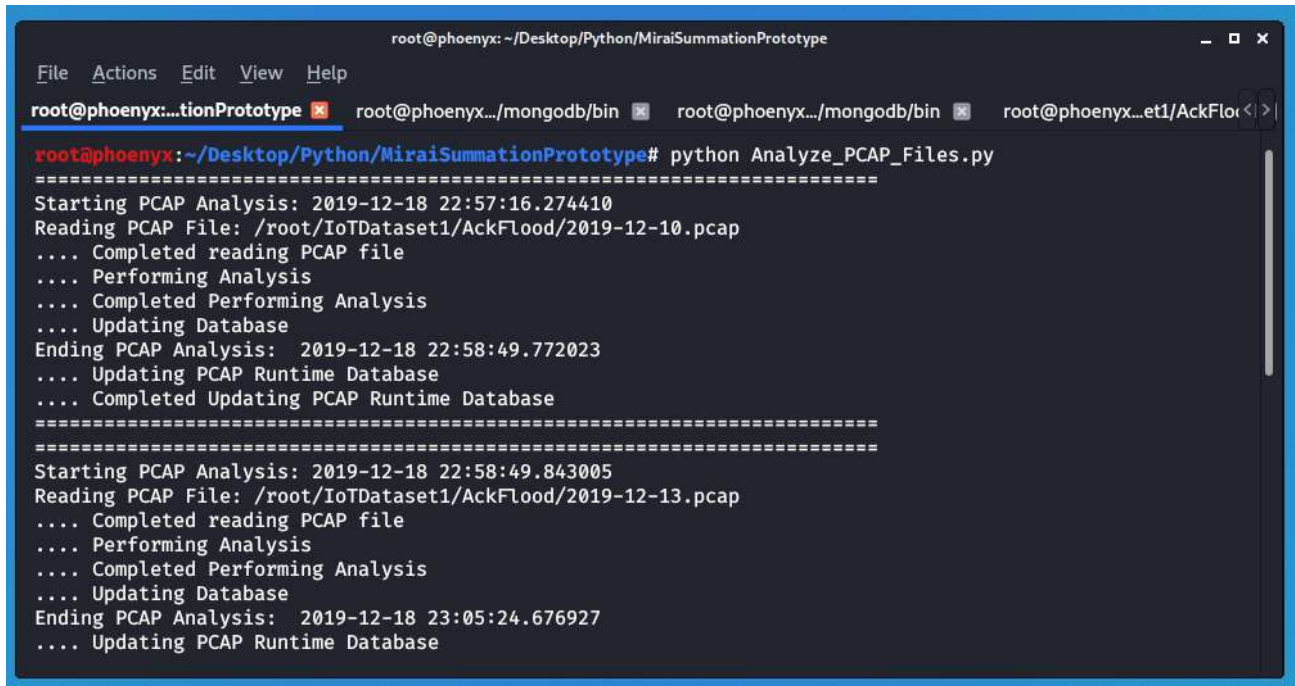


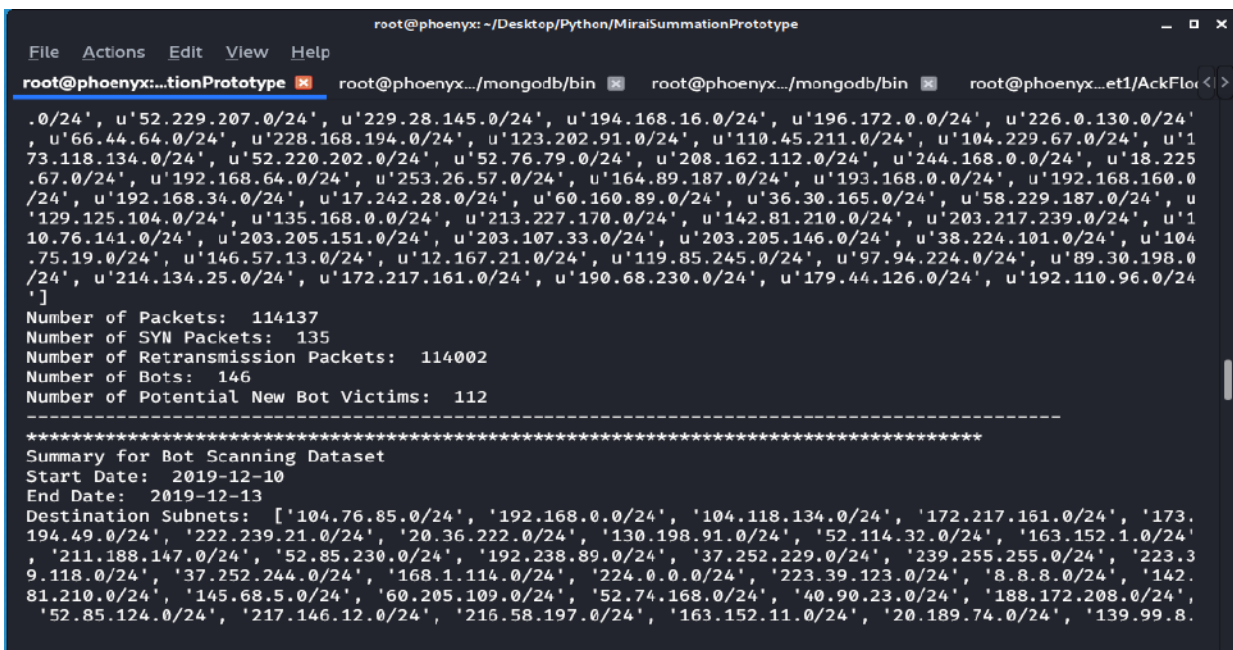
Figure 4: Applying filter to mirai-ackflooding-1-dec.pcap in Wireshark

Figure 6 presents some of the assessment results from the summation of Figure 5. The assessment results (although incorrect) is for each of the packets summated in the Mirai AckFlood folder which contains packet files generated as a result of Mirai Ack Flood DoS attack and benign packets as described in the dataset provided by Kang et al., (2019).



```
root@phoenix: ~/Desktop/Python/MiraiSummationPrototype
File Actions Edit View Help
root@phoenix:~/Desktop/Python/MiraiSummationPrototype# python Analyze_PCAP_Files.py
=====
Starting PCAP Analysis: 2019-12-18 22:57:16.274410
Reading PCAP File: /root/IoTDataset1/AckFlood/2019-12-10.pcap
... Completed reading PCAP file
... Performing Analysis
... Completed Performing Analysis
... Updating Database
Ending PCAP Analysis: 2019-12-18 22:58:49.772023
... Updating PCAP Runtime Database
... Completed Updating PCAP Runtime Database
=====
Starting PCAP Analysis: 2019-12-18 22:58:49.843005
Reading PCAP File: /root/IoTDataset1/AckFlood/2019-12-13.pcap
... Completed reading PCAP file
... Performing Analysis
... Completed Performing Analysis
... Updating Database
Ending PCAP Analysis: 2019-12-18 23:05:24.676927
... Updating PCAP Runtime Database
```

Figure 5: Summing AckFlood Files with Mirai Bot Scanner Summation Prototype



```
root@phoenix: ~/Desktop/Python/MiraiSummationPrototype
File Actions Edit View Help
root@phoenix:~/tionPrototype x root@phoenix~/mongodb/bin x root@phoenix~/mongodb/bin x root@phoenix...et1/AckFlor <>
.0/24', u'52.229.207.0/24', u'229.28.145.0/24', u'194.168.16.0/24', u'196.172.0.0/24', u'226.0.130.0/24',
u'66.44.64.0/24', u'228.168.194.0/24', u'123.202.91.0/24', u'110.45.211.0/24', u'104.229.67.0/24', u'1
73.118.134.0/24', u'52.220.202.0/24', u'52.76.79.0/24', u'208.162.112.0/24', u'244.168.0.0/24', u'18.225
.67.0/24', u'192.168.64.0/24', u'253.26.57.0/24', u'164.89.187.0/24', u'193.168.0.0/24', u'192.168.160.0
/24', u'192.168.34.0/24', u'17.242.28.0/24', u'60.160.89.0/24', u'36.30.165.0/24', u'58.229.187.0/24', u
'129.125.104.0/24', u'135.168.0.0/24', u'213.227.170.0/24', u'142.81.210.0/24', u'203.217.239.0/24', u'1
10.76.141.0/24', u'203.205.151.0/24', u'203.107.33.0/24', u'203.205.146.0/24', u'38.224.101.0/24', u'104
.75.19.0/24', u'146.57.13.0/24', u'12.167.21.0/24', u'119.85.245.0/24', u'97.94.224.0/24', u'89.30.198.0
/24', u'214.134.25.0/24', u'172.217.161.0/24', u'190.68.230.0/24', u'179.44.126.0/24', u'192.110.96.0/24
']
Number of Packets: 114137
Number of SYN Packets: 135
Number of Retransmission Packets: 114002
Number of Bots: 146
Number of Potential New Bot Victims: 112
-----
*****
Summary for Bot Scanning Dataset
Start Date: 2019-12-10
End Date: 2019-12-13
Destination Subnets: ['104.76.85.0/24', '192.168.0.0/24', '104.118.134.0/24', '172.217.161.0/24', '173.
194.49.0/24', '222.239.21.0/24', '20.36.222.0/24', '130.198.91.0/24', '52.114.32.0/24', '163.152.1.0/24',
'211.188.147.0/24', '52.85.230.0/24', '192.238.89.0/24', '37.252.229.0/24', '239.255.255.0/24', '223.3
9.118.0/24', '37.252.244.0/24', '168.1.114.0/24', '224.0.0.0/24', '223.39.123.0/24', '8.8.8.0/24', '142.
81.210.0/24', '145.68.5.0/24', '60.205.109.0/24', '52.74.168.0/24', '40.90.23.0/24', '188.172.208.0/24',
'52.85.124.0/24', '217.146.12.0/24', '216.58.197.0/24', '163.152.11.0/24', '20.189.74.0/24', '139.99.8.
```

Figure 6: Assessment Results

Figure 7 presents the Improved Mirai Bot Summation Algorithm. Line 13 adds the check for the packet to ensure it is a SYN Telnet packet. Next we run the Improved Mirai Bot Summation Algorithm which is implemented in the BotScanner.py component of the Mirai Bot Scanner Summation Prototype developed by Frank (2019). The Mirai Bot Scanner Summation Prototype is available for download from its Github repository¹

Figure 8 is a code snippet that implements the line 13 of the Improved Mirai Bot Summation Algorithm that checks for a packet being a SYN Telnet packet. The code snippet is implemented in the function analyze_pcap_file(). Variable SYN has been initialized outside the function with the value 0x02, which is the hexadecimal representation of the TCP SYN flag (Chandel, 2018).

¹ https://github.com/infosecchazzy/Mirai_Bot_Scanner_Summation_Prototype

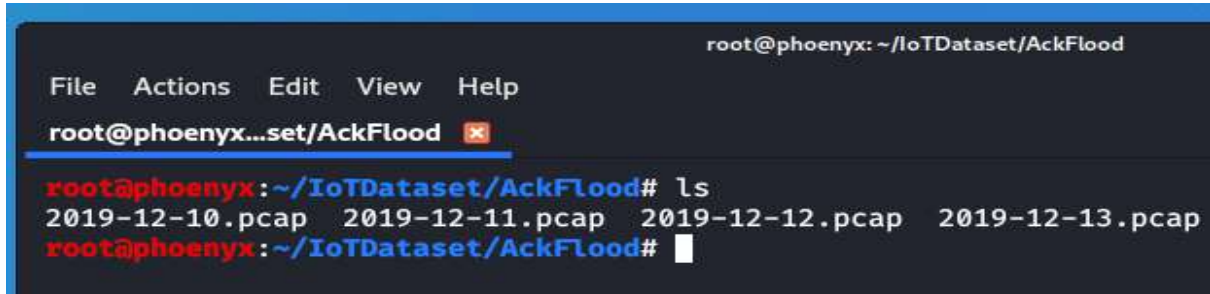
```
01. //Initialization
02. Total_Bots = 0, Total_Potential_New_Bot_Victims = 0, Total_SYN = 0
03. Total_Retransmission = 0, Total_Packets = 0, Starting_Time = 0, Ending_Time = 0
04. Packet_date = 0, L = [], S = [], SUBNETS = []
05. Starting_Time = now
06. Packet_date = date_from_filename(PCAP)
07. // Read the network packets of the PCAP file
08. Insert into list L the source and destination IP of each network packet
09. // Go thru each element of L
10. For i in L
11.     // Summate total packets
12.     Total_Packets = Total_Packets + 1
13.     If i == Telnet SYN packet
14.         // Determine subnet of destination IP
15.         Add Subnet(L[i].destination_IP) to SUBNETS
16.         // Unique source IP represents a Bot
17.         If the count(L[i].source_IP in L) == 1
18.             Total_Bots = Total_Bots + 1
19.         // Unique SYN packet
20.         If the count (L[i] in L) == 1
21.             Insert L[i].destination_IP into S
22.             Total_SYN = Total_SYN + 1
23.         // Retransmission packet
24.         If the count (L[i]) > 1
25.             Total_Retransmission = Total_Retransmission + 1
26.
27. // Go thru each destination IP in S
28. For j in S
29.     // a unique destination IP in S represent a potential New Bot Victim
30.     If the count(L[j] in S) == 1
31.         Total_Potential_New_Bot_Vicitms = Total_Potential_New_Bot_Vicitms + 1
32.
33. Ending_Time = now
34.
35. //Insert summation results into the database
36. Insert Total_Bots, Total_Potential_New_Bot_Victims, SUBNETS
37.     Total_SYN, Total_Retransmission, Total_Packets,
38.     Starting_Time, Ending_Time, Packet_date
39. Into
40. Persistent Storage
```

Figure 7: Improved Mirai Bot Summation Algorithm

```
119
120     try:
121         # check if it is a bot SYN packet
122         flag = each_packet.getlayer(TCP).flags
123         dest_port = each_packet[TCP].dport
124
125         if (flag == SYN) and (dest_port == 23 or dest_port == 2323):
126
```

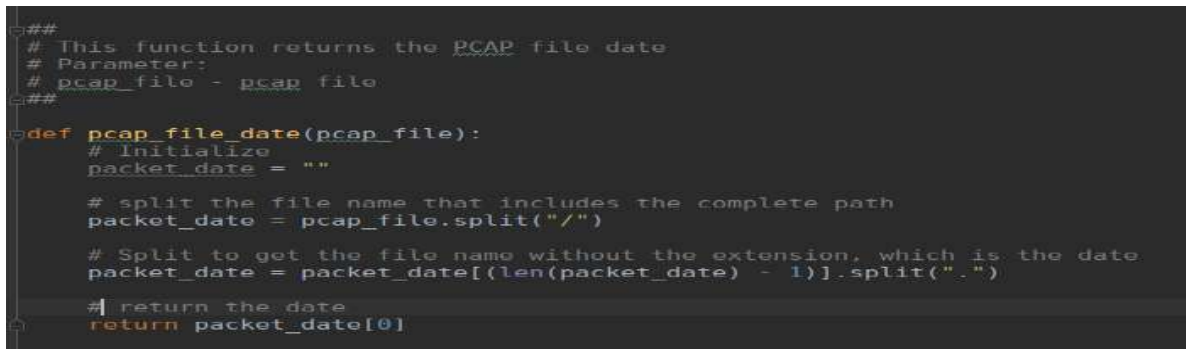
Figure 8: Code Snippet Containing the Check for the SYN Telnet Packet

In both implementations of the Mirai Summation Algorithm and that of the Improved Mirai Summation Algorithm we had to rename the packets in the mirai-ackflooding-n(1~4)-dec.pcap folder with dates from 10-12-2019 to 13-12-2019 as seen in Figure 9. This is in order to comply with the function pcap_file_date() in BotScanner.py component of the Mirai Bot Scanner Summation Prototype which requires the name of the packet files to be in date format as seen in Figure 10.



```
root@phoenyx: ~/IoTDataset/AckFlood
File Actions Edit View Help
root@phoenyx...set/AckFlood x
root@phoenyx:~/IoTDataset/AckFlood# ls
2019-12-10.pcap 2019-12-11.pcap 2019-12-12.pcap 2019-12-13.pcap
root@phoenyx:~/IoTDataset/AckFlood#
```

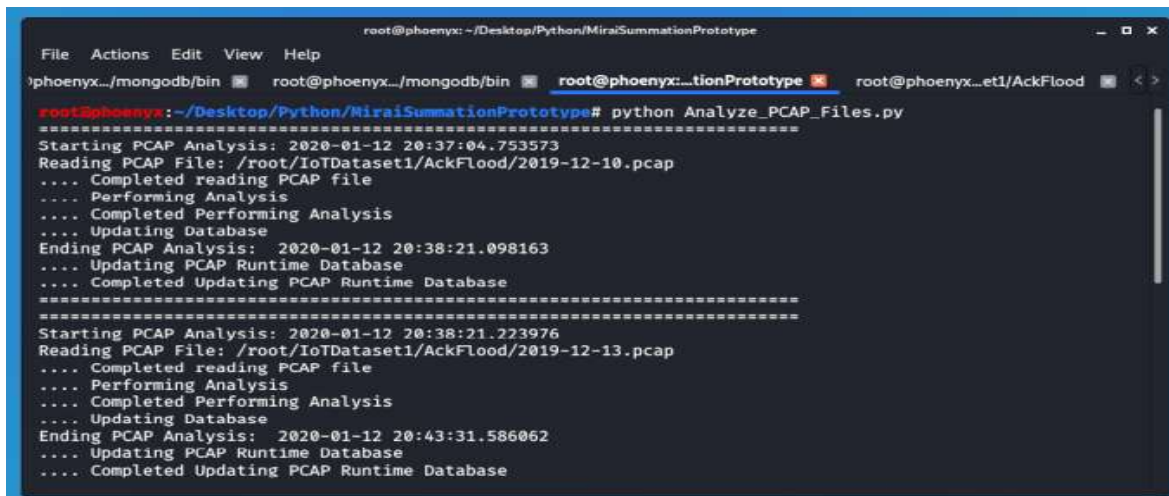
Figure 9: Renaming the Files in mirai-ackflooding-n(1~4)-dec.pcap



```
###
# This function returns the PCAP file date
# Parameter:
# pcap_file - pcap file
###
def pcap_file_date(pcap_file):
    # Initialize
    packet_date = ""
    # split the file name that includes the complete path
    packet_date = pcap_file.split("/")
    # Split to get the file name without the extension, which is the date
    packet_date = packet_date[(len(packet_date) - 1)].split(".")
    # return the date
    return packet_date[0]
```

Figure 10: Packet Files Required to be in Date Format

Next we proceed to run the Improved Mirai Bot Scanner Summation Prototype over the AckFlood packets by invoking the Analyze_PCAP_Files python script as seen in Figure 11.



```
root@phoenyx: ~/Desktop/Python/MiraiSummationPrototype
File Actions Edit View Help
root@phoenyx...tionPrototype x root@phoenyx...et1/AckFlood <>
root@phoenyx:~/Desktop/Python/MiraiSummationPrototype# python Analyze_PCAP_Files.py
Starting PCAP Analysis: 2020-01-12 20:37:04.753573
Reading PCAP File: /root/IoTDataset1/AckFlood/2019-12-10.pcap
.... Completed reading PCAP file
.... Performing Analysis
.... Completed Performing Analysis
.... Updating Database
Ending PCAP Analysis: 2020-01-12 20:38:21.098163
.... Updating PCAP Runtime Database
.... Completed Updating PCAP Runtime Database
Starting PCAP Analysis: 2020-01-12 20:38:21.223976
Reading PCAP File: /root/IoTDataset1/AckFlood/2019-12-13.pcap
.... Completed reading PCAP file
.... Performing Analysis
.... Completed Performing Analysis
.... Updating Database
Ending PCAP Analysis: 2020-01-12 20:43:31.586062
.... Updating PCAP Runtime Database
.... Completed Updating PCAP Runtime Database
```

Figure 11: Running the Analyze PCAP Files Python Script

When we invoke the Answer_Research_Questions.py python scripts, a component of the Mirai Bot Scanner Summation Prototype that parses through the MongoDB to tabulate the number of bots, potential bot victims and number of packets, it didn't shows that there are no bots and potential bots victims which is right, since the AckFlood dataset contains AckFlood packets and not Mirai bot scanner packets. This is seen in Figure 12.

```
*****
*****
Summary for Bot Scanning Dataset
Start Date: 2019-12-10
End Date: 2019-12-14
Destination Subnets: []
-----
Total number of packets: 313462
Total number of successful SYN packets: 0
Total number of re-transmission packets: 313462
-----
Average number of Bots scanning (per PCAP): 0.00
Average number of potential new Bot Victims (per PCAP): 0.00
-----
Average Number of Packets (per minute): 54.42
Average Number of Bots Scanning (per minute): 0.00
Average Potential New Bot Victims (per minute): 0.00
Average Potential New Bot Victims (per hour): 0.00
*****
root@sphoenix:~/Desktop/Python/MiraiSummationPrototype#
```

Figure 12: Assessment Results for AckFlood Packets

The Mirai HostBruteforce pcap file contains benign and initial phase of Mirai malware including host discovery and Telnet brute-force attack according to the dataset description provided by Kang, et al., (2019). So we expect to see Mirai bot scanner SYN packets sent over Telnet port 23 or 2323. We also validate that using Wireshark and the TCP filter "tcp.flags.syn==1 and tcp.flags.ack==0 and (tcp.port==23 or tcp.port==2323)". From Figure 13 we can see that mirai-hostbruteforce-1-dec.pcap contains Mirai bot scanner packets.

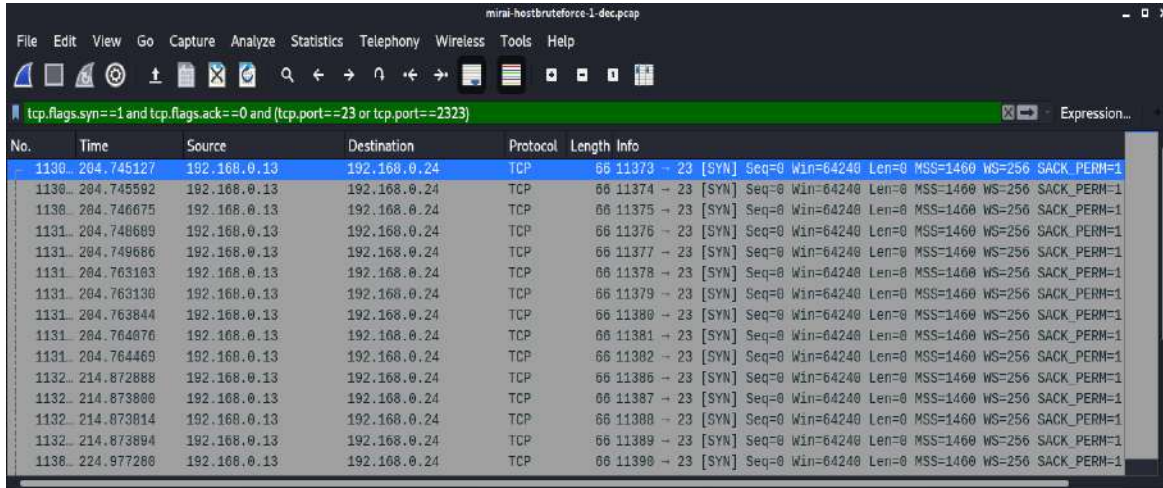


Figure 13: Viewing mirai-hostbruteforce-1-dec.pcap with Wireshark

Next we proceed to run the Mirai Bot Scanner Summation Prototype against the mirai-hostbruteforce-1-dec.pcap by invoking the Analyze_PCAP_Files.py after which we invoke the Answer_Research_Questions.py python script to carry out assessment of the summated data in the MongoDB database. The assessment result is presented in Figure 14. From Figure 14 we can see that there is a single Mirai bot per pcap file (for the 4 pcap files passed to the program), the destination subnet is 192.168.0.0/24 and there are 453,355 total packets.).

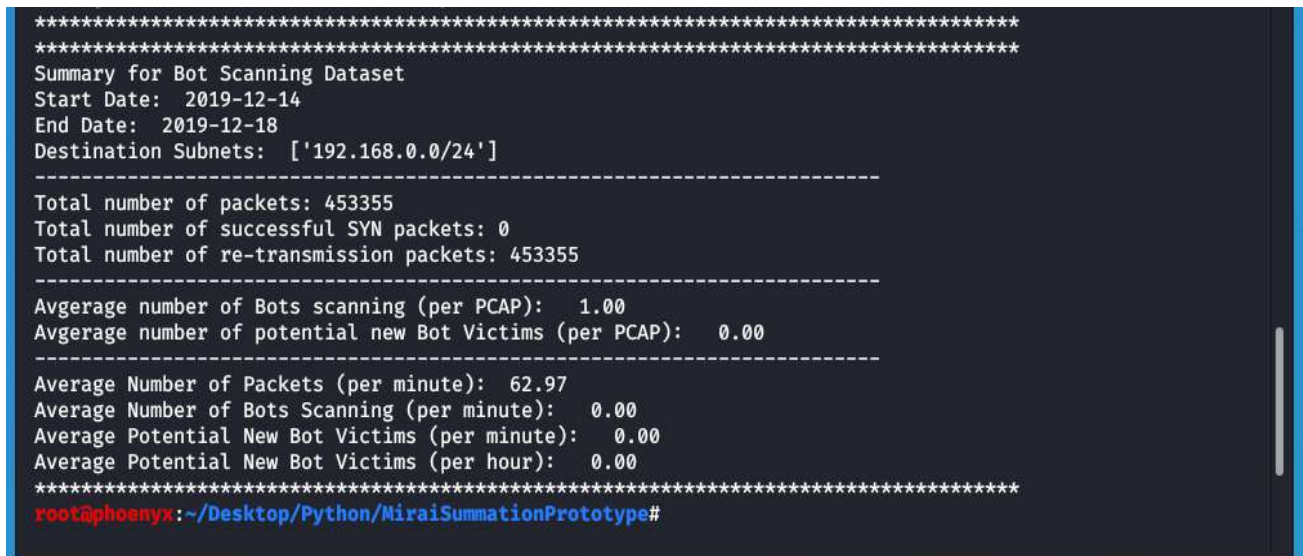


Figure 14: Assessment Results for Mirai HostBruteforce Packets

CONCLUSION AND FUTURE WORK

This paper have presented Improved Mirai Bot Scanner Summation Algorithm which is an improvement upon the Mirai Bot Scanner Summation Algorithm proposed by Frank (2019). The paper has evaluated both algorithms with IoT Network Intrusion Dataset provided by Kang, et al., (2019). Evaluation results have shown that the Improved Mirai Bot Scanner Summation Algorithm analyzes Mirai bot scanner pcap files more accurately. Future work will extend the Mirai Bot Scanner Summation Prototype developed by Frank (2019) to address those component of Mirai Malware operations not handled by the Mirai Bot Scanner Summation Prototype which include Mirai command and control, Mirai bruteforce login and Mirai Denial of Service (DoS) attacks.

REFERENCES

1. A. Kumar and T. J. Lim, "Early Detection of Mirai-Like IoT Bots In Large-Scale Networks Through Sub-Sampled Packet Traffic Analysis," in *Advances in Information and Communication. FICC 2019. Lecture Notes in Networks and Systems*, San Francisco, CA, USA , 2020.
2. C. Frank, "Mirai Bot Scanner Summation Prototype," Masters Theses & Doctoral Dissertations, 2019.
3. H. Kang, D. H. Ahn, G. M. Lee, J. D. Yoo, K. H. Park and H. K. Kim, "IoT network intrusion dataset," 09 September 2019. [Online]. Available: <https://ieee-dataport.org/open-access/iot-network-intrusion-dataset>.
4. K. Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets," *arXiv*, pp. 1-16, 2017.
5. K. York, "Read Dyn's Statement on the 10/21/2016 DNS DDoS Attack," 2 October 2016. [Online]. Available: <https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>.
6. M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, A. J. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C.

Seaman, N. Sullivan, K. Thomas and Y. Zhou, "Understanding the Mirai Botnet," in *26th USENIX Security Symposium*, Vancouver, BC, Canada, 2017.

7. M. De-Donno, N. Dragoni, A. Giaretta and A. Spognardi, "DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation," *Hindawi Security and Communication Networks*, pp. 1-30, 2018.
8. R. Chandel, "Nmap Scans using Hex Value of Flags," 31 January 2018. [Online]. Available: <https://www.hackingarticles.in/nmap-scans-using-hex-value-flags/>.
9. Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai and Y. Elovici, "N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders," *IEEE PERVASIVE COMPUTING*, vol. 13, no. 9, pp. 1 - 6, 2018.

One-time pad – How breakable it is and How we can use it in the future

Levan Niparishvili, Bachelor in Business Administration, Doing Master in IT Management at Caucasus University of Georgia

ABSTRACT: The article is about to show that One-time pad is unbreakable if all rules are correctly applied. It gives some examples to prove that ciphertext does not leak any information about the plaintext. There are situations when One-time pad can be broken in case it is based on crypto algorithm generator or when it is used more than once. Also, there is analyzed the use of one-time pad in the future.

KEYWORDS: *one-time pad, encryption scheme*

ARTICLE:

The question is: “Is one-time pad really unbreakable” – a simple answer to this question is: “Yes, in case all rules are applied correctly”. The scheme is simple and transparent and mathematically one cannot break it. One-time pad is base on the equation of two unknown variables (a plaintext and a key) out of which one is random. Let us consider the example given below:

Ciphertext:	QJKES	QJKES	QJKES
OTP-Key:	XVHEU	FJRAB	DFPAB
	-----	-----	-----
Plain text:	TODAY	LATER	NEVER

Here we have a plaintext “QJKES” encrypted by one-time pad. If an attacker tries to break it, let’s say by using a brute force attack, he would find a key “XVHEU” and get a plaintext “TODAY”.

Unfortunately, he can also find other keys like “FJRAB” or “DFPAB” and get a plaintext “LATER” or “NEVER”. He will have no clue which is correct. He can use different keys and produce any plaintext he wants. But the truth is there are many “proper” wrong keys to get a desired plaintext.

Let us give other examples based on digits. In order to encrypt a message, it is subtracted with a key, for decryption, the key is added to the cyphertext. For text-to-digit conversion we will use the following board:

CODE	A	E	I	N	O	T	CT No 1		
0	1	2	3	4	5	6	English		
B	C	D	F	G	H	J	K	L	M
70	71	72	73	74	75	76	77	78	79
P	Q	R	S	U	V	W	X	Y	Z
80	81	82	83	84	85	86	87	88	89
FIG	(.)	(:)	(')	()	(+)	(-)	(=)	REQ	SPC
90	91	92	93	94	95	96	97	98	99

Supposing that we have the following Ciphertext: 34818 25667 24857 50594 38586. There are many possible keys to crack it. Some examples are given below:

Ciphertext 34818 25667 24857 50594 38586
Key 1 +58472 33602 88472 58584 86707

Plaincode 82280 58269 02229 08078 14283

82 2 80 5 82 6 90 222 90 80 78 1 4 2 83
R E P O R T fi 222 fi P L A N E S

Recovered plaintext: "REPORT TWO PLANES"

Ciphertext 34818 25667 24857 50594 38586
Key 3 +58472 33605 28941 36331 20507

Plaincode 82280 58262 42798 86825 58083

82 2 80 5 82 6 2 4 2 79 88 6 82 5 5 80 83
R E P O R T E N E M Y T R O O P S

Recovered plaintext: "REPORT ENEMY TROOPS"

Ciphertext 34818 25667 24857 50594 38586
Key 2 +58472 33602 81702 57464 98606

Plaincode 82280 58269 05559 07958 26182

82 2 80 5 82 6 90 555 90 79 5 82 6 1 82
R E P O R T fi 555 fi M O R T A R

Recovered plaintext: "REPORT FIVE MORTAR"

These examples prove that we can produce any plaintext out of any cyphertext, if we apply a “proper” wrong key. That happens because a sequence of truly random digits. Codebreakers have no idea about which one was chosen. There is no mathematical solution to find a plaintext, in this way. But an attacker can think the other way. They can try to break they key and not a cyphertext and then reveal the plaintext. Therefore, it is critical to have a random key[1,2]. If we have a key generated by a deterministic

algorithm, an attacker will find a way to break it. For example, crypto algorithms used for key generation, lowers the security of a one-time pad and it enables an attacker to break it.

There is one important limitation to consider when working with one-time pad. If a key is used more than once, even if it is truly random, simple cryptanalysis can reveal the key. In this case, an attacker will be able to find out the connection between two cyphertexts and it will give information about the key. There can be used heuristic analysis or a known plaintext attack. Simply, there will be a crib, a presumed piece of the first plaintext to be used to reverse-calculate a piece of the key. Then we apply this presumed key to the second cyphertext. If the cribs were correct, it reveals a readable part of the second plaintext and it provides clues that help to expand the cribs.

Regarding the usability of one-time pad, we can say that it is only possible if the sender and the receiver both possess the same key. In this case, we need to ensure its secure exchange process. But we have some more drawbacks regarding the scheme. One-time pad encryption does not provide message authentication and integrity. Even though the sender is authentic and he is assigned to produce a cyphertext, we cannot verify when the message is corrupted by transition errors or by an adversary. Here a solution is to use hash algorithm with the plaintext and send the hash value along with the message [3-5]. An adversary cannot predict neither the effect of his action to the cyphertext, nor the hash value. But the receiver can reveal and compare the hashed value with the message.

As a conclusion, one-time pad is evolving while the computational power grows and the technology advances. It uses new solutions and accepts the challenges. One-time pad encryption will continue in the future securely, as we use it today, and as they were using it in the past.

REFERENCES:

1. M. Iavich, G. Iashvili, A.Gagnidze, S. Gnatyuk, V. Vialkova; Lattice Based Merkle; IVUS2019; CEUR-WS.org; 2019
2. Horstmeyer, R., Judkewitz, B., Vellekoop, I. et al. Physical key-protected one-time pad. Sci Rep 3, 3543 (2013). <https://doi.org/10.1038/srep03543>
3. Gagnidze A.G., Iavich M.P., Iashvili G.U., Analysis of Post Quantum Cryptography use in Practice, Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 2, 2017, p.29-36.
4. A. Gagnidze, M. Iavich, G. Iashvili// Novel Version of Merkle Cryptosystem// BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 11, no. 4, 2017, p. 28-33
5. S. Tang and F. Liu, "A one-time pad encryption algorithm based on one-way hash and conventional block cipher," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 2012, pp. 72-74, doi: 10.1109/CECNet.2012.6201917.

OUR PASSWORD SECURITY PRACTICES: SECURE OR VULNERABLE

Safwana Haque BRAC University, Dhaka, Bangladesh
Farhana Haque Anwer Khan Modern University
Md Abdul Haque International University of Business Agriculture and Technology

ABSTRACT: Text-based password is the most commonly used method to authenticate systems, and plays a vital role in keeping our data safe from attackers, therefore, it is important to have adequate knowledge for secured password practices. This study carried out an online survey of 500 people to study their response to password security. It was seen that 63% of the participants were vulnerable to password attacks because of their chosen methods. People of age 65 and above were found to be at the highest risk, while 80% of the female population have either never experienced or do not have any idea of a breach in their account. It was seen that 90% of the participants used information of personal significance in their lives, but 53% would still like secure passwords. This study suggests improvements for each chosen method that would make our system more reliable and immune to attacks.

KEYWORDS: *Password Security, Security Awareness, User Behavior, Security Practices, Cybersecurity*

INTRODUCTION

Cisco defines cyber-security as ‘the practice of protecting systems, networks, and programs from digital attacks’(CISCO n.d.). The users, programs and methods must all have an individual contribution to be safe and secure in a network. The users of the network or system must understand what is required to keep it safe such as choosing a secure password, accessing e-mails and websites that are safe, backing up data occasionally, etc (Armerding 2018). There are many ways of keeping a network, computer or account safe and password security is only one vital part of a more complex problem of providing security in an organization.

Passwords are the most popular and commonly used methods to restrict access to unauthorized users of a system or account (Techopedia n.d.). A password is usually a combination of alphabetic, symbolic, alphanumeric, or numeric characters. As mentioned, passwords are meant to restrict access to unauthorized users. It has been seen previously that the user passwords of very famous companies such as Yahoo, eBay, Uber, etc. have been hacked by using some sophisticated algorithm, and confidential information like date of birth, email address and password were stolen. As of 2013, Yahoo reported a huge security breach where three billion of its user accounts were compromised and this led to a loss of \$350 million in sales (Armerding 2018). The massive loss and alarming numbers of stolen information lead to a huge concern on password security.

Text-based passwords are the most commonly used authentication methods and monitoring the patterns of passwords of users regularly is necessary to understand the vulnerabilities that exist in a network. In this way, users could be educated and stronger securities policies and techniques could be implemented to keep data safe from attackers.

RELATED STUDY

Password security should be taken seriously by individuals and organizations where people should properly know how to create good passwords, change it occasionally and also record it safely and

properly for later use (Techopedia n.d.). An issue of choosing passwords is that people tend to choose very easy passwords, most of all they tend to choose from one set of characters e.g. all small letter alphabets which would possibly be a word from the dictionary or a name of someone. Another issue of password security is when the actions of ex-workers who would have very detailed knowledge of the system and resources in an organization cannot be controlled (Morris and Thompson 1979). In these cases, passwords become very vulnerable to attacks. Password security should also be made as convenient as possible for users, so that unauthorized people may not be able to log in and also users that are logged in will not be able to carry out any unauthorized or illegal activity (Morris and Thompson 1979).

(Morris and Thompson 1979) conducted an experiment on the choice of passwords created by users when they were not enforced with any criteria of password creation. A total number of 3,289 passwords were collected out of which 477 were four alphanumeric characters, 706 were composed of five letters where all the letters were either in upper-case or lower case characters, and 605 were six-letter passwords, all in lower case. The authors further ran a test to see how fast they could identify the passwords with a matching algorithm and if the passwords were from the dictionary. It was reported that one-third of the passwords were words from the dictionary and took five minutes to run the test. This experiment was carried out in 1979 on a UNIX system and it is expected that with the advancement of hardware and software technology now, lesser time would be required identify these passwords (Klein 1992). It was suggested that users should be forced to use longer passwords, select passwords from a large character set or use a program that would generate the password for the user. In 1989, a survey carried out by (Klein 1992) on password showed that out of 15000 participants, 2.7% used their usernames as their passwords and this was easily cracked in the first 15 minutes of the experiment.

Some suggested ways of formulating a good password are the use of room, social security, license plate or telephone numbers, names of streets, cities or first names with the first letter in uppercase, and also words from the dictionary that are spelt backwards (Morris and Thompson 1979). Although it was suggested in (Klein 1992) that passwords that contain these numbers solely is not a good security practice because hackers understand that people will choose numbers that have special meanings attached to it. These should be combined with other words or numbers that make it difficult to guess. Using words from the dictionary are known to be bad practices as this could be easily cracked and also common words spelt backward as mentioned in (Morris and Thompson 1979) are not advisable to use as passwords (Klein 1992). However, using a combination of words is a good practice, and if combined with a punctuation mark or uppercase characters increases its difficulty of being cracked. Using the initials from a long sentence also makes it difficult (Klein 1992). Another way of checking the vulnerability of a password is by using a password checker that would immediately reject common words from the dictionary, initials from the user's names, usernames as passwords, patterns of keys from the keyboard, words shorter than specific length, etc.

Apart from the fact that users select very easy passwords that could be hacked easily, other ways of identifying passwords are by gaining access to the system, eavesdropping on the communication line between the user and the system and studying the way the password matching algorithm works (Lamport 1981).

These were experiments or studies carried out in the 20th century, but what about the 21st century? Have the password choosing habits of people changed? Are people well aware now as the technology is improving?

A survey carried out by (Riley 2006) on the knowledge of user password security showed that out of 315 respondents, 73% knew that it was advisable to change passwords every 6 to 12 months, but 53% reported not changing passwords till it was necessary. 51% understood that using special characters is a good practice but only 4.8% used such characters in their passwords. 71% reported that using words of interest to a person or strong meaningful words should be avoided as this could easily be hacked if a profile study was conducted by the hacker, however 50% reported using these words. Just like

meaningful words, 68.3% understood that personal numbers such as telephone, date of birth, etc. should be avoided but 55% reported that they used such numbers in their passwords. 60% of the respondents reported that they do not change their password even if it depends on the complexity of the situation such as bank account passwords and all these are based on the fact that users have a difficulty remembering too many passwords. These studies show that users are actually aware of the security issues, but always go back on using simple strategies to remembering passwords which makes it vulnerable to attacks.

(Gaw and Felten 2006) carried out a survey with 49 undergraduate students and it showed that the respondents understood that password security was essential but had difficulty remembering passwords. Some responded that they had variations of a particular password which they used for different websites, and this had helped them remember passwords. They understood the necessity of using randomly generated password, but they still pictured an attacker as a human, hence they chose passwords difficult for a human to crack, but failed to realise that sophisticated algorithms are now used to hack into accounts. Some also mentioned that they would change their passwords regularly if they were asked to do so, and it was suggested that websites should keep a record of the frequency of logins from users. The websites should then send reminders to the users to change their passwords from time to time. It was observed that the users are educated, have technical knowledge, and easily adapt to new and emerging technologies, but they still have difficulty understanding the method of attacks.

(Florencio and Herley 2007) conducted a three-month study on password habits of half a million users and it was found out that an average user had approximately seven passwords where each password was reused in approximately four other websites. During a three-week period, it was also observed that about 436, 000 clients visited a phishing site, so on an average about 0.4% of the population visits a malicious website annually. It was found that people tend to forget their passwords a lot and at least 1.5% of Yahoo users forget their password each month and this could be because a user has 25 other accounts and signs in into at least 8 per day. This has already been reflected in the study carried out in (Gaw and Felten 2006) where it was mentioned that with time, remembering passwords would be tougher as people will have more accounts to handle.

Over time, some websites or management systems came up with password creation policy and this meant that a password must have a minimum of 6 to 8 characters, contain an uppercase and digit, and it must not be constructed from dictionary words. This policy was introduced in a university and (Shay et al. 2010) carried out a survey on user feedback few days after the policy was introduced. The survey included 470 respondents from the university; it was found out that the change in password policy annoyed most users even though they understood that their accounts were trying to be better protected. Users who created and forgot their passwords were more annoyed and were likely to write their passwords down in a place that would be fast to access, but would be less secure. The study, however, showed that forgetting password did not depend on IT literacy or age factors. In fact, women tend to forget their passwords more than men. One-fourth of the users had shared their old and new passwords with someone. The results obtained showed that younger generation mostly shared their passwords with someone. Three-fourth of the participants reused passwords and half modified old passwords which indicates that even when forced to change passwords, many do not create completely new passwords which still is a breach to password security as obtaining access to any one account of a user can enable access to other accounts. About 69% of the female participants reported using slight modifications of old or other passwords used for other accounts compared to 55% of the male respondents. More than 80% of the users still used a dictionary word and attaching special characters to it which indicates that people still like using words they can easily remember or have special meaning to them.

As mentioned in (Shay et al. 2010) text-based passwords are still very popular as it does not require any hardware device, and is cheaper to implement than other methods such as the biometric authentication procedure. This method is however, vulnerable to dictionary attacks as people tend to use words that are used on daily basis, and also shoulder surfing which is also known as spying. This means the attacker simply spies and observes the user entering the password (Raza et al. 2012). It is easy to pick up the

password if the user is typing slowly, hence when creating complex password policies, this should be considered.

In a survey carried out by (Awad et al. 2017) on 140 university students, it was found that females were more inclined to use longer passwords than males. Less than one-third of the participants used special characters and they were used mostly in the middle of the passwords; 90% used numbers, which were used at the end of passwords making them weak as the words could easily be guessed. On the average, 48.5% use uppercase but 80% of these have it as the first letter making it easy for attack, as spellings or sentences mostly start with capitals and a combination of characters could easily guess the password. 60% of the passwords used in the university could be cracked within days. The study clearly showed that people tend to think they are secure, but their password habits prove it otherwise.

It is necessary to educate users on their password choosing strategies, strengths and weaknesses to improve cyber security; hence a tool was devised in a study which would allow users to enter potential passwords and the tool would predict how strong or weak the chosen password was. As seen in (Tsokkis and Stavrou 2018), only 10% of 30 respondents used random passwords, while there was a high tendency of using dates as part of passwords (40%). 47% of the users entered predictable passwords and after the test, 80% of the users agreed to change their password understanding the lack of security of their passwords. It was emphasized by researchers that users should be educated more frequently on their password habits and policies should be enforced so that users are obliged to choose strong passwords.

Computers and the internet were introduced long time ago in most of the places discussed above, but as for Bangladesh, internet was introduced in 1995 and in 1996, there were only two internet service providers in the whole country (Hamidur 2009). In February 2019, it was reported that there were about 92 million internet users (Anonymous 2019). It is therefore necessary to continuously monitor user password trends as the country is progressing very fast towards internet usage. As it can be seen, humans play a key role in maintaining a secure system, as their decisions can have either a positive or negative effect on the security of accounts and a network as a whole. The objective of this study was therefore to understand the password choosing strategies, effects of poor password practices for accounts and suggest necessary steps to rectify these problems.

METHODOLOGY

This study was carried out in Bangladesh in 2019, using an e-survey comprising of 28 questions, of which five collected the demographic information of the respondents, while the rest were used to determine the behavior of the respondents towards password practices. A total of 500 Bangladeshi respondents participated in this survey and the results of the survey were broadly categorized according to the following demographic parameters:

- **Gender:** respondents were classified into male and female gender groups. About 65.9% of the respondents were male, while 34.1% were female.
- **Age:** respondents were grouped into five categories; 18-24 (56.2%), 25-34 (33%), 35-49 (7.8%), 50-64 (2.2%) and ≥ 65 (0.8%). It was noticed that the younger the age group, the more the number of respondents. This could be attributed to the possibility that younger generations are more tech-savvy whereas the older generations are not.
- **Technical know-how:** respondents were categorized into four groups depending on their educational and technical backgrounds, that is, science background (54.2%), non-science background (16.8%), IT professional (15%) and non-IT professional (14%).

The survey conducted comprised of different types of questions but most were of dichotomous and multiple-choice types. About five questions were open-ended which were used to understand the users' ability to discern between weak and strong passwords. Detailed analysis and explanation of the results obtained from the survey conducted are given in the following section.

RESULTS AND DISCUSSIONS

NUMBER OF PASSWORDS

Online dependency is immense nowadays as most websites require users to have an account with them in order to carry out some form of transaction or communication with them. There are many different types of online accounts possible such as email clients, bank accounts, health services, e-commerce sites, utility services, social media accounts, and government services. *Fig. 1.* shows that people most commonly have at least five different types of online accounts. From the total number of respondents, it was found that almost 70% of people have at least 5 or more different account types which could mean that one could own up to 10 or more accounts. For example, someone could have Yahoo, Gmail and Hotmail email client accounts at the same time and also could use Twitter, Facebook, Instagram, Viber, WhatsApp, and Skype social media applications. In this way, one could have a large number of online accounts.

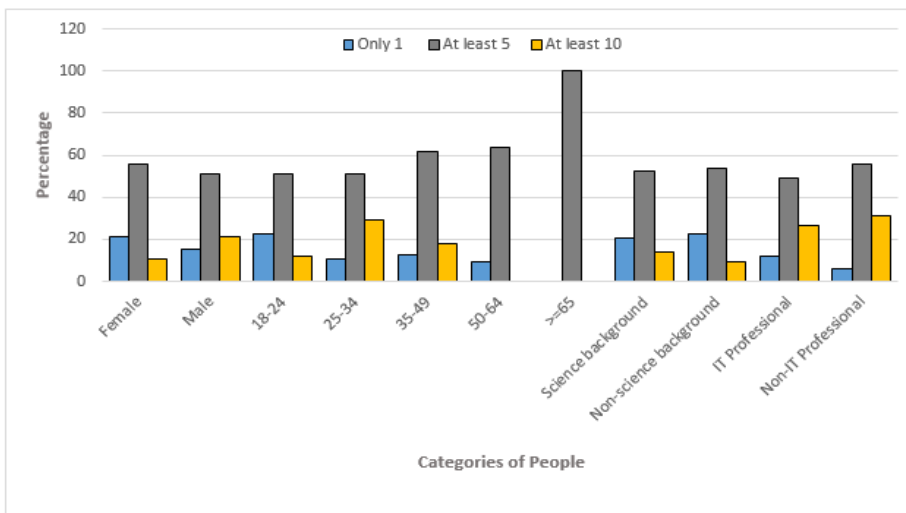


Fig. 1. Number of online accounts owned by different categories of people

PASSWORD COMPOSITION

Most online accounts nowadays set some password requirements such as length of passwords, combination of characters, numbers and cases. To satisfy these requirements, users use different pieces of information to form a password combination. From *Error! Reference source not found.*, it can be seen that 90% of the users used the most common types of personal information such as names of self, relatives, pets etc.; a number such as telephone number, identification number etc.; a date or year of relevance such as birthdays, anniversaries etc.; something about oneself such as hobbies, likes and dislikes etc.; a dictionary word found in a language or a combination of some or all the above mentioned. Use of commonly known facts about oneself is highly dissuaded as these pieces of information can be easily gathered from online stalking or profiling.

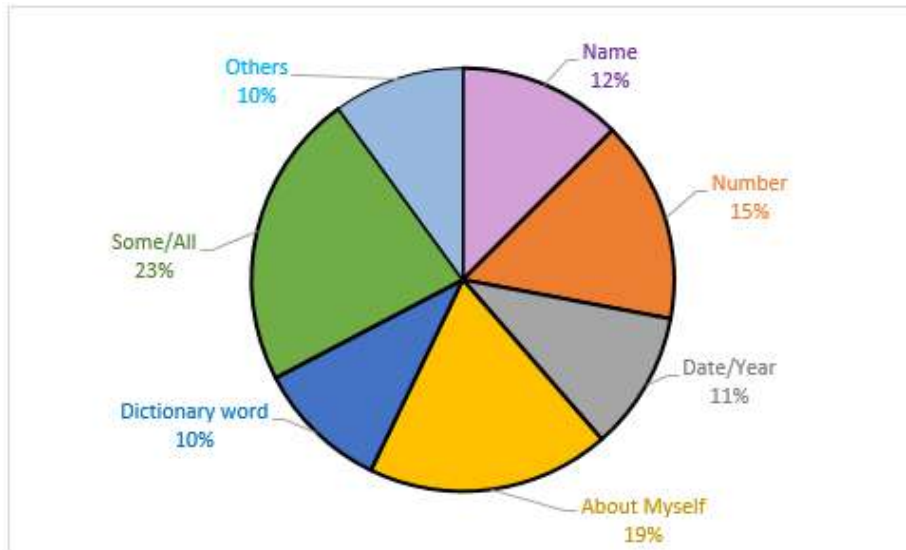


Fig. 2. Most-used pieces of information to form passwords

PASSWORD REMEMBERING TECHNIQUE

As the number of online accounts owned per person increases, the more challenging it becomes remembering and maintaining different passwords for each account. There are several ways employed by people which help them in remembering their passwords as shown in *Fig. 3*.

It can be seen that most popular choices for recalling passwords are choosing an easy password and writing down in a book, notepad, diary, etc. for later reference. Choosing easier passwords is higher amongst the female participants (38%) compared to the male participants (27%). Usage of easy passwords is a very common practice amongst all categories, and writing down passwords is seen to be very widely used in the age group of 50-64 (45%). Both these methods are not recommended as easy passwords can be easily cracked or guessed by others and a book of passwords can be dangerous if it falls in the wrong hands as it would contain all the usernames and passwords of all accounts the owner has. Using passphrases unique to each account may be a better choice, for example, having Y! I5 my 1st 3m@il @ccT for a Yahoo account and 1 @m v3rY !rr39u1@r on F8 for a Facebook account.

Another option would be using a password manager. A password manager is simply a software which could be used to store passwords in an encrypted format, and the user would require a key password to view or manage the passwords stored. However, one must be careful and smart about selecting the master key that would keep all other passwords safe.

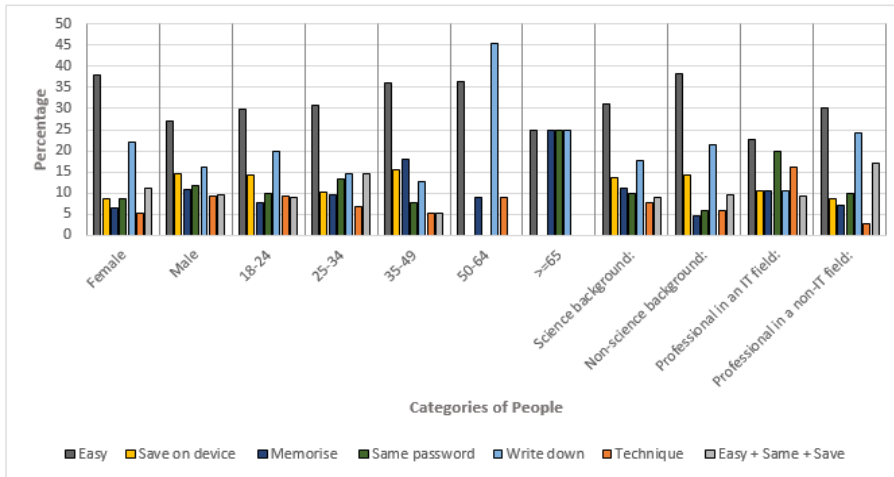


Fig. 3. Remembering techniques among the different categories of people

PASSWORD RE-USE

It is recommended to use a different password for every different account so as to prevent access to all of one’s accounts in case a third-party gains access to one password/account. From this study, it was seen that 32% of all respondents re-use their passwords in some/all of their accounts. From Fig. 4, it can be seen that people who are 65 years and above are more than likely to re-use their passwords. It is also surprising to note that those from an IT background have a high percentage (40%) of password re-use.

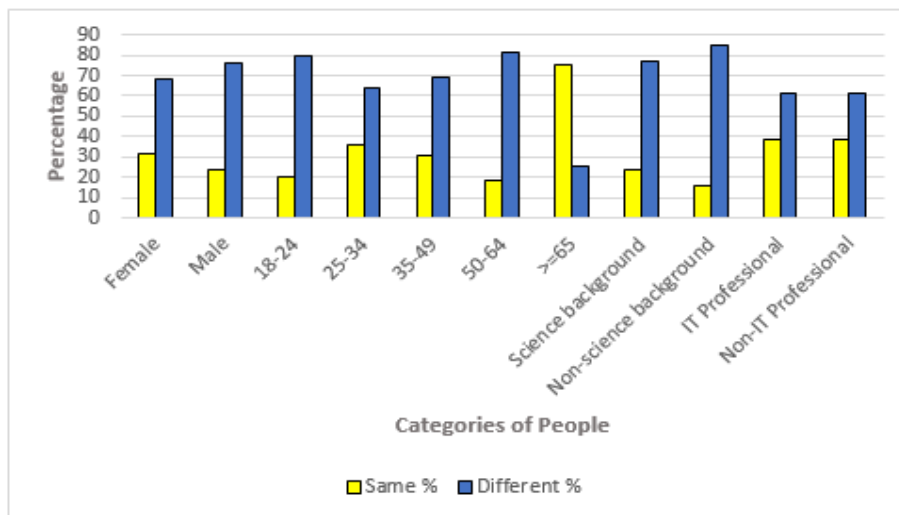


Fig. 4. Password re-use among the different population categories

PASSWORD CONFIDENTIALITY

Passwords are meant to be personal and private at all times to the authorized parties only to avoid breach of confidentiality such as the unauthorized access and use of data. However, it was seen from the survey that users gave out their passwords deliberately to different people without thinking about or realizing the repercussions of doing so. Fig. 5 indicates that only 43% of the respondents did not share their passwords, while up to 6% of the respondents shared their passwords with at least five people or even

more. **Fig. 6** presents the percentages of whom people mostly shared their passwords with. Even though 87% of the respondents shared their passwords with their loved ones (husband, wife, boyfriend, girlfriend, siblings or friends), who can mostly be assumed to be trustworthy, sharing passwords can still be very risky as these people may intentionally or inadvertently compromise sensitive data or account details.

Fig. 7 shows that at least 50% of each of the respondents across all of the demographic parameters compared have shared their passwords. It can also be seen that among all the different groups of respondents, the people above the age of 65 years can be the most vulnerable as 80% of this group share their passwords. Alarmingly, it was found from the survey that only less than 1% of the respondents who shared their passwords with some other person(s) changed their passwords afterwards.

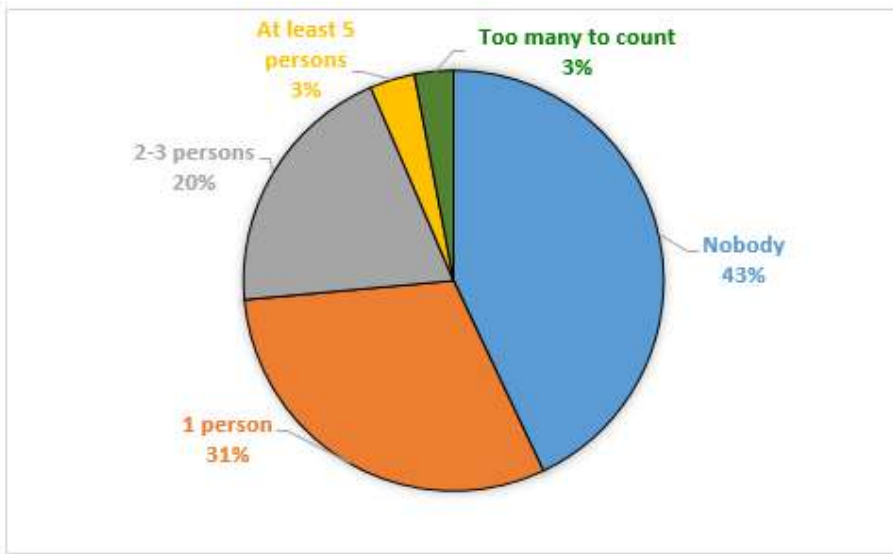


Fig. 5. Number of people passwords was shared with

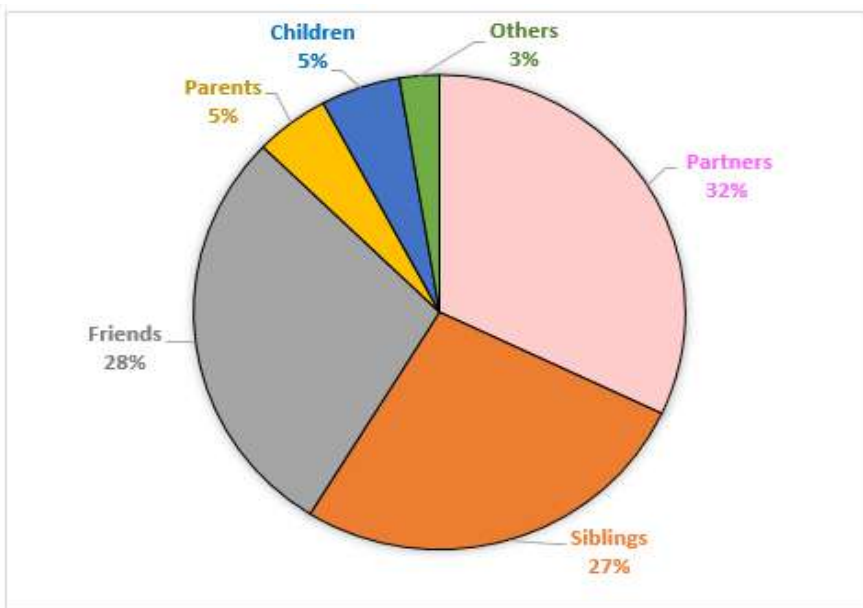


Fig. 6. Categories of people passwords are shared with

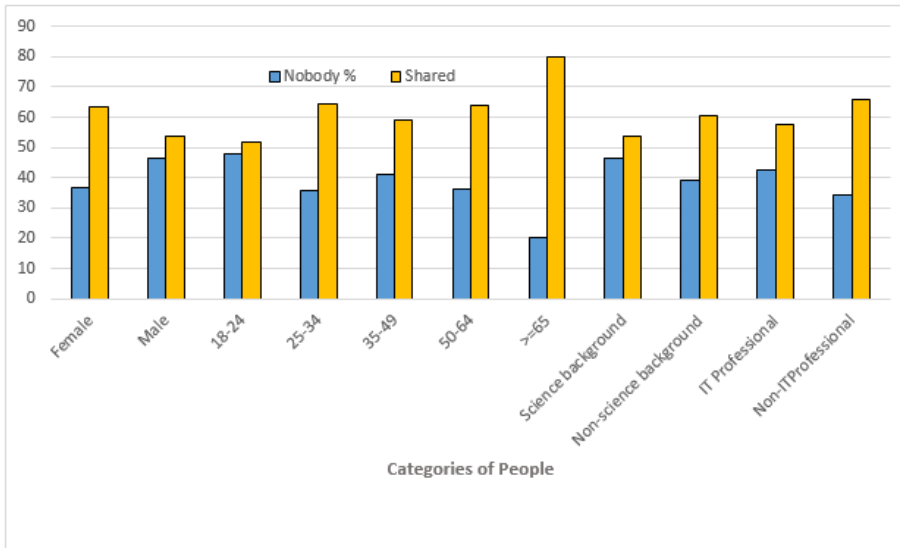


Fig. 7. Password sharing percentages among the various demographics compared

PASSWORD CHANGE FREQUENCY

Various experts and studies suggest that regularly changing or updating one’s passwords could increase the password security of one’s online accounts. Nowadays, it is recommended to regularly change one’s password at least once or twice a year especially if one is not using two-form factor authentication (Gott 2018). This ensures safety of one’s password even if a third party has gained access.

However, from Fig. 8, it can be seen that 47% of all respondents changed their passwords only when required to do so, that is, if one could not remember one’s password or if required by system etc. and 16% had never changed their passwords. From Fig. 9, it can be seen that changing passwords only when required to do so is a popular choice across all the different population types studied. It is noted that people who are 65 years and above are less likely to change their passwords unless required to do so and thus, can be considered to be the most vulnerable group surveyed. It has been suggested by various authors that websites should send a reminder to their users to change their passwords once in a while, but it has also been studied that users tend to get annoyed when forced to change their passwords.

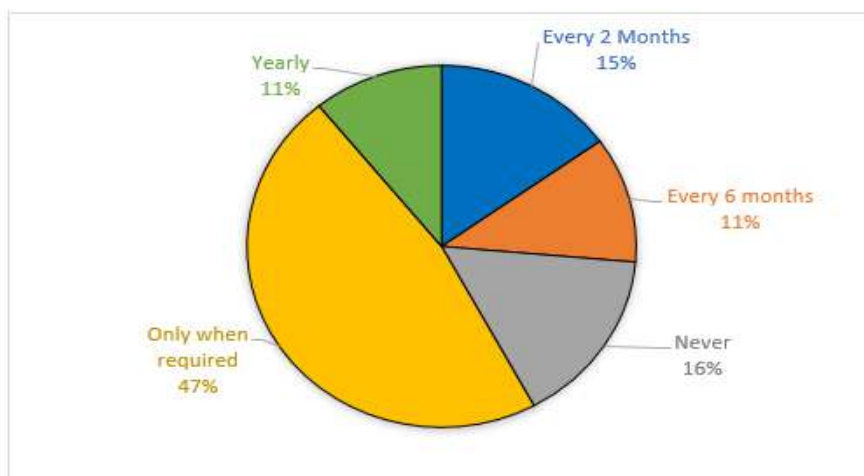


Fig. 8. Frequency of changing passwords

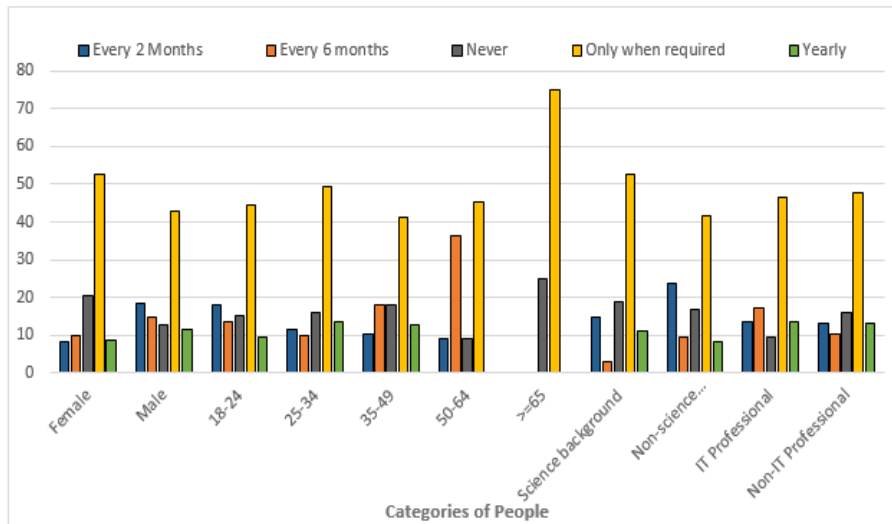


Fig. 9. Frequency of changing passwords in percentage among the various groups of people

TWO-FORM FACTOR (2FA) USAGE

2FA is a type of authentication technique that allows a user to gain access to his or her online account only after providing a combination of at least two pieces of information about what he or she knows (e.g. password, security question), has (identification card, mobile phone) or is (biometric property e.g. finger print). An example of a 2FA can be a pair of passwords and a one-time password (OTP) sent to the mobile phone.

Fig. 10 shows that only 48% of the population surveyed use some form of 2FA with their online accounts. What is more alarming to note is that 28% of the respondents are not aware of 2FA and another 24% who are aware choose not to use this with any of their accounts.

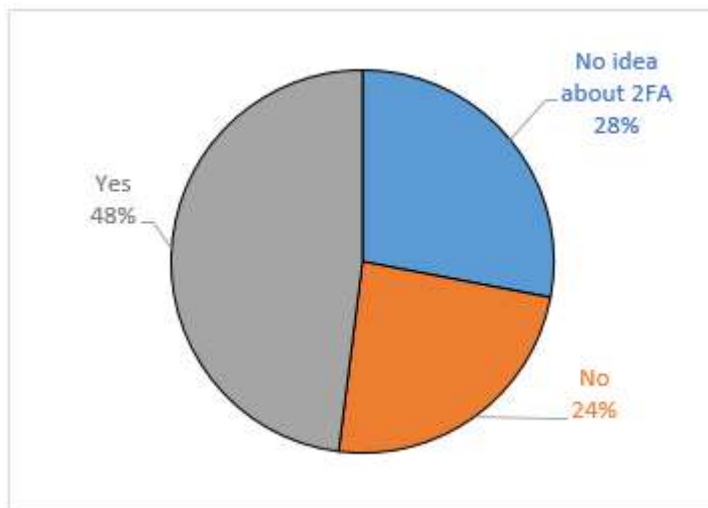


Fig. 10. Use of 2FA among the respondents

Fig. 11 shows that a higher percentage of respondents from each group of people surveyed do not use 2FA except those with some IT background, though it is still far from satisfactory even with this category of people. This shows that people need to be made aware of the importance of 2FA which gives an extra level of protection in addition to having good password practices.

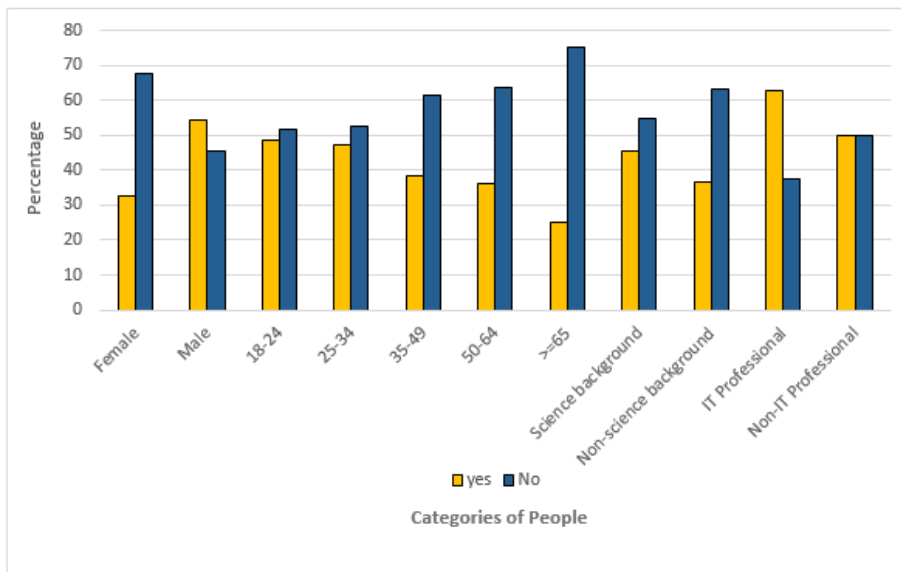


Fig. 11. Use of 2FA among the various categories of respondents

PASSPHRASE USAGE

Passphrase is a form of password with some techniques involved that make them stronger, sometimes longer, easier to remember and more secured. The key is to use a sentence or phrase that would be easy to remember but at the same time difficult for others to guess. Also, these phrases could be tweaked e.g. using only the first letters of every word in the phrase and also varying the use of cases and punctuation marks. For example, a passphrase could be **I l0v3 8ur93r5& Ch!p5** which would be easy to remember as it is personal and also difficult for others because of the combination and style of representation. Another representation of passphrases could be **!L&c0@rd** (for I love burgers and chips on a rainy day).

The use of passphrase has been noticed to be significantly low among the respondents. Only about 21% of the total respondents have ever used passphrases, 79% have never used passphrases, of which 41% have never heard about passphrases.

From **Fig. 12** it can be seen that as age increases, the use of passphrases decreases. Also, those with an IT background or profession have a higher percentage of usage but it is still insignificant.

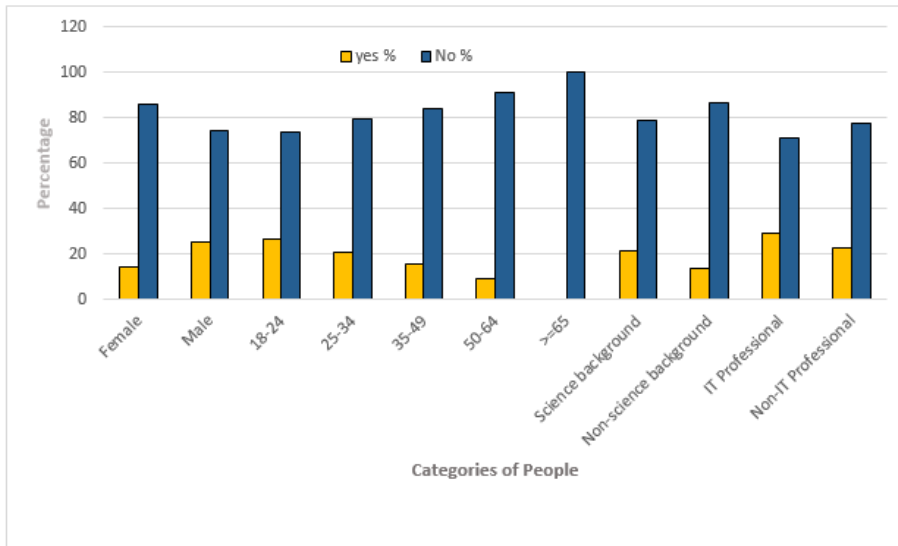


Fig. 12. Passphrase use among the different population types

ACCOUNT COMPROMISE

From the survey, it was found that 30% of the respondents had their online accounts compromised at least once in their lifetime. This, in essence, means approximately one in every three persons is vulnerable to account breach and this is a serious issue from a security point of view.

Fig. 13 shows that the groups of people who have experienced the highest number of account breaches are the males (91%) and those who are 65 years and above (100%). This could attribute to the fact seen earlier that the age group of 65 years and above either never changed their passwords or changed it only when required, shared it with others or might have used numbers or words which have significant importance to them. This would allow a hacker to profile a user and access the account easily. It is also interesting to note that 80% of the female population have either never experienced a breach in their account or suspected so.

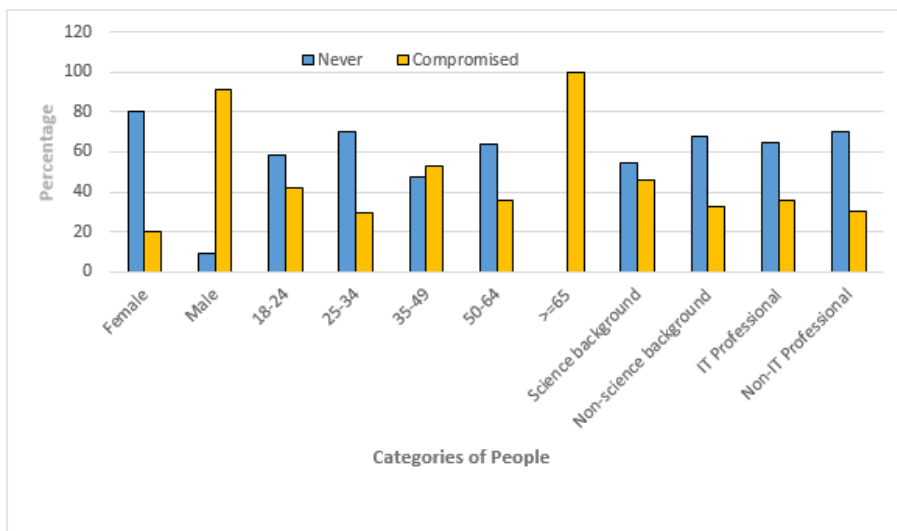


Fig. 13. Percentages of Accounts breached across the different categories of respondents

CONCLUSION

This study shows that even though online passwords have been actively used for over 20 years, the security practices and awareness are still seriously lacking. The age group of 65 years and above were found to be the most vulnerable group as it was seen that 100% of the group had their accounts compromised, followed by the male participants with a 91% of accounts compromised. It is worthy to note that 80% of the female population have either never experienced a breach in their account or do not have any idea if their accounts have been breached.

It was seen that 90% of the participants used words or numbers related to dates, phone numbers or names which had a personal significance or importance in their lives. These are easily remembered, but are highly discouraged as it can be used for profiling or stalking and making a password vulnerable to attack. It was also seen that out of 500 participants, 63% were vulnerable to password attacks as it includes people who never change their password or change it only when asked to do so; 23% would prefer passwords that were easy to remember; 53% would prefer secure passwords; while 24% would like their passwords to be easy and secure at the same time. In practice, however, it may not be feasible to implement easy to remember passwords that are secure at the same time. To achieve this, awareness should be created among users on the use of passphrases, password managers and multi-form factor authentication techniques which would improve online security.

ACKNOWLEDGEMENT

The authors thank all the respondents who participated in the survey and made it possible to carry out the research.

REFERENCES

1. Anonymous. 2019. "Bangladesh Telecommunication Regulatory Commission." 2019. <http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-february-2019>.
2. Armerding, Taylor. 2018. "The 18 Biggest Data Breaches of the 21st Century." CSO. 2018.
3. Awad, Mohammed, Zakaria Al-Qudah, Sahar Idwan, and Abdul Halim Jallad. 2017. "Password Security: Password Behavior Analysis at a Small University." *International Conference on Electronic Devices, Systems, and Applications*, 3–6.
4. CISCO. n.d. "What Is Cybersecurity?" Accessed January 21, 2019. <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>.
5. Florencio, Dinei, and Cormac Herley. 2007. "A Large-Scale Study of Web Password Habits." *Proceedings of the 16th International Conference on World Wide Web - WWW '07*, 657.
6. Gaw, Shirley, and Edward W. Felten. 2006. "Password Management Strategies for Online Accounts." In *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06*, 44. New York, New York, USA: ACM Press.
7. Gott, Amber. 2018. "How Often Should You Change Your Password?" 2018. <https://blog.lastpass.com/2018/08/often-change-password.html/>.
8. Hamidur. 2009. "Internet History of Bangladesh." 2009. <http://wirelessbangladesh.blogspot.com/2009/04/internet-history-of-bangladesh.html>.
9. Klein, Daniel V. 1992. "Foiling the Cracker: A Survey of, and Improvements to, Password Security." *Programming and Computer Software* 17 (3): 5–14.
10. Lamport, Leslie. 1981. "Password Authentication with Insecure Communication." *Communications of the ACM* 24 (11): 770–72.
11. Morris, Robert, and Ken Thompson. 1979. "Password Security: A Case History." *Communications of the ACM* 22 (11): 594–97.
12. Raza, Mudassar, Muhammad Iqbal, Muhammad Sharif, and Waqas Haider. 2012. "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication." *World Applied Sciences Journal* 19 (4): 439–44.
13. Riley, Shannon. 2006. "Password Security: What Users Know and What They Actually Do."

Usability News 8 (1): 2833–2836.

14. Shay, Richard, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. "Encountering Stronger Password Requirements : User Attitudes and Behaviors Categories and Subject Descriptors." *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, 1.
15. Techopedia. n.d. "Password." Accessed January 22, 2019. <https://www.techopedia.com/definition/4042/password>.
16. Tsokkis, Pieris, and Eliana Stavrou. 2018. "A Password Generator Tool to Increase Users' Awareness on Bad Password Construction Strategies." *2018 International Symposium on Networks, Computers and Communications, ISNCC 2018*, 1–5.

RECOMMENDATIONS TO THE SELECTION OF STAKEHOLDERS FOR THE PROTECTION OF CORPORATE INFORMATION AND TELECOMMUNICATIONS SYSTEMS

¹ Osadcha Olha, ² Vialkova Vira¹⁻² Faculty of Information Technology
Taras Shevchenko National University of Kyiv, Ukraine

ANNOTATION. With Next-Generation Firewall (NGFW), businesses can quickly create security policies that comply with business policies, are easy to maintain, and adapt to a dynamic enterprise environment. They reduce response time through automated policy-based actions, while the IT department is able to quickly automate workflows by integrating with administration tools.

KEYWORDS: *next generation firewall, next generation firewall, next-generation firewall, NGFW, policy, ITS, information security management, cybersecurity, threats, network, protection, administration, attacks.*

INTRODUCTION

The main problem of information security management is insufficient funding of this area by organizations, both public and private. If we talk about direct management, employees who have already studied in the field of information security management (as a managerial function) or management of technical means of security at the university begin to work in the direction and successfully use their skills in relevant positions in business or government.

In this report, I want to consider how, with sufficient funding, a competent manager and technician can improve the situation of a private or public enterprise with the help of technical means of information protection.

FORMULATION OF THE PROBLEM

The relevance of the topic is that such organizations are evolving and need protection, so face the following problems:

- increase in information risks due to the emergence of modern threats to information systems;
- free access of personal computers to global resources leads to the dissemination of confidential information;
- a significant increase in the amount of information resources that are accumulated, stored and processed by computers and computers. According to various estimates, today about 90% of the information capital of all existing enterprises is stored in digital form;
- rapid modernization of information systems, which has become a catalyst for the emergence of new threats to information resources. Modern software due to competition and the desire of companies to continuously increase profits enter the market with shortcomings and vulnerabilities.

PROTECTION OF INFORMATION AND TELECOMMUNICATION SYSTEM OF THE ENTERPRISE

If we talk about the functional area, it is at this time that there are problems in choosing the technical means. The information security market offers a wide range of both software and hardware products. In this report, we will consider the next-generation firewall as a universal means of enterprise protection.

Let's analyze the main factors in choosing the products of the next generation of firewalls:

1. The highest priority of the firewall is to prevent attacks and ensure the security of the company. Therefore, the product must have the following capabilities:
 - blocking threats before they enter the network;
 - high-quality next-generation IPS system integrated into the firewall in order to detect hidden threats and quickly neutralize them;
 - filtering URLs to enforce policies on hundreds of millions of URLs;
 - built-in "sandbox" and advanced protection against malware, which continuously analyzes the behavior of files for quick detection and elimination of threats;
 - own anti-virus analytics department, which conducts global threat research and provides NGFW firewalls with the latest updates to prevent emerging threats.
2. Full visibility of events in the network. Your firewall should provide a holistic view of network activity that allows you to evaluate:
 - activity threats to users, hosts, networks and forced downtime; where and when the threat occurred, where else it was in your extended network and what the situation is now; активні програми та веб-сайти;
 - communication between virtual machines, file transfer and more.
3. Flexible management and deployment capabilities. No matter what the size of the business - small, medium or large enterprise - the firewall must meet the specific requirements of our company. On-Demand Management - Choose from the NGFW's built-in "manager" or centralized management system for all devices. Deployment option - locally or in a virtualization system using a virtual firewall. Customize features to suit your needs - just get new subscriptions to get more features.
4. Fast detection time. The next generation firewall should be able to:
 - detect threats in seconds;
 - determine the presence of a successful break within a few hours or minutes;
 - prioritize reports of attacks so that a specialist or IS can quickly and accurately address threats.
5. Integrated security architecture provides automation and reduces the complexity of administration. The next-generation firewall should not be an isolated tool: it should share information and work with other components of the security architecture. Therefore, choose a product that meets the following requirements:
 - easily integrates with other tools from the same manufacturer;
 - automatically exchanges data on threats, events, policies and contextual information with email security tools, endpoints and network components;
 - automates security tasks such as impact assessment, policy setting, and user identification.

Firewall helps to universally protect data of any type of organization.

According to Gartner analysts, next-generation firewalls are guaranteed to provide the following:

- protection against continuous attacks by infected systems;
- standard features for the first generation of firewalls;
- IPS-based application type signatures;
- traffic inspection, including applications, as well as detailed and customizable control at the application level;
- the ability to include information outside the firewall (for example, integration with network directories, "white" and "black" lists of applications);
- the ability to constantly update databases and applications and threats;
- inspection of SSL-encrypted traffic.

The main task is the correct configuration, constant monitoring by the technical staff. In this case, the firewall can prevent most problems.

USING THE SANDBOX MECHANISM FOR ADDITIONAL ITS PROTECTION

Modern cyberattacks are increasingly targeted at a specific industry or a specific company. The unique nature of such threats allows you to easily bypass the classic means of protection - antivirus, firewalls, IPS, mail and web gateways, etc. The ultimate goal of the attackers - to transfer money in their favor, to commit espionage, theft of valuable information, extortion, stop production and disable equipment.

Means of detecting modern attacks, such as sandboxes, as well as preventive measures (incident analysis, localization of infection in the network, actions to prevent attacks and prevent recurrence of incidents) help to effectively neutralize targeted attacks[1-4].

Sandbox - a mechanism for safe execution of programs. Sandboxes are often used to run unverified code from unknown sources and detect viruses and bookmarks[5-8]. In antiviral tools, simple detection methods, such as signature analysis, the presence of behavioral analysis, do not allow to detect carefully planned penetration. And the mechanism of the sandbox launches a file on a regular OS with a complete analysis of what is happening. It is launched at an isolated station under close supervision. This is especially true in cases where the malware pauses at the beginning of its work.

The known and deliberately malicious code will not go to the sandbox, because the verdict is so clear, the firewall will not miss it. Only if the firewall does not have enough data to make a decision, it sends it to the sandbox.

The sandbox can be cloudy, and can work locally in the company, the functionality does not change. The code is run, its behavior is monitored. This way you can track what is happening on the virtual machine and see what this file could do if it got on your PC.

Usually not all firewalls are able to delay the file to get a verdict from the sandbox, you need another agent on the workstation. And then you need that after the file is downloaded, the check in the sandbox is not instantaneous (the manufacturer usually guarantees around 5 minutes). In any case, the user has enough time to open this file. Often it is a set of technical solutions at different levels, which serves one task.

Manufacturers maintain specialized knowledge bases that allow you to identify more threats. There are reputational checks, in which case the reputational model is used. The necessary information gets there, and then on its basis the indicator of compromise is formed. That is, it detects a malicious file, we understand how it works, and in this case it is more efficient to send information about it to all PCs. If he accesses a file, renames it, the combination of these factors can mean an indicator of compromise, sending it to everyone, we can quickly detect vulnerabilities without resorting to the capabilities of the sandbox[9-11].

Harm testing should not be the first in the line of defense. Initially, it can be firewall, antispam, anti-phishing, which are embedded in the mail system, proxy servers, intrusion detection at the network level, and only after the file passes these barriers is the sandbox - the last resort. At this stage, it is necessary to understand that the efficiency of file verification requires large resources, a large flow of such files will incur additional costs. To reduce them, you must first make the most effective use of existing remedies.

CONCLUSION

You should be especially careful to choose equipment that protects your LAN. You need to know what set of features should be included in the device for a specific situation and company. If the company needs to meet high safety requirements, you need to choose NGFW.

Recently, the number of cyberattacks on businesses has increased significantly. In this regard, the author recommends using NGFW to protect the perimeter of the network and internal services of the company.

In addition, the use of equipment with a sandbox mechanism is recommended. With its advent, the security of many companies has risen to a new level.

REFERENCES:

1. Jithin Aby Alex, Being a firewall engineer: An operational approach: A Comprehensive guide on firewall management operations and best practices, 1st Edition, 2018.
2. Aaron Woland, Vivek Santuka, Mason Harris, Jamie Sanbower, Integrated Security Technologies and Solutions - Volume I, 1st Edition, 2018.
3. What are the advantages of next-generation firewalls? Review of popular NGFW . Access mode: <https://www.ixbt.com/live/market/v-chem-preimuschestva-fayrvolov-sleduyuschego-pokoleniya-obzor-populyarnyh-ngfw.html>.

4. Site organization Gartner. Access mode: <https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws>
5. 5 critical mistakes when evaluating a next-generation firewall. Access mode: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/white-papers/five-critical-mistakes-to-avoid-when-evaluating-a-ngfw.pdf.
6. A. Gagnidze., M. Iavich., G. Iashvili, Analysis of Post Quantum Cryptography use in Practice, Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 2, 2017, p.29-36.
7. A. Gagnidze, M. Iavich, G. Iashvili// Novel Version of Merkle Cryptosystem, BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 11, no. 4, 2017, p. 28-33
8. NGFW or UTM: How to Choose. Access mode: <https://www.watchguard.com/en/wgrd-resource-center/help-me-choose>
9. 5 Tips for Choosing a Next-Generation Firewall. Access mode: <https://www.cisco.com/c/dam/en/us/products/collateral/security/next-gen-firewall.pdf>.
10. Overview of programs for working with virtual sandboxes. Access mode: <https://www.ixbt.com/soft/sandboxes.shtml>
11. Гагнидзе А.Г., Явич М.П., Иашвили Г.Ю. Пост-квантовые криптосистемы // Современные научные исследования и инновации. 2016. № 5 [Электронный ресурс]. URL: <http://web.snauka.ru/issues/2016/05/67264>

АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ И МЕТОДИК ДИАГНОСТИРОВАНИЕ КИБЕРНЕТИЧЕСКОЙ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЕ В КИБЕРНЕТИЧЕСКОМ ПРОСТРАНСТВЕ

Козубцова Леся Михайловна, Военный институт телекоммуникаций и информатизации, г. Киев, Украина
к.т.н., доцент Кит Григорий Васильевич, Ивано-Франковский филиал Открытого международного университета развития человека «Украина» г. Ивано-Франковск, Украина
к.т.н., профессор РАЕ Козубцов Игорь Николаевич, Научный центр связи и информатизации Военного института телекоммуникаций и информатизации, г. Киев, Украина

АННОТАЦИЯ. В статье проведен анализ известных методов и методик диагностирование кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве. Установлено, что на данное время существуют несколько однотипных решений, у которых отсутствуют объяснения каким образом осуществляется расчет некоторых составляющих параметров.

ЦЕЛЮ СТАТЬИ является апробация результатов анализа известных методов и методик диагностирование кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве.

Практическое значение результата заключается в обосновании необходимости усовершенствования известных однотипных результатов до уровня их возможного практического применения.

КЛЮЧЕВЫЕ СЛОВА: анализ, методика, диагностирование, кибернетическая устойчивость, защищенность, надежность, живучесть, информационная система специального назначения, деструктивное информационное влияние.

ANALYSIS OF KNOWN METHODS AND TECHNIQUES DIAGNOSTICS OF CYBERNETIC STABILITY OF THE FUNCTIONING OF A SPECIAL PURPOSE INFORMATION SYSTEM IN CYBERNETIC SPACE

Lesya Kozubtsova, Military institute of telecommunications and informatization, Kiev, Ukraine
Ph.D., associate Professor Gregory Kit, Ivano-Frankivsk branch of the Open international University for human development "Ukraine" Ivano-Frankivsk, Ukraine

Ph.D., Professor RAE, Igor Kozubtsov Scientific center of communication and Informatization of the Military Institute of telecommunications and Informatization, Kiev, Ukraine

ABSTRACT. The article analyzes the known methods and techniques for diagnosing the cybernetic stability of the functioning of a special purpose information system in cybernetic space. It is established that at this time there are several solutions of the same type, which do not have explanations of how to calculate some of the component parameters.

The purpose of the article is to test the results of the analysis of known methods and techniques for diagnosing the cybernetic stability of the functioning of a special purpose information system in cybernetic space.

The practical significance of the result is to justify the need to improve the known results of the same type to the level of their possible practical application.

KEYWORDS: analysis, methodology, diagnostics, cybernetic stability, security, reliability, survivability, special-purpose information system, destructive information influence.

ВВЕДЕНИЕ

Современные информационные системы специальных пользователей используются для решения задач широкого спектра научных и производственных задач сбора, обработки, накопления и хранения информации с ограниченным доступом, управления критическими объектами в реальном масштабе времени. Решение данных задач является актуальным в повседневной деятельности специальных пользователей Украины и имеет важное значение для национальной безопасности Украины. Поскольку функционирование информационных системы специальных пользователей предусмотрено в киберпространстве, в котором существуют кибернетические уязвимости и угрозы [27; 28; 24], поэтому выдвигается высокий уровень требований к адекватности,

оптимальности, оперативности, устойчивости, непрерывности, скрытности [26; 1; 4; 23]. Из перечисленных требований, в диссертационном исследовании ограничимся рассмотрением «кибернетической устойчивости». Исходя из этого возникает научная задача разработки нового инструментария диагностирования кибернетической устойчивости функционирования ИС СН.

Под «кибернетической устойчивостью функционированием ИС СН» будем понимать состояние ее защищенности, которое обеспечивает устойчивое функционирование в условиях преднамеренных и случайных действий кибернетических деструктивных информационных воздействий (ДИВ).

Если не уделить должного внимания решению данного вопроса, то в контексте описания «Будущее безопасность среда 2030. Анализ стратегического предвидения» выполнено исследователи Военного института телекоммуникаций и информатизации в работах [10; 14; 13; 11] прогнозируют неминуемое наступление коллапса в различных сферах автоматизации и информатизации:

опасность искажения, подмена информации во всемирно известных электронных научно-технических библиотеках, энциклопедиях, наукометрических базах (библиотека им. В.И. Вернадского, Wikipedia, SciVerse Scopus, Web of Science (WoS), Google Scholar, и тому подобное [20; 12]);

вмешательство в работу оборудования – атаки на компьютеры или серверы, которые обеспечивают работу гражданских коммуникаций (нарушение системы водоснабжения, электроэнергии, транспорта и т. п.) [5];

нарушение функционирования автоматизированных систем управления войсками (функциональный сбой и несанкционированное управление войсками и вооружением, как примера ход событий в научно-фантастическом фильме «Terminator», где искусственный интеллект сети «SkyNet» получив доступ к управлению системой противоракетной обороны и ядерным вооружением Вооруженных сил США создал условия для уничтожения человечества. И хотя на первый взгляд это выглядит фантастически, но сегодняшние «кибервойны» и «киберпространство», из научно-фантастического романа У. Гибсона «Нейромант» (1982), перекочевали в современную реальность [2].

За перечисленных последствий возможно нарушение функционирования информационно-телекоммуникационных систем, в результате так называемого коллапса. До появления коллапсов в информационно-телекоммуникационных системах в следствие кибернетических угроз, были известны лишь «экономический коллапс», «экологический коллапс», «финансовый коллапс», «политический коллапс», «социальный коллапс» и др.

Таким образом, если не уделить должного внимания решению данного вопроса, то прогнозируют неминуемое наступление коллапса в различных сферах автоматизации и информатизации, что приведет к нарушению национальной безопасности Украины.

ЦЕЛЬ СТАТЬИ

Апробировать результаты анализа известных методов и методик диагностирование кибернетической устойчивости (компонентов устойчивости) функционирования информационной системы специального назначения в кибернетическом пространстве

ОСНОВНОЙ РЕЗУЛЬТАТ

В соответствии с целью исследования проанализируем известные существующие подходы, методы и методики диагностирование информационной системы специального назначения в такой последовательности: «кибернетическая устойчивость», «кибернетическая надежность», «кибернетическая живучесть».

Проанализируем известные методы и методики диагностирование кибернетической устойчивости информационной системы специального назначения. Решение данной научной задачи начато с поиска в открытых источниках информации по ключевым словам «подходы методы и методики диагностирование кибернетической устойчивости функционирования информационной системы специального назначения».

На данный момент времени, благодаря Будапештской инициативе открытого доступа к научным публикациям (The Budapest Open Access Initiative) найдены следующие научные публикации [7; 21; 22; 3], в которых объектом исследования выступала киберустойчивость объектов критической информационной инфраструктуры (КИИ).

Проработав данные работы было установлено, что методика оценки киберустойчивости КИИ в общем виде состоит из следующих этапов:

1. Этап оценки киберустойчивости каждого объекта КИИ ($K_{\text{ОКИИ}}^{\text{УО}}$) отдельно (1).

$$K_{\text{ОКИИ}}^{\text{УО}} = K_{\text{ОКИИ}}^{\text{ЖИВ}} \times K_{\text{ОКИИ}}^{\text{ПОМ}} \times K_{\text{ОКИИ}}^{\text{НАД}} \quad (1)$$

где $K_{\text{ОКИИ}}^{\text{ЖИВ}}$ – киберживучесть – живучесть объекта КИИ;

$(K_{\text{ОКИИ}}^{\text{УО}})$ – киберзащищенность однозвенного объекта КИИ;

$K_{\text{ОКИИ}}^{\text{над}}$ – кибернадежность однозвенного объекта КИИ.

1.1 Оценка однозвенного объекта КИИ.

Оценка киберзащищённости – вероятность выхода из строя i -го технического средства обработки информации (ТСОИ) в условиях ДИВ.

Оценить коэффициент связанности i -го ТСОИ и его вклад в целевую функцию объекта КИИ.

Оценка киберживучести – предела состояний однозвенного объекта КИИ.

1.2. Оценка многозвенного объекта КИИ.

Оценка киберзащищённости – вероятность выхода из строя j -го однозвенного объекта КИИ в условиях воздействия ИИИ.

Оценить коэффициент связанности j -го однозвенного объекта КИИ и его вклад в целевую функцию многозвенного объекта КИИ.

Оценка киберживучести – предел состояний многозвенного объекта КИИ.

2. Этап оценки киберустойчивости взаимодействующих объектов КИИ (стволов объектов КИИ).

Оценка киберзащищённости – вероятность выхода из строя n -го многозвенного объекта КИИ в условиях воздействия ДИВ.

Оценить коэффициент связанности n -го многозвенного объекта КИИ и его вклад в целевую функцию многозвенного объекта КИИ.

Оценка киберживучести – предел состояний ствола КИИ.

3. Этап оценки киберустойчивости КИИ через сумму устойчивости ее элементов с учетом их коэффициента связности.

Оценка киберживучести КИИ в целом, соответственно до текущего состояния стволов КИИ и степенью важности, в данный момент времени, выполнения ими функций.

Для нашего исследования ценными являются работы [7; 21; 22], которые исследовали киберустойчивость КИИ. Однако авторы не раскрывают ни подходов, ни алгоритма оценки коэффициентов связности. В следствие этого невозможным практическое использование известной методики для специальных пользователей, что подтверждено попыткой экспериментальной проверки во время исследования на военных стратегических командно-штабных учениях с органами военного управления, войсками (силами) Вооруженных Сил Украины “Несокрушимая устойчивость – 2017” в период с 11.09.2017 по 26.09.2017 г. офицерами-исследователями Научного центра связи и информатизации Военного института телекоммуникаций и информатизации. Также известную методику нельзя сравнить с предложенной нами в диссертации, поскольку отсутствие сведений относительно коэффициентов связанности. Возможна через то, что разработкой методики занимались работники Краснодарского высшего военного училища им. генерала армии С.М. Штеменко, Российской Федерации (РФ) И.Д. Королев и Г.И. Захарченко и отдельные результаты могли составлять государственную тайну РФ, как следствие не подлежали к публикации в открытых источниках. Не исключение, детализация методики опубликована в научном сборнике с грифом «Секретно».

Таким образом, для обеспечения диагностирование кибернетической устойчивости ИС СН нуждается в совершенствовании известных результаты [7; 21; 22].

На основании отсутствия сведений относительно нахождения коэффициентов связанности, необходимо усовершенствовать данную методику путем адаптации ее для обеспечения диагностирование кибернетической устойчивости ИС СН. Данное решение будет одной из научных задач нашего диссертационного исследования.

Проанализируем известные методы и методики диагностирование кибернетической надежности информационной системы специального назначения.

Надежность – это комплексная свойство, что включает в себя безотказность, ремонтпригодность и сохранность [19].

Безотказность – свойство системы или ее элементов непрерывно выполнять востребованную функцию в заданном интервале времени или некоторые наработки. Нарботкой называют интервал времени, в течение которого изделие находится в состоянии функционирования.

Ремонтпригодность – способность системы при заданных условиях эксплуатации к поддержке или восстановлению состояния за счет технического обслуживание, в котором она может выполнять востребованную функцию.

Сохранностью называют способность системы выполнять востребованную функцию в течение и после хранения или транспортировки.

Комплексность понятие «надежность», с учетом выше сказанного, делает его фундаментальным, таким всесторонне охватывает техническую эксплуатацию систем и элементов. В свою очередь, надежность является

составной более широкого понятие эффективность, под которой понимают способность системы выполнять заданные функции с необходимой качеством.

Показателями надежности есть количественные характеристики способности, что составляют надежности системы.

Поскольку отказа и сбоев имеют случайный характер, то показатели надежности являются вероятностными величинами и при исследовании прибегают к методов, что используются в теории вероятности и математические статистике.

Наиболее распространенными количественными характеристиками надежности есть: вероятность безотказной работы в определенный интервал времени – $P(t)$; среднее наработки до первого отказа – T_{CP} ; вероятность отказа – $Q(t)$; наработки на отказ – t_{CP} ; частота отказов – $a(t)$; интенсивность отказов – $\lambda(t)$; параметр потока отказов – $\omega(t)$; функция готовности – $K_T(t)$; коэффициент готовности – K_T .

Выбор количественных характеристик надежности зависит от вида объекта исследования – восстанавливаемого или невосстанавливаемого.

Возобновляемыми называют объекты, которые допускают ремонт в процессе выполнения своих функций. При отказе такие объекты прекращают функционирования только на период устранения отказа. Не возобновляемые объекты в процессе выполнения своих функций не допускают ремонта.

Следует отметить, что большинство элементов (компонентов) ИС СН построены по микросхемной технологии, поэтому ее ремонт (микросхемы) невозможен, а соответственно объекты – не возобновляемые.

Кроме того, в нашем исследовании область ограничивается оперированием только обобщенной надежностью, которая является составной кибернетической устойчивости. Поэтому в дальнейшем исследовании расчет составляющих надежности мы упускаем, путем введением выше указанного ограничения.

Для выяснения существующих подходов, методов и методик диагностирование кибернетической надежности информационной системы специального назначения осуществим поиск в открытых источниках информации по ключевым словами «подходы, методы и методики диагностирование кибернетической надежности функционирования информационной системы специального назначения».

Установлено, что в открытых научных источниках [7; 21; 22; 3] упоминается кибернадёжность, как составляющая расчетной формулы киберустойчивости.

Следует отметить, что кибернадёжность в методике оценки устойчивости функционирования объектов КИИ не рассчитывается, а принимается следующее предположение: техническая надёжность за счет ряда специальных мероприятий по повышению оперативности устранения технических и программных отказов ТСОИ (например, за счет кластеризация серверов, резервирование средств с низкой надёжностью компонентов ТСОИ) при своевременном и качественном проведении технического обслуживания считается приближенно малой, то есть $P_{TH} = 1$.

Как свидетельствует современная практика, для обеспечения надёжной работоспособности ИС применяют подход обновления ТСОИ до их предельных сроков наработки на отказ вследствие морального или физического старения.

Нельзя ограничиваться только физическим износом или старением некоторых объектов ИС. Для всех без исключения объектов ИС характерно моральное старение или экономическое старения. Под фактором морального старения понимается наступления события, когда заказчику, пользователю или тем, кто эксплуатирует ИС доступны объекты с лучшими характеристиками по показателю «цена/качество» или с лучшими функциональными возможностями, чем те, которые содержатся в данной системе. Фактор экономического старения имеет место тогда, когда экономически нецелесообразна дальнейшая эксплуатация любого объекта или группы объектов, или ИС в целом, хотя их физический износ еще не наступил и даже не скоро настанет. Для ИС типична более высокая скорость морального старения в сравнении с экономическим, и тем более физическим старением или износом (см. рис. 1) [25, с. 22]. На этом рисунке приведены зависимости от времени показателей цена/качество (Ц/Я) в отношении морального старения (кривая $S_{MOP}(t)$), старения через экономическую нецелесообразность дальнейшей эксплуатации объекта (кривая $S_{ЭЖОН}(t)$), физического старения или износа (кривая $S_{Физ}(t)$).

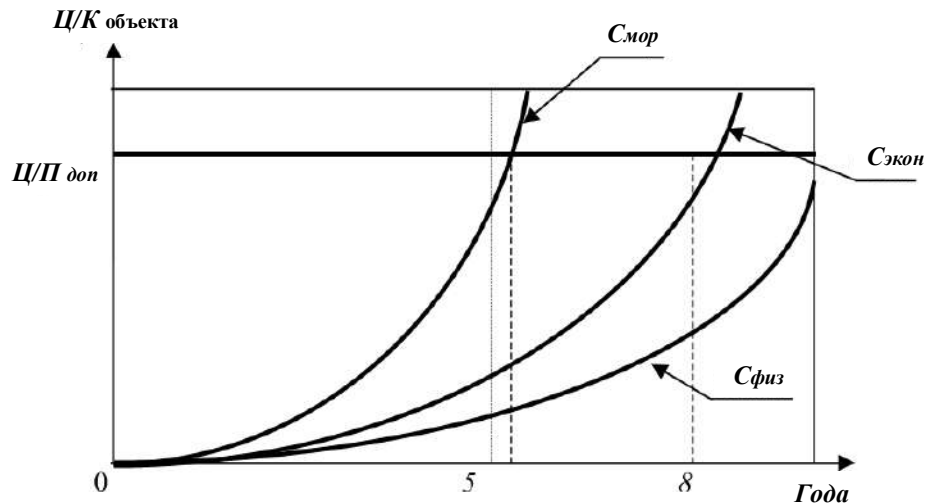


Рисунок 1 – Графики изменений скорости морального, экономической нецелесообразности или физического старения объекта ИС по критериям цена/качество (Ц/К) с учетом допустимого значения этого критерия

Эти зависимости носят качественный характер. Однако практика показывает, что уже через 5 лет эксплуатации, вследствие морального старения, целесообразно заменять ряд объектов ИС на более новые, хотя физическое старения или износ таких объектов далеки от предельного состояния. Это связано с тем, что кривая морального старения объекта пересекает и превышает предельно допустимый уровень показателя Ц/Я и, следовательно, дальнейшая его эксплуатация нерентабельна.

На рис.2, подано график кривой изменения интенсивности отказов средств в течение срока эксплуатации. Как практика показывает I фаза от 0 до t_1 имеет краткое промежуток времени, поэтому можно ею пренебречь. А за период от t_1 до t_2 превышает моральное старение.

Исходя из этого, авторы работы [3], также принимают ограничения, что $P_{ТН} = 1$, как и в работах [7; 21; 22] на аналогичных этапах в расчете объектов КИ Объединенной энергосистемы Украины. Тогда расчетная формула (1) примет упрощенного вида (2):

$$K_{ОКИИ}^{yo} = K_{ОКИИ}^{жив} \times K_{ОКИИ}^{пом} \quad (2)$$

Таким образом, анализ научной литературы по обеспечению кибернетической надежности ИС показал, что практически не рассмотрены вопросы, которые связанные с разработкой методов диагностирования кибернетической надежности в разных условиях их функционирования. Данное решение будет одной из частичных научных задач нашего исследования.

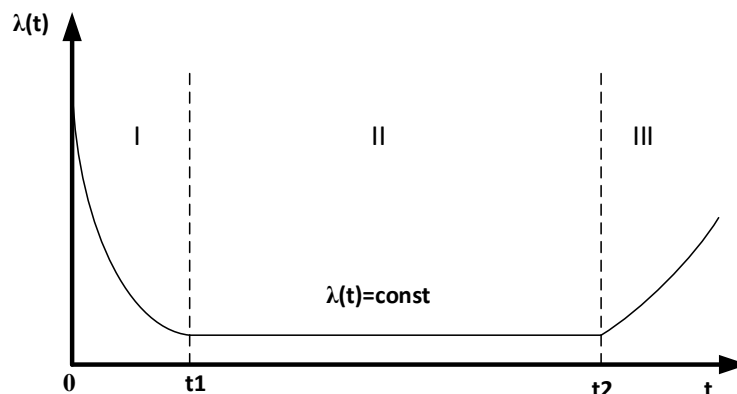


Рисунок 2 – График кривой изменения интенсивности отказов средств в течение срока эксплуатации

Проанализируем известные методы и методики диагностирование кибернетической живучести информационной системы специального назначения. Решение данной научной задачи начато с поиска в открытых источниках информации по ключевым словами «подходы, методы и методики диагностирование

кибернетической живучести функционирования информационной системы специального назначения».

В открытых научных источниках [7; 21; 22] упоминается киберживучесть, как составляющая киберустойчивости и рассчитывается на следующих этапах:

1.1 Оценка однозвенного объекта ИС.

Оценка киберживучести – предела состояний однозвенного объекта КИИ. $K_{ОКИИ}^{жил}$ – киберживучесть – живучесть объекта КИИ, трактуется как вероятность сохранения его работоспособности (выживание) в условиях выхода из строя технических средств обработки информации, то есть по сути – вклад каждого базового элемента однозвенного объекта КИИ в исполнение им целевой функции.

1.2. Оценка многозвенного объекта ИС. Оценка киберживучести – предела состояний многозвенного объекта ИС.

2. Этап оценка киберстойкости взаимодействующих объектов ИС (стволов объектов ИС).

Оценка киберживучести – предел состояний ствола ИС.

3. Этап оценки киберстойкости ИС как сумма устойчивости ее элементов с учетом их коэффициента связности. Оценка киберживучести ИС в целом, соответственно до текущего состояния стволов ИС и степенью важности, в данный момент времени, выполнения ими функций.

В указанной методике авторами работ [7; 21; 22] не приведены механизма диагностирования и расчетных соотношений.

Следует отметить, что авторы работы [3] позаимствовали наработки с научных работ [7; 21; 22] и в аналогичных этапах расчета киберживучести объектов КИ Объединенной энергосистемы Украины. Они также не приводят математический аппарат расчета.

Поскольку в расчетной формуле кибернетической устойчивости (1) содержится как кибернетическая составляющая живучесть, поэтому возникает необходимость в определении киберживучести.

Анализ проработанной научной литературы по вопросу кибернетической живучести показал, что практически не рассмотрены вопросы, которые связанные с разработкой методов диагностирования кибернетической живучести в информационных системах в различных условиях их функционирования в кибернетическом пространстве. Вычисления составляющей кибернетической живучести и диагностирование будет частичной научной задачей нашего диссертационного исследования.

Недостающий компонент в формуле (1) киберзащищенности предлагается получать по результатам его диагностирования по ранее разработанной методике [8; 18].

Постановка научной задачи на диссертационное исследование

Для обеспечения эффективного и бесперебойного функционирования информационной системы специального назначения в кибернетическом пространстве в условиях действий ДИВ определим приоритетные направления научного исследования:

усовершенствование нормативно-правовой базы в сфере кибернетической безопасности;

разработка и реализация адекватных организационных мероприятий;

разработка и применение комплексов и систем кибернетической защиты на принципах масштабирования и дополнения [16];

периодическое тестирование [9], обучение и аттестация штатного личного состава ответственного за эксплуатацию и обслуживание [15];

Как показывает практика, на сегодняшний день, ни одно из этих решений отдельно не может обеспечить необходимый уровень защиты.

Поэтому, цель исследования должна заключаться в необходимости обосновании теоретических и практических основ ранней диагностики кибернетической устойчивости и ее настроек для обеспечения эффективного и бесперебойного функционирования информационной системы специального назначения в кибернетическом пространстве в условиях неизбежных кибернетических действий ДИВ.

Это обеспечит повышение кибернетической безопасности и готовности ИС СН к выполнению поставленных задач без значительной потери активов на время восстановления.

В соответствии с выше рассмотренным нами определены основные задачи будущих исследований и их решения:

1. Анализ содержание понятия кибернетической устойчивости в научных исследованиях [6].

2. Обоснования методики диагностирования кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве [17; 29].

3. Обоснования методики расчета составляющих показателей кибернетической устойчивости функционирования информационной системы в кибернетическом пространстве.

4. Обоснования методики диагностирование кибернетической защищенности информационной системы с учетом ДИВ.

Перечисленные научные задачи исследования, их структурно-логический связь продемонстрировано на структурно-функциональной схеме, что одновременно определяет последовательность исследования и связь между результатным, представлены на рис.3.

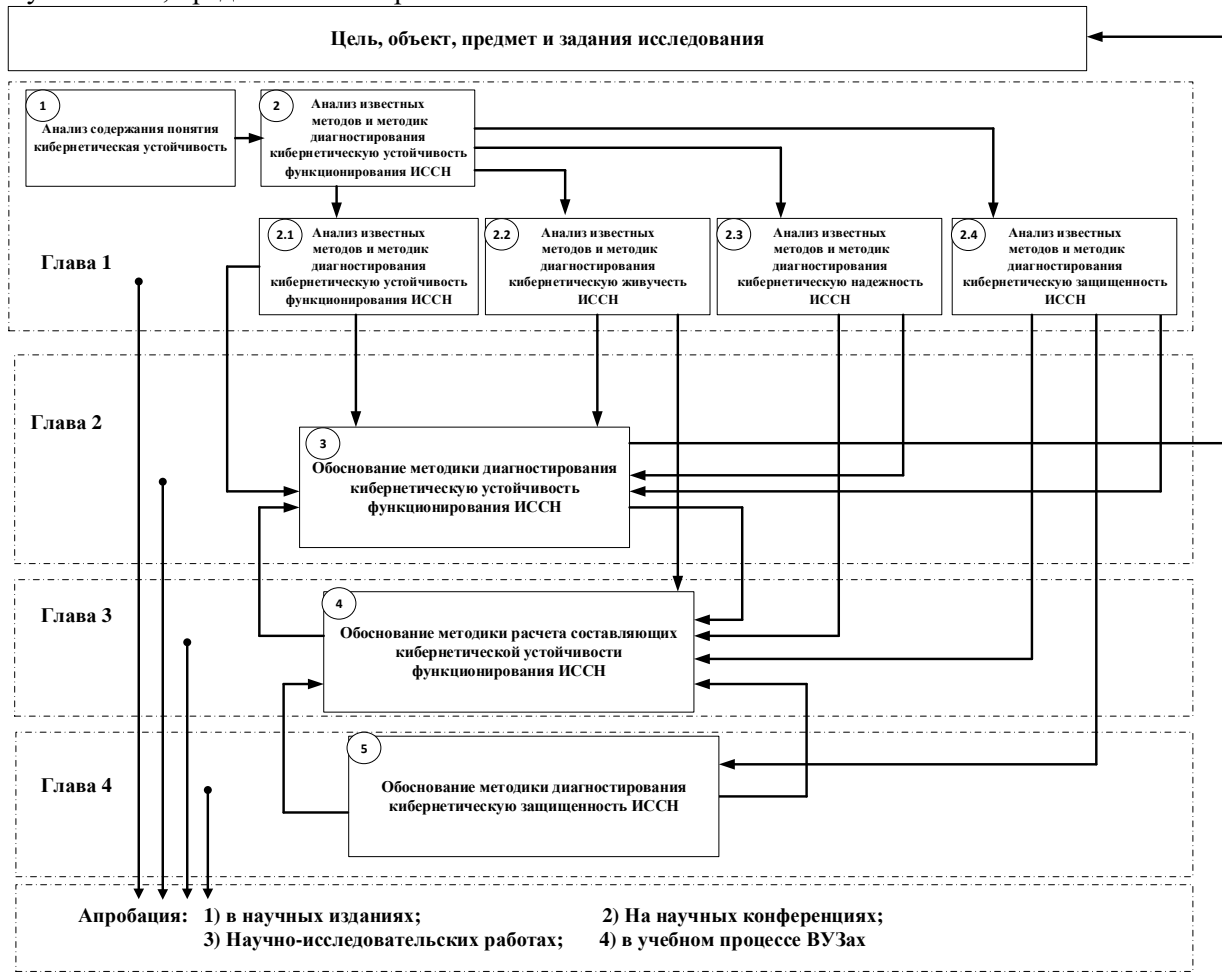


Рисунок 3 – Структурно-функциональная схема научного исследования

ВЫВОДЫ.

Важнейшими научными и практическими результатами являются:

1. Проанализированы известные методы и методики диагностирование кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве. Установлено, что в настоящее время отсутствует методика диагностирование кибернетической устойчивости.

2. Таким образом, цель исследования должна заключаться в необходимости обоснования теоретических и практических основ ранней диагностики кибернетической устойчивости и ее настроек для обеспечения эффективного и бесперебойного функционирования информационной системы специального назначения в кибернетическом пространстве за неизбежных условий кибернетических действий деструктивных информационных воздействий.

3. Полученные научные результаты исследования является основанием к формированию научных задач на разработку методики диагностирование кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. Боговик А.В., Игнатов В.В. Теория управления в системах военного назначения. СПб.: ВАС, 2008. 460 с.

2. Гибсон У. Нейромант: Фантастический роман / Пер. с англ. Е. Летова, М. Пчелинцева. М.: Аст; СПб.: Terra Fantastica, 2000. 317с.
3. Гончар С.Ф., Герасимов Р.П., Ткаченко В.В. Дослідження проблеми кіберживучості Об'єднаної енергосистеми України // Міжнародний науково-теоретичний журнал «Електронне моделювання». 2019. Т.41. №1. С. 43 – 54.
4. Давыдов А.Е., Савицкий О.К., Максимов Р.В. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. Москва: Воентелеком, 2015. 520 с.
5. Даник Ю.Г. Вдовенко С.Г. Ланцюгові ефекти в кібердіях // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2019. № 64. С. 71 – 90.
6. Забара С.С., Хлапонин Ю.И., Козубцова Л.М. Анализ понятия кибернетической стойкости информационной системы специального назначения // Materials of the XVI International scientific and practical Conference Science without borders – 2020 (March 30 – April 7, 2020): Sheffield. Science and education LTD. Pp. 20 – 23. ISBN 978-966-8736-05-6.
7. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Научные технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52 – 61.
8. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Методика оцінки кібернетичної захищеності системи зв'язку організації // Сучасні інформаційні технології у сфері безпеки та оборони. 2018. №1 (31). С. 43 – 46.
9. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Стратегічні напрямки анкетування спеціалістів інформаційної та кібернетичної безпеки для з'ясування рівня кібернетичної захищеності організації // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). К.: Нац. акад. СБУ, 2018. С. 89 – 91.
10. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П., Штонда Р.М, Черноног О.О. Обґрунтування поняття терміну глобального колапсу інформаційно-телекомунікаційних систем // Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” (15 березня 2019 року, м. Харків). Харків. Національна академія Національної гвардії України, 2019. С. 57 – 59.
11. Козубцов І.М., Козубцова Л.М., Терещенко Т.П., Куцаєв В.В. Глобальний колапс інформаційно-телекомунікаційних систем в наслідок порушення роботи сучасних інформаційних технологій у секторі безпеки і оборони // Міжнародна науково-практична конференція «Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи» (м. Одеса 12-13 вересня 2019 р.). Одеса. Військова академія, 2019. С. 229 – 230.
12. Козубцов І.М., Куцаєв В.В. Філософія інформаційної безпеки в умовах її кібернетичного розповсюдження в сучасній динамічній науковій картині світу на прикладі надання знань молодим вченим та студентам // Гілея: науковий вісник. Збірник наукових праць. К.: ВІР УАН, 2013. Вип. 73(№6). С. 291 – 293.
13. Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П. Кібернетичні атаки як механізм створення штучного глобального колапсу інформаційно-телекомунікаційних систем // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). К.: Нац. акад. СБУ, 2019. С.221 – 223.
14. Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П. Тлумачення терміну “кібернетична безпека” через призму кібернетики // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). К.: Нац. акад. СБУ, 2019. С.219 – 221.
15. Козубцов І.М., Куцаєв В.В., Срібний С.П. Концепція нового підходу до підготовки фахівців з інформаційною безпекою // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів науково-практичної конференції (Київ, 20 березня 2014 року): у 2 ч. Ч.1. К.: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. С. 170 – 175.
16. Козубцов І.М., Куцаєв В.В., Ткач В.О., Козубцова Л.М. Концептуальний підхід до побудови системи кібернетичної безпеки стаціонарних інформаційно-телекомунікаційних вузлів України на принципах масштабування та доповнення // Науково-практичний журнал. Сучасні інформаційні технології у сфері безпеки та оборони. Національний університет оборони України. 2015. №3(24) С.

47 – 55.

17. Козубцова Л.М. Апробація структури методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі // Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” (17 березня 2020 року, м. Харків). Харків. Національна академія Національної гвардії України, 2020. С. 141 – 142.
18. Куцаєв В.В., Радченко М.М., Козубцова Л.М. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку // Збірник наукових праць ВІТІ. К.: ВІТІ, 2018. № 2. С. 67 – 76.
19. Ложков А.В. Методика оценки надежности вычислительной сети // Научные записки молодых исследователей. 2014. № 4. С. 28 – 31.
20. Мараховський Л.Ф., Козубцов І.М. Філософія формування цілісної динамічної наукової картини світу знань : реалізація ідеї академіка Володимира Івановича Вернадського // Філософський журнал Донецького національного технічного університету „Ноосфера і цивілізація”. 2013. Вип. 1(14). С. 108 – 116.
21. Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И. Критическая информационная инфраструктура: оценка устойчивости функционирования // Радиопромышленность. 2018. Т. 28. №4. С. 59 – 67.
22.] Минаев В.А., Крупенин А.В., Королев И.Д., Бондарь К.М., Захарченко Р.И. Оценка устойчивости функционирования критической информационной инфраструктуры // «Вестник РосНОУ», серия «Сложные системы: модели, анализ и управление». 2018. Выпуск 4. Информатика и вычислительная техника. С. 129 – 138.
23. Моисеев В.С., Козар А.Н., Дятчин В.В. Информационная безопасность автоматизированных систем управления специального назначения: Монография. Казань. Казанское высшее артиллерийское командное училище (военный институт) имени маршала артиллерии М.Н. Чистякова, 2006. – 384 с.
24. Слипченко В.И. Войны шестого поколения оружие и военное искусство будущего. М.: Вече, 2002. 382 с.
25. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с.
26. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012, 296 с.
27. Department of Defense Instruction. Number 8530.01, March 7, 2016 “Cybersecurity Activities Support to DoD Information Network Operations”. 44 p. <https://apps.dtic.mil/dtic/tr/fulltext/u2/1005132.pdf>.
28. Department of Defense Instruction. Number 8530.01, March 7, 2016, Incorporating Change 1, July 25, 2017. “Cybersecurity Activities Support to DoD Information Network Operations”. 45 p. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf>.
29. Zabara S., Khlaponin Yu., Kozubtsova L. Methods for diagnosing cybernetic stability of a special purpose information system // Scientific and Practical Cyber Security Journal (SPCSJ). 2020. Vol. 4(1). Pp. 80 – 86 ISSN 2587-4667 Scientific Cyber Security Association (SCSA). URL: <https://journal.scsa.ge/wp-content/uploads/2020/04/10-41-spcsj.pdf>.

ეკონომიკური დაზვერვისა და კონტრდაზვერვის მიმართულებები
**THE DIRECTIONS OF ECONOMIC INTELLIGENCE AND COUNTER-
INTELLIGENCE**

ილია ხუციშვილი სსიპ-შსს აკადემია - სამართლის მაგისტრი „ნიუ ვიჟენ“ უნივერსიტეტი -
სამართლის დოქტორანტი

Ilia Khutsishvili LEPL - Academy Of The Ministry Of Internal Affairs Of Georgia- Master's Academic Degree of
Law New Vision University - The Ph.D Programme in Law, Doctoral Student

ანოტაცია: სახელმწიფოს უსაფრთხოების უზრუნველყოფა ერთ-ერთ მნიშვნელოვან სექტორს ეკონომიკა წარმოადგენს, სწორედ ამიტომ, სახელმწიფოთა სამსახურები სხვადასხვა მეთოდის გამოყენებით ცდილობენ პოტენციურად მოწინააღმდეგე სახელმწიფოთა ეკონომიკის დასუსტებას ან ისედაც ცუდი ეკონომიკის მქონე ქვეყანაზე ახარხებენ მაქსიმალური კონტროლის დაწესებას.

ეკონომიკური დაზვერვა, როგორც სადაზვერვო საქმიანობის ერთ-ერთი მიმართულება გულისხმობს ეკონომიკასთან დაკავშირებული ინფორმაციის დროულ და სრულყოფილ მოპოვებას, მის ანალიზსა და სათანადო რეალიზაციას.

ეკონომიკურ სფეროში ინფორმაციის მოპოვება შესაძლებელია როგორც კერძო, ასევე საჯარო სექტორებიდან, საწარმოო დაწესებულებებიდან და ორგანიზაციებიდან. ეკონომიკურ საკითხებზე ინფორმაცია შეძლება იყოს როგორც ღია ასევე დახურული წყაროებიდან მოპოვებული. სწორედ ამიტომ სახელმწიფოს მნიშვნელოვან საზრუნავს საჯარო და კერძო სექტორის კონტრსადაზვერვო, ხოლო საერთაშორისო არენაზე პოტენციურად მოწინააღმდეგე სახელმწიფოებში იმავე სეგმენტის სადაზვერვო უზრუნველყოფა წარმოადგენს. შესაბამისად მნიშვნელოვანია ნაშრომის ფარგლებში განხილულ იქნას ეკონომიკური დაზვერვისა და კონტრდაზვერვის ის ძირითადი მიმართულებები, რომლებსაც სახელმწიფოთა სპეცსამსახურები ახორციელებენ საკუთარი პოლიტიკური, ეკონომიკური თუ გეოსტრატეგიული ინტერესების გასამყარებლად.

საკვანძო სიტყვები: *ეროვნული უსაფრთხოება, ეკონომიკური უსაფრთხოება, სპეცსამსახურები, სადაზვერვო საქმიანობა*

ABSTRACT:The economy is one of the key sectors ensuring state security and thus, the state services, by applying various methods, strive to decline the potentially rival economies or undertake the maximal control on already weak economies.

Economic intelligence, as one of the directions of the intelligence activity, implies the timely obtainment of the comprehensive economy-related information, its analysis, and due realization.

Obtainment of information in the economic sector can be achieved from private so from the public sectors, from the enterprises and organizations. Information on economic issues may be obtained from the open so from the closed sources. Hence, the counter-intelligence of the public and private sectors is the key task for the state, similar to the intelligence provision in the same segment in the potentially rival states at the international theatre.

Correspondingly, it is paramount to discuss the key directions of the economic intelligence and counter-intelligence within the scope of the Article, undertaken by the special services of the countries to reinforce their own political, economic and geo-strategic interests.

KEYWORDS: *National Security, Economic Security, Special Services, Intelligence Activity.*

ეროვნული უსაფრთხოების სისტემაში შემავალი ერთ-ერთი ძირითადი სეგმენტის, ეკონომიკური უსაფრთხოების განმტკიცება, ე.ი მისი სადაზვერვო და კონტრსადაზვერვო უზრუნველყოფა საჭიროებს არა მარტო ინფორმაციულ მხარდაჭერას, არამედ ამ ინფორმაციის ანალიზს და წარმატებულ რეალიზაციას. ინფორმაციული მხარდაჭერა უნდა ხასიათდებოდეს დროულობითა და სრულყოფილებით. პრაქტიკულად ანალოგიურად ხორციელდება კორპორაციული შპიონაჟიც სადაზვერვო საქმიანობასთან კომბინირებულად.

ეკონომიკური დაზვერვის მიმართულებით ოპერატიული საქმიანობის ეტაპები პირობითად ორ ნაწილად იყოფა:¹ ინფორმაციის მოპოვება, შეფასება და ანალიზი, ეს არის ინფორმაციის დამუშავების პროცესი, რომლის დროსაც ხდება ღონისძიების დაგეგმვა, ხოლო მეორე ნაწილი კი გულისხმობს უკვე დაგეგმილი ღონისძიების რეალიზაციას. მთელი პროცესის აუცილებელი პირობაა კი ის, რომ მოხდეს მისი მართვა და კოორდინაცია, რომელიც უწყვეტ პროცესად უნდა მიმდინარეობდეს. ზემოაღნიშნული ეტაპების დასრულების შემდგომ იწყება დამაზიანებელი სადაზვერვო-ოპერატიული ქმედებები.

ზოგადად, როგორც ოპერატიული საქმიანობისას, ისე ეკონომიკური დაზვერვის მიმართულებით სადაზვერვო ინფორმაციის მოპოვება ხორციელდება როგორც ღია ისე დახურული წყაროებიდან. ამ მიზნით, განსაკუთრებული შესწავლის ობიექტებს სახელმწიფო და კერძო სექტორში შემავალი ორგანიზაცია-დაწესებულებები წარმოადგენენ.² სწორედ ამიტომ სახელმწიფოს მნიშვნელოვან საზრუნავს საჯარო და კერძო სექტორის კონტრსადაზვერვო, ხოლო საერთაშორისო არენაზე პოტენციურად მოწინააღმდეგე სახელმწიფოებში იმავე სეგმენტის სადაზვერვო უზრუნველყოფა წარმოადგენს.

ეკონომიკური დაზვერვის მიზნებსა და ამოცანებსა განსაზღვრავს სახელმწიფოს პოლიტიკური, სოციალურ-ეკონომიკური, გეოსტრატეგიული და სხვა უამრავი ფაქტორი, რომელთა შორის აღსანიშნავია სახელმწიფოს ეკონომიკური ინტერესები პოტენციურად მოწინააღმდეგე ქვეყანაში.

უცხო სახელმწიფოს სპეცსამსახურების ეკონომიკური დაზვერვის ოპერატიული შესწავლის ერთ-ერთ ძირითად ამოცანას პოტენციურად მოწინააღმდეგე სახელმწიფოს/სახელმწიფოების ეკონომიკის დასუსტება და მასზე ზეგავლენის გაადვილება წარმოადგენს. ამ მიმართებით მნიშვნელოვანი ადგილი უკავია ყველა ხარისხის საიდუმლოების რეჟიმის მოშლას, რომლის დამაზიანებელი ზემოქმედებაც კონტრსადაზვერვო სამსახურების მიერ უნდა იქნეს აცილებული.

ეკონომიკური დაზვერვის ერთ-ერთ მნიშვნელოვან მიმართულებას საერთაშორისო ბაზრებზე საკუთარი ქვეყნის კომპანიების წარმატებით შეღწევა-დამკვიდრება წარმოადგენს.³ სწორედ ამიტომ სახელმწიფოთა შორის ინვესტიციების განხორციელებამდე და ეკონომიკური ხელშეკრულებების გაფორმებამდე ოპერატიულ-აგენტურული და სამეცნიერო შესწავლის პროცესების უზრუნველყოფა აუცილებელია, როგორც სადაზვერვო, ისე კონტრსადაზვერვო საქმიანობის ფარგლებში, რათა თავიდან იქნას აცილებული ეროვნული

¹ Strategic Dossier 162 B Economic intelligence in a global world, 2014. Spanish Institute for Strategic Studies, Ministry Of Defence, official web, 22, Accessed on 4 April 2020. https://publicaciones.defensa.gob.es/media/downloadable/files/links/c/e/ce_162_b.pdf

² საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 01.01.2016-31.12.2016, 8, წვდომის თარიღი: 4 აპრილი 2020. <https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/angarishi2016.pdf>

³ იქვე, გვ. 9.

უსაფრთხოებისათვის ისეთი დამაზიანებელი შედეგები, როგორცაა ეკონომიკური ექსპანსია.

წარმატებული ეკონომიკური საქმიანობის პირობების უზრუნველსაყოფად საკუთარი ქვეყნის კომპანიაში სადაზვერვო (მათ შორის კორპორაციული შპიონაჟით შენიღბული) შეღწევადობის თავიდან ასაცილებლად აუცილებელია კონტრსადაზვერვო უზრუნველყოფა. ამ კუთხით, უახლეს ისტორიაში არსებობს მაგალითები, როდესაც კერძო კომპანიებში⁴ ხორციელდება დაზვერვისა და კონტრდაზვერვის ყოფილი თანამშრომლების განთავსება, რაც მათი მხრიდან საკუთარი სახელმწიფოს სასარგებლო სადაზვერვო და კონტრსადაზვერვო საქმიანობის გაგრძელებას უნდა ნიშნავდეს.*

ადამიანური რესურსის სახით ინფორმაციის მოპოვების მნიშვნელოვან ობიექტებად გვევლინებიან სახელმწიფო და კერძო სექტორში მომუშავე პირები. გამოდის, რომ ისინი სადაზვერვო აგენტურული შეღწევადობის ერთ-ერთ მნიშვნელოვან ობიექტებს წარმოადგენენ.⁵

ეკონომიკური დაზვერვის განსახორციელებლად მოწყვლად სფეროებს წარმოადგენს სოფლის მეურნეობისა და ფინანსური სექტორი, საბაჟო და შემოსავლების სამსახურები და სხვ. საკუთარი პოზიციების გასამყარებლად უცხო ქვეყნის სპეცსამსახურები მუდმივად ცდილობენ გადაიბირონ ან/და ჩანერგონ კონკრეტული პირები რათა მოიპოვონ საიდუმლო ინფორმაცია ეკონომიკურ სფეროებში მიმდინარე პროცესების შესახებ.⁶

ეკონომიკური დაზვერვის მიმართულებით, წარმატებული და მასშტაბური აგენტურული შეღწევა, პოტენციურად მოწინააღმდეგე სახელმწიფოს ეკონომიკური შესაძლებლობებისა და რესურსების დროული და სწორი შეფასების ხელსაყრელი პირობაა. ამ მიმართულებით წარმატებული საქმიანობის შედეგად, სხვა მნიშვნელოვან საკითხებთან ერთად შესაძლებელია გაირკვეს თუ როგორ ანაწილებს პოტენციურად მოწინააღმდეგე სახელმწიფო საკუთარ რესურსებს, როგორ იმოქმედებს იგი სამხედრო შეიარაღებული კონფლიქტის შემთხვევაში და რა რესურსის გამოყენება შეეძლება მას საგანგებო ან/და საომარი მდგომარეობის დროს. აქედან გამომდინარე შეიძლება ითქვას, რომ პრაქტიკულად ეკონომიკურ დაზვერვას გააჩნია თავსებადობა სამხედრო, სტრატეგიულ და პოლიტიკურ დაზვერვასთან.

⁴About Strategic Forecasting Inc, Accessed on 7 April 2020. <https://www.stratfor.com/about>

* ამერიკის შეერთებულ შტატებში მოღვაწე, კერძო კომპანია (ანალიტიკური სამსახური) „Strategic Forecasting Inc.“ სტრატეგიული პროგნოზირების კორპორაციაა. იგი მასობრივი ინფორმაციის საშუალებებიდან და სხვა ღია წყაროებიდან, საკუთარ ე.წ. აგენტურული აპარატის მეშვეობით მოიპოვებს და აანალიზებს ინფორმაციას მსოფლიოში მიმდინარე მნიშვნელოვანი ეკონომიკური, პოლიტიკური და გეოპოლიტიკური მოვლენების შესახებ. კორპორაციის მიერ განხორციელებული ანალიტიკა, რომელიც ფართო საზოგადოებისათვის ხელმისაწვდომია, ის პრაქტიკულად ყოველთვის ამერიკის შეერთებული შტატების სტრატეგიული ინტერესების თანხვედრია. კომპანიის თანამშრომლები დაკოპლექტებულნი არიან სადაზვერვო და უსაფრთხოების სექტორის ყოფილი თანამშრომლებით. კომპანიის ანალიტიკოსებად მუშაობენ ყოფილი დიპლომატები (რომლებიც, როგორც სადაზვერვო ისტორია აჩვენებს სადაზვერვო საქმიანობის განმახორციელებელი სუბექტები არიან) და უსაფრთხოების სამსახურის ყოფილი თანამშრომლები.

⁵ საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 01.01.2017-31.12.2017, 9, წვდომის თარიღი: 4 აპრილი 2020. <https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/angarihi%202017.pdf>

⁶ იქვე, გვ. 10.

ზემოაღნიშნული მიმართულებით საინტერესოა მეორე მსოფლიო ომის დროს გერმანელ მზვერავ-დივერსანტთა ჯგუფის მიერ განხორციელებული ქმედებები ამერიკის შეერთებული შტატების სტრატეგიული ობიექტების წინააღმდეგ.

მეორე მსოფლიო ომის დროს, გერმანიის ხელისუფლების სამხედრო-სტრატეგიულ ინტერესებში შედიოდა ამერიკის შეერთებული შტატების ეკონომიკაზე დამაზიანებელი ზემოქმედების ორგანიზება, რათა ამერიკის შეერთებულ შტატებს მხარი არ დაეჭირა საბჭოთა კავშირისათვის. გერმანიის სამხედრო-სადაზვერვო სამსახურის „აზვერი“-ს⁷ მიერ დაიგეგმა ამერიკის შეერთებული შტატების ეკონომიკისათვის მნიშვნელოვანი სტრატეგიული ობიექტების (ნიუ-იორკის ხიდის “Hell Gate Bridge”, ნიაგარას ჩანჩქერზე აგებული ჰიდროელექტროსადგური, ფილადელფიის ალუმინის ქარხანა და სხვ.) დაზიანება.

ჯორჯ ჯონ დაჩისა და ედუარდ ჯონ კერლინგის ხელმძღვანელობით მისიის შესრულება, გერმანელ მზვერავ-დივერსანტთა (ერნესტ პიტერ ბარგერი, ჰენრი ჰერმ ჰეინცი, რიჩარდ ქურინი, ვერნერ ტიელი, ჰერბერტ ჰანს ჰაუბტი, ჰერმან ოტო ნეუბაუერი)⁸ იმ ჯგუფს დაევა, რომელსაც შესაბამისი მომზადება ბერლინის საბოტაჟის სკოლაში ჰქონდა გავლილი. აქედან გამომდინარე შეიძლება ითქვას, რომ უცხო სახელმწიფოთა სადაზვერვო შესწავლის ობიექტსა და სამიზნეს წარმოადგენს სახელმწიფოს სტრატეგიული დანიშნულების ობიექტები.⁹

ეკონომიკური დაზვერვის კუთხით უახლეს ისტორიაში საყურადღებოა სადაზვერვო საქმიანობის ისეთი მიმართულება, როგორცაა **ელექტრონული დაზვერვა**, რომლის ოპერაციული ქმედებების ერთ-ერთ მიმართულებად **კიბერშეტევები** გვევლინება. ამ კუთხით დაზიანების მნიშვნელოვან სამიზნეს ფინანსური და საბანკო სექტორი, ენერგეტიკული სისტემა და ჰიდროელექტროსადგურები წარმოადგენენ.¹⁰

2013 წელს, ირანელი ჰაკერების მიერ, ამერიკის შეერთებულ შტატებში, ნიუ-იორკის ჰიდროელექტროსადგურზე განხორციელდა კიბერ შეტევა,¹¹ რა დროსაც ჰაკერებმა ჰიდროელექტროსადგურის დაცულ კომპიუტერულ სისტემაში შეაღწიეს, რითაც კიბერტერორისტებს საშუალება მიეცათ ეკონტროლებინათ ჰიდროელექტროსადგურის მუშაობა, ე.ი. შეექმნათ ხელსაყრელი პირობა დივერსიის განხორციელებისთვის. აღნიშნული ოპერაცია ემსახურებოდა ობიექტის დაცულობის სისტემის შემოწმებას, თუმცა მას ჰქონდა დამთრგუნველი ზემოქმედება იმ თვალსაზრისით, რომ ირანის სახელმწიფოს შეეძლო ამერიკის შეერთებული შტატების ენერგეტიკულ სექტორზე დამაზიანებელი ზემოქმედება.

⁷ The Central Intelligence Agency, 2001. Nazi War Crimes Disclosure Act, Accessed on 4 April 2020. https://www.cia.gov/library/readingroom/docs/GERMAN%20INTELLIGENCE%20SERVICE%20%28WWII%29%2C%20%20VOL.%201_0003.pdf

⁸ Federal Bureau of Investigation, “George John Dasch and the Nazi Saboteurs”, Accessed on 4 April 2020. <https://www.fbi.gov/history/famous-cases/nazi-saboteurs-and-george-dasch>

⁹ საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 01.01.2018-31.12.2018, 14-15, წვდომის თარიღი: 4 აპრილი 2020. <https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%98%202018.pdf>

¹⁰ იქვე, გვ.13.

¹¹ BBC News, 2015. „Iranian hackers 'targeted' New York dam”, Accessed on 4 April 2020. <http://www.bbc.com/news/technology-35151492>

უახლეს ისტორიაში ეკონომიკური დაზვერვის ერთ-ერთ მნიშვნელოვან მიმართულებას კორპორაციული შპიონაჟი წარმოადგენს. კორპორაციული შპიონაჟი¹² ეს არის კომერციული საიდუმლოების მოპარვა, იმ მიზნით, რომ დაზარალდეს კომპანიის ან სახელმწიფოს სავაჭრო ინტერესები როგორც ქვეყნის შიგნით, ისე საერთშორისო ბაზარზე. აღნიშნული ქმედება გამოიხატება ისეთი საიდუმლო დოკუმენტის, ნახაზის, სქემის, ტექნოლოგიის მოპარვაში, გადაწერაში, ატვირთვა-ჩამოტვირთვაში ან განადგურებაში, რომლის გამჟღავნება ზიანის მომტანია როგორც კომპანიისათვის ისე სახელმწიფოს ეკონომიკური უსაფრთხოებისათვის.

აღსანიშნავია ის გარემოება, რომ კორპორაციული შპიონაჟის გამოყენება შესაძლებელია სადაზვერვო საქმიანობასთან კომბინირებულად, რაც ობიექტი სახელმწიფოსათვის დამაზიანებელ შედეგს კიდევ უფრო ზრდის.

კორპორაციული შპიონაჟის კუთხით საინტერესოა ამერიკის შეერთებულ შტატებში ჩინელი პროფესორი ჰაო ზენგისა და მისი ხუთი ჩინელი სტუდენტის (ჩინეთის მოქალაქეები)¹³ მიერ განხორციელებული კორპორაციული შპიონაჟის ფაქტი ჩინეთის სახალხო რესპუბლიკის სასარგებლოდ, რომელიც ათი წელი გრძელდებოდა და გამოძიების ფედერალური ბიუროს მიერ 2015 წელს იქნა აღკვეთილი. აღნიშნული პირები მუშაობდნენ ამერიკულ კომპანიებში: „Avago Technologies“ და „Skyworks Solutions“, სადაც აწარმოებდნენ მობილური ტელეფონებისთვის რადიოსიხშირულ ფილტრებს. ამ პირებმა ტექნოლოგიები გაიტანეს ჩინეთში, დააარსეს საკუთარი კომპანია და ჩინეთის სამხედრო ორგანიზაციებისათვის დაიწყეს ანალოგიური ფილტრების წარმოება. ყოველივე კორპორაციული შპიონაჟის ფარგლებში ახალი ტექნოლოგიების მოპარვის ფაქტზე მიანიშნებს.

სადაზვერვო და კონტრსადაზვერვო უზრუნველყოფის ერთ-ერთ მნიშვნელოვან მიმართულებას აგრარული სექტორის აგროტერორიზმისგან დაცვა წარმოადგენს, რომელსაც განმარტავენ როგორც დამაზიანებელ ზემოქმედებათა ერთობლიობას, რომელიც მიმართულია სოფლის მეურნეობის დარგის, მცენარეების, ცხოველების, სასურსათო უსაფრთხოების სისტემის რღვევისკენ და საშიში დაავადებების გავრცელებისკენ, რომელიც იწვევს ეკონომიკურ ზარალს, საფრთხის ქვეშ დგება მოსახლეობის სიცოცხლე და ჯანმრთელობა და სახელმწიფოს ნორმალური ფუნქციონირება.¹⁴ აგროტერორიზმის მიზანია არა უბრალოდ სასოფლო-სამეურნეო კულტურების განადგურება, არამედ მოსახლეობაში პანიკის დათესვა, მათში დაუცველობის განცდის გაჩენა. ყოველივე სადაზვერვო-ოპერაციული ქმედებების შემადგენელ საფეხურებს წარმოადგენს, რაც კიდევ უფრო ამყარებს მოსაზრებას აგროტერორიზმის სადაზვერვო მიზნებით გამოყენების შესახებ.

¹² Office of The National Counterintelligence Executive, 2009-2011. „Foreign Spies Stealing US Economic Secrets in Cyberspace”, Report to Congress on Foreign Economic Collection and Industrial Espionage, Accessed on 10 April 2020. https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

¹³ Department of Justice Office of Public Affairs, 2015. „Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People’s Republic of China”, Accessed on 4 April 2020. <https://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets>

¹⁴ Monke J., 2007. “Agroterrorism: Threats and Preparedness”, CRS Report for Congress, Accessed on 11 April 2020. <https://www.fas.org/sgp/crs/terror/RL32521.pdf>

გამოთქმული მოსაზრებას ადასტურებს ქვემოთმოყვანილი ისტორიული ფაქტები:¹⁵

- პირველი მსოფლიო ომის პერიოდში (1914-1918 წწ.) გერმანიის მიერ გამოყენებულ იქნა სპეციალური ვირუსი, მოკავშირეთა ცხენების დასახოცად, რათა მოწინააღმდეგის სწრაფი გადაადგილების პარალიზება მომხდარიყო;
- მეორე მსოფლიო ომის დროს (1939-1945წწ.), იაპონიის მიერ მოწინააღმდეგის შესაჩერებლად და მასზე უპირატესობის მოსაპოვებლად აქტიურად გამოიყენებოდა ვირუსები, რითაც ხოცავდნენ და ანადგურებდნენ სასოფლო-სამეურნეო პროდუქტებსა და ცხოველებს, რაც ასევე იწვევდა ჯარისკაცების დაავადებას;
- 1952 წელს კენიაში ტერორისტული ორგანიზაცია „მაუ-მაუს“ მიერ გამოყენებულ იქნა აფრიკული შხამიანი რძე (მცენარის), რითაც მოწამლეს და გაანადგურეს საქონლის ფერმა;
- ვიეტნამის ომის (1954-1975წწ.) დროს ამერიკის შეერთებული შტატების მიერ გამოყენებულ იქნა შხამ-ქიმიკატები ვიეტნამში მოსავლიანი მიწებისა და მარცვლეული კულტურის გასანადგურებლად;
- 1970 წელს „კუ კლუს“ კლანის წევრების მიერ, ალაბამაში, მოწამლულ იქნა წყლის მარაგი, რომლითაც მარაგდებოდა შავკანიანი მუსლიმი მოსახლეობის სოფელი და ფერმა. ამის შედეგად დაიხოცა პირუტყვი და დაავადდა მოსახლეობა;
- 1980 წელს საბჭოთა ჯარების მიერ გამოყენებულ იქნა ვირუსი ავღანეთში ჯიჰადისტების ცხენების გასანადგურებლად, რომ მოწინააღმდეგის სწრაფი გადაადგილების საშუალება მოესპოთ;
- 1999 წელს ბელგიის, საფრანგეთისა და ნიდერლანდების ფერმაში, ფრინველების (ქათამი) საკვებში აღმოჩენილ იქნა კარცეროგენი-დიოქსინი, რასაც ბელგიიდან ქათმის, საქონლისა და ღორის ხორცის იმპორტის აკრძალვა მოჰყვა. რის შედეგადაც ბელგიის სახელმწიფოს მიაღდა 1 მილიარდი დოლარი ზარალი.¹⁶

უნდა აღინიშნოს, რომ აგროტერორიზმი ამერიკის შეერთებული შტატების მიერ, 2001 წლის 11 სექტემბრის ტერაქტის შემდეგ აღიარებულ იქნა ეროვნული უსაფრთხოების წინააღმდეგ მიმართულ ერთ-ერთ მძიმე დანაშაულად.

ამრიგად შეიძლება ითქვას, რომ აგროტერორიზმი, როგორც ტერორიზმის ერთ-ერთი მიმართულება, ეკონომიკური და კორპორაციული (ან კომბინირებულად ორივე ერთად) დაზვერვის განხორციელების ერთ-ერთ ძირითად მიმართულებას განეკუთვნება, რომელიც დამაზიანებელ ზეგავლენას ახდენს სასურსათო უსაფრთხოებაზე, უარყოფითად ზემოქმედებს ქვეყნის ეკონომიკაზე და ქმნის ეკონომიკური უსაფრთხოების რღვევის საშიშროებას.

ეკონომიკური დაზვერვის ერთ-ერთ მნიშვნელოვან მიმართულებას, ქვეყნის ბუნებრივ რესურსებზე კონტროლის დამყარება წარმოადგენს. ამ კუთხით საყურადღებოა ამერიკის შეერთებული შტატების ცენტრალური სადაზვერვო სააგენტოს (CIA) ფარული სადაზვერვო ოპერაცია ირანში კოდური სახელწოდებით - „TP-Ajax“.¹⁷ ოპერაცია მიზნად

¹⁵ Pate J., and Cameron G., 2002. *Covert Biological Weapons Attacks against Agricultural Targets: Assessing the Impact against U.S. Agriculture*, 7-9.

¹⁶ კუხალაშვილი დ., გურული-კუხალაშვილი მ., ბრეგაძე თ., 2014. *ტერორიზმის როლი სასურსათო და ტურიზმის უსაფრთხოების უზრუნველყოფაში*, თბილისი, 35-46.

¹⁷ Saeed K. Dehghan and Richard N. Taylor, *The Gurdian*, 2013. “CIA admits role in 1953 Iranian coup“, Accessed on 8 April 2020. <http://www.theguardian.com/world/2013/aug/19/cia-admits-role-1953-iranian-coup>

ისახავდა ირანის პრემიერ-მინისტრის მუჰამედ მოსადეგის ხელისუფლებიდან ჩამოცილებას.¹⁸

საიდუმლო ოპერაციის დაგეგმვა-განხორციელების ძირითადი მიზეზი 1951 წელს მოსადეგის ინცირებით ირანის პარლამენტის (მეჯლისის) მიერ დიდი ბრიტანეთის კონტროლს დაქვემდებარებული ირანული ნავთობკომპანიის ნაციონალიზაცია გახდა. ეკონომიკური ზიანის თავიდან ასაცილებლად დიდმა ბრიტანეთმა ირანის ნავთობის მიმართ სადაზვერვო ბერკეტები აამოქმედა და ირანულ ნავთობზე ემზარგო დააწესა.¹⁹

ამასთანვე დიდი ბრიტანეთისა და ამერიკის მთავრობებმა, იმის შიშით, რომ ირანი საბჭოთა კავშირის გავლენის სფეროში არ გადასულიყო გადაწყვიტეს ხელოვნურად შეეცვალათ მუჰამედ მოსადეგის ხელისუფლება. ამ მიზნითა დაიწყო ფარული სადაზვერვო ოპერაცია ირანის ხელისუფლების წინააღმდეგ.

ოპერაციის ხელმძღვანელი იყო კერმიტ რუზველტი (ცენტრალური სადაზვერვო სააგენტოს ოფიცერი, ფარული ოპერაციების ხელმძღვანელის თანაშემწე), რომელმაც მოკლე დროში შეძლო და მოისყიდა ირანის მეჯლისის (პარლამენტის) წევრები, გამომცემლები, რედაქტორები და ჟურნალისტები. დაიწყო ირანში გამომავალი ჟურნალ-გაზეთების 80%-ის ფინანსური უზრუნველყოფა.

შესრულდა ფარული სადაზვერვო ოპერაციის ისეთი ეტაპები, როგორცაა:

- შეიქმნა (მათ შორის სასულიერო პირების მხრიდან) საზოგადოებრივი აზრი მუჰამედ მოსადეგზე, როგორც კომუნისტზე;
- ირანის წინააღმდეგ ეკონომიკური დივერსიის (მათ შორის ფულის ინფლაციის ინსპირირებისათვის) მოსაწყობად ლონდონსა და ნიუ-იორკში დაიწყო ყალბი ირანული ბანკნოტების ბეჭდვა-გასაღება;
- სადაზვერვო შეღწევადობით დაქირავებულმა პირებმა, თითქოსდა მოსადეგის მომხრეებმა დაიწყეს მეჩეთებსა აფეთქება, მეჩეთებში მუსლიმი მოსახლეობის დახვრეტა, მალაზიების დარბევა, კომუნისტური პარტიის ლოზუნგებით გამოსვლა, მასობრივი არეულობა;

ხელისუფლების მხრიდან სამხედრო შენაერთების გამოყენებას 800 ადამიანის დაღუპვა მოჰყვა. ყოველივე ეს მოსადეგის დააპატიმრებით, შესაბამისად მისი ხელისუფლებიდან ჩამოცილებით, სასურველი მმართველის ხელისუფლებაში მოყვანით, ირანის ნავთობზე დიდი ბრიტანეთის კონტროლის (ბრიტანეთის ნავთობის კომპანია-British Petroleum Company) აღდგენით დასრულდა.²⁰

ამავე კუთხით საყურადღებოა 1954 წელს ამერიკის შეერთებული შტატების ცენტრალური სადაზვერვო სააგენტოს მიერ ჩატარებული ფარული სადაზვერვო ოპერაცია

¹⁸ Campaigning to Install Pro-western Government in Iran, CIA Archive Documents, Accessed on 4 April 2020. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB435/docs/Doc%202%20-%201954-00-00%20Summary%20of%20Wilber%20history.pdf>

¹⁹ Torey L. McMurdo, 2012. „The Economics of Overthrow, The United States, Britain, and the Hidden Justification of Operation TPAJAX“, 15-16, Accessed on 4 April 2020. <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-2/pdfs/McMurdo-The%20Economics%20of%20Overthrow.pdf>

²⁰ Risen J., 2000. New York Times, Special Report: „The C.I.A In Iran“, Accessed on 4 April 2020. https://archive.nytimes.com/www.nytimes.com/library/world/mideast/041600iran-cia-index.html?_r=1

სახელწოდებით „PBSUCCESS“²¹ გვატემალაში, რომელსაც კანონიერი პრეზიდენტის ხაკობო არბენზის გადაყენება და ოპერაციის ორგანიზატორი სახელმწიფოს ინტერესების გამტარებელი მმართველის კარლოს კასტილიო არმასის სამხედრო რეჟიმის დამყარება მოჰყვა. ოპერაციის ხელმძღვანელი იყო პოლკოვნიკი ალბერტ რიჩარდ ჰანი, ²² რომლის ოპერატიული შტაბი „ლინკოლნი“ განთავსებული იყო ფლორიდის შტატში, მაიამიში.

1931-1944 წლებში გვატემალაში გენერალი ხორხე უბიკო ამერიკის შეერთებული შტატების ინტერესების გამტარებელ პოლიტიკურ ფიგურას წარმოადგენდა. მისი მხარდაჭერისთვის ამერიკის შეერთებულმა შტატებმა მიიღო ჰექტრობით მიწები ამერიკული ხილის კომპანიისთვის (the American United Fruit Company (UFCO)).²³ ამასთან ერთად უბიკომ ამერიკის შეერთებული შტატების სამხედრო შეიარაღებულ ძალებს საშუალება მისცა მათ ქვეყანაში განეთავსებინათ სამხედრო ბაზები. მისი გადაყენება 1944 წელს მასობრივი გამოსვლებისა და არეულობის შედეგად მოხდა. 1951 წელს ახალი არჩევნების შედეგების მიხედვით გვატემალის პრეზიდენტი ხაკობო არბენზი გახდა, რომელმაც აგრარული რეფორმის შედეგად 1952 წელს 600 ათასი ჰექტარი მიწა დაურიგა გლეხებს, რამაც გამოიწვია ამერიკული ხილის კომპანიის (UFCO) კონტროლიდან მიწების ნახევარზე მეტის დაკარგვა. აღნიშნული ქმედება ამერიკის შეერთებული შტატების სტრატეგიული და ეკონომიკური ინტერესების საზიანოდ ჩაითვალა, რასაც მოჰყვა კიდევ ზემოაღნიშნული საიდუმლო ოპერაციის დაგეგმვა-განხორციელება.

ეკონომიკური დაზვერვის ამოცანების შესასრულებლად ცენტრალური სადაზვერვო სააგენტოს ორგანიზებით განხორციელდა სადაზვერვო-აგენტურული შეღწევადობის უზრუნველსაყოფად ისეთი ქმედებები, როგორიცაა:

- გვატემალას მთავრობის მოწინააღმდეგე პირებთან კონტაქტის დამყარება, მათ შორის კასტილიო არმასთან;
- შეიქმნა ანტისამთავრობო შეიარაღებული დანაყოფები და დაჯგუფებები, უზრუნველყოფილ იქნა მათი მხარდაჭერა როგორც ფინანსურად ისე შეიარაღებით;
- საიდუმლო ოპერაციის დროს, საომარი ქმედების პირობებში, ნაციონალური რადიოსადგურის მეშვეობით, გამოყენებულ იქნა დეზინფორმაციის მეთოდი;

წარმატებული ოპერაციის შემდეგ, თანამდებობიდან გადადგა, ამერიკის შეერთებული შტატების სახელმწიფო მდივნის მოადგილე და ცენტრალური სადაზვერვო სააგენტოს ყოფილი დირექტორი უოლტერ სმიტი²⁴ და ამერიკული ხილის კომპანიის (The American United Fruit Company (UFCO)) დირექტორთა საბჭოს წევრი გახდა, რაც სადაზვერვო საქმიანობის უწყვეტობაზე უნდა მიანიშნებდეს.

გვატემალაში განხორციელებული ფარული სადაზვერვო ოპერაციის შედეგად:

- ამერიკულმა ხილის კომპანიამ (UFCO) გვატემალას მთავრობისგან დაიბრუნა წართმეული მიწები;

²¹ The National Security Archive, George Washington university, Accessed on 4 April 2020. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB4/docs/doc01.pdf>

²² Prados J., 2006. *Safe for Democracy: The Secret Wars of the CIA*, 97-123.

²³ Chullater N., CIA Historical Review Program, „The United States and Guatemala 1952-1954, Operation „PBSUCCESS“, Accessed on 4 April 2020. https://www.cia.gov/library/readingroom/docs/DOC_0000134974.pdf

²⁴ კუხალაშვილი დ., 2010. *ცენტრალური სადაზვერვო სამმართველო ამერიკის შეერთებული შტატების სამსახურში*, თბილისი, 74-78.

- გაფორმდა ახალი ხელშეკრულება ამერიკის შეერთებულ შტატებსა და გვატემალას მთავრობებს შორის ინვესტიციების განხორციელების შესახებ;
- გაუქმდა უცხოური კაპიტალიდან მიღებულ შემოსავალზე გადასახადის შესახებ კანონი, რითაც მთელ მოგებას მხოლოდ ამერიკული კომპანია იღებდა და სახელმწიფო ბიუჯეტის სასარგებლოდ აღარ იხდიდა გადასახადს;

გასული საუკუნის 60-იან წლებში ეკონომიკური დაზვერვის ორგანიზების კუთხით საკუთარი ინტერესების დასაცავად და მსოფლიოში დომინანტური მდგომარეობის შესანარჩუნებლად სპეციალურ ფარულ ოპერაციებს საბჭოთა კავშირიც აქტიურად მიმართავდა. ამ კუთხით აღსანიშნავია სპეცოპერაცია კოდური სახელწოდებით „კედრ“-ი („KEDR“),²⁵ რომელიც 12 წელი მზადდებოდა და კანადასა და ჩრდილოეთ ამერიკას შორის არსებულ ნავთობის გადამამუშავებელი ქარხნისა, გაზისა და ნავთობის მიღებზე დივერსიული აქტების, საბოტაჟის განხორციელებას ისახავდა მიზნად.

ოპერაციის აქტიური ფაზის დაწყებამდე საბჭოთა დაზვერვის მიერ მოწყვლადობის განსაზღვრის მიზნით ხდებოდა ობიექტების ფოტოგადაღება, იერიშის მისატანად მოხერხებული გზების, ტერაქტის შემდგომ გაქცევის მარშრუტის შესწავლა და სათანადო საიდუმლო რუკების შედგენა. ოპერაციის მიზანს დაზვერვას დაქვემდებარებულ ქვეყნებში შიშის, პანიკის და მისგან მომდინარე მძიმე შედეგების ინსპირირება წარმოადგენდა.

ნაშრომში მოყვანილი ისტორიული ფაქტებისა და მაგალითების განხილვისა და გაანალიზების საფუძველზე შეიძლება ითქვას, რომ:

- სახელმწიფოთა სპეცსამსახურების საქმიანობის ერთ-ერთი მიმართულებას ეკონომიკური დაზვერვა წარმოადგენს;
- ეკონომიკური დივერსიების განხორციელებით სახელმწიფოები ცდილობენ დააზიანონ ქვეყნის ეროვნული უსაფრთხოების უზრუნველმყოფი ერთ-ერთი ძირითადი სეგმენტი - ეკონომიკური უსაფრთხოება;
- ქვეყნის ეკონომიკური უსაფრთხოების დაზიანება აადვილებს მასზე გავლენის მოპოვებას (პოლიტიკურს, ეკონომიკურს) და ზრდის მის დამოკიდებულებას უცხო სახელმწიფოზე;
- ეკონომიკური დაზვერვისა და კონტრდაზვერვის განხორციელების მნიშვნელოვან პირობას დროულობით და სრულყოფილებით გამორჩეული ინფორმაციულ მხარდაჭერა, ინფორმაციული ანალიზი და წარმატებულ რეალიზაცია წარმოადგენს;
- ეკონომიკური დაზვერვის მიზნები და ამოცანები განისაზღვრება სახელმწიფოს პილიტიკური, სოციალურ-ეკონომიკური, გეოსტრატეგიული და სხვა უამრავი ფაქტორით, რომელთა შორის მნიშვნელოვანია სახელმწიფოს ეკონომიკური ინტერესები;
- ეკონომიკური დაზვერვის განსახორციელებლად მოწყვლად სფეროებს სოფლის მეურნეობის, ფინანსურ-ეკონომიკური, საბაჟო და სახელმწიფოსათვის სხვა მნიშვნელოვანი სექტორები წარმოადგენს;

²⁵ Andrew C., 1999. *The Sword and The Shield, The Mitrokhin Archive And The Secret History of KGB*, 363-364.

- ეკონომიკურ დაზვერვას გააჩნია თავსებადობა სამხედრო, სტრატეგიულ და პოლიტიკურ დაზვერვასთან, რომელთა საერთო ინტერესს ობიექტი ქვეყნის რესურსები წარმოადგენს;
- ეკონომიკური დაზვერვის ერთ-ერთ მნიშვნელოვან მიმართულებას საერთაშორისო ბაზრებზე საკუთარი სახელმწიფოს კომპანიების (შესაბამისად პროდუქციის) წარმატებით შეღწევა-დამკვიდრება წარმოადგენს, შესაბამისად ამ ფარგლებში კომბინირებულად შესაძლებელია კორპორაციული შპიონაჟის განხორციელება, რაც ე.წ ეკონომიკური ექსპანსიის განხორციელების ერთ-ერთი ხერხია;
- ეკონომიკური დაზვერვის განსახორციელებლად სახელმწიფოები კერძო კომპანიებში დაზვერვისა და კონტრდაზვერვის ყოფილი თანამშრომლების განთავსებას, საკუთარი სახელმწიფოს სასარგებლო სადაზვერვო და კონტრსადაზვერვო საქმიანობის გაგრძელების უზრუნველსაყოფად ახორციელებენ;
- ეკონომიკური დაზვერვის მიმართულებით დროულობით, სრულყოფილებით და სანდოობით გამორჩეული ინფორმაციის მოპოვება სახელმწიფო და კერძო სტრუქტურებიდან ოპერატიულ-აგენტურული ქსელების ორგანიზებით ხორციელდება.
- ეკონომიკური დაზვერვის ინფორმაციის მოპოვების მნიშვნელოვან ობიექტებად სახელმწიფო და კერძო სექტორში მომუშავე ან დათხოვნილი პირები გვევლინებიან, ე.ი. ისინი სადაზვერვო აგენტურული შეღწევადობის ობიექტებს წარმოადგენენ;
- ეკონომიკური დაზვერვისა და კორპორაციული შპიონაჟის პირობებში შესაბამისი ღონისძიების დაგეგმვა-გატარება მოიცავს შემდეგ საფეხურებს: ინფორმაციის მოპოვება, შეფასება, ანალიზი, რეალიზაცია, რომლის დროსაც მართვა და კოორდინაცია უწყვეტ პროცესად მიმდინარეობს;
- მსოფლიოში მიმდინარე მნიშვნელოვანი ეკონომიკური, პოლიტიკური და გეოპოლიტიკური მოვლენების შესახებ ინფორმაციული უზრუნველყოფისა და სასურველი საზოგადოებრივი აზრის მობილიზებისათვის ეკონომიკური დაზვერვის ფარგლებში გამოყენებადია კერძო სექტორი, რომლის ნიშანსაც ამავე სექტორის სპეცსამსახურების ყოფილი თანამშრომლებით კომპლექტაცია წარმოადგენს;
- ეკონომიკური დაზვერვის განხორციელების მნიშვნელოვან ხერხებს ტერორიზმის ისეთი სახეობის გამოყენება წარმოადგენს, როგორცაა: კიბერტერორიზმი, აგროტერორიზმი, რომელთა განხორციელება შესაძლებელია, როგორც სამოქალაქო ისე სამხედრო (ან კომბინირებულად ორივე ერთად) სექტორის დასაზიანებლად. ეკონომიკური დაზვერვის მნიშვნელოვანი მიზანი ობიექტ სახელმწიფოში დამთრგუნველი საზოგადოებრივი აზრის ფორმირებაა, რაც ქმნის სადაზვერვო შეღწევადობისათვის ხელსაყრელ პირობებს;
- კორპორაციული (კერძო კომპანიებს შორის) შპიონაჟის გამოყენება შესაძლებელია სადაზვერვო საქმიანობასთან კომბინირებულად.

ბიბლიოგრაფია

1. კუხალაშვილი დ., 2010. ცენტრალური სადაზვერვო სამმართველო ამერიკის შეერთებული შტატების სამსახურში, თბილისი, 74-78.
2. კუხალაშვილი დ., გურული-კუხალაშვილი მ., ბრეგაძე თ., 2014. ტერორიზმის როლი სასურსათო და ტურიზმის უსაფრთხოების უზრუნველყოფაში, თბილისი, 35-46.
3. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 01.01.2016-31.12.2016, 8, წვდომის თარიღი: 4 აპრილი 2020. <https://sbg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/angarishi2016.pdf>
4. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 01.01.2017-31.12.2017, 9, წვდომის თარიღი: 4 აპრილი 2020. <https://sbg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/angarishi%202017.pdf>
5. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 01.01.2018-31.12.2018, 14-15, წვდომის თარიღი: 4 აპრილი 2020. <https://sbg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%98%202018.pdf>
6. Andrew C., 1999. *The Sword and The Shield, The Mitrokhin Archive And The Secret History of KGB*, 363-364.
7. About Strategic Forecasting Inc, Accessed on 7 April 2020. <https://www.stratfor.com/about>
8. BBC News, 2015. „Iranian hackers 'targeted' New York dam”, Accessed on 4 April 2020. <http://www.bbc.com/news/technology-35151492>
9. Chullater N., CIA Historical Review Program, „The United States and Guatemala 1952-1954, Operation „PBSUCCESS“, Accessed on 4 April 2020. https://www.cia.gov/library/readingroom/docs/DOC_0000134974.pdf
10. Campaign to Install Pro-western Government in Iran, CIA Archive Documents, Accessed on 4 April 2020. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB435/docs/Doc%202%20-%201954-00-00%20Summary%20of%20Wilber%20history.pdf>
11. Department of Justice Office of Public Affairs, 2015. „Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People’s Republic of China”, Accessed on 4 April 2020. <https://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets>
12. Federal Bureau of Investigation, “George John Dasch and the Nazi Saboteurs”, Accessed on 4 April 2020. <https://www.fbi.gov/history/famous-cases/nazi-saboteurs-and-george-dasch>
13. Monke J., 2007. “Agroterrorism: Threats and Preparedness”, CRS Report for Congress, Accessed on 11 April 2020. <https://www.fas.org/sgp/crs/terror/RL32521.pdf>
14. Office of The National Counterintelligence Executive, 2009-2011. „Foreign Spies Stealing US Economic Secrets in Cyberspace”, Report to Congress on Foreign Economic Collection and Industrial Espionage, Accessed on 10 April 2020. https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
15. Pate J., and Cameron G., 2002. *Covert Biological Weapons Attacks against Agricultural Targets: Assessing the Impact against U.S. Agriculture*, 7-9.
16. Prados J., 2006. *Safe for Democracy: The Secret Wars of the CIA*, 97-123.
17. Risen J., 2000. New York Times, Special Report: „The C.I.A In Iran“, Accessed on 4 April 2020.

18. Saeed K. Dehghan and Richard N. Taylor, The Gurdian, 2013. "CIA admits role in 1953 Iranian coup", Accessed on 8 April 2020. <http://www.theguardian.com/world/2013/aug/19/cia-admits-role-1953-iranian-coup>
19. Strategic Dossier 162 B Economic intelligence in a global world, 2014. Spanish Institute for Strategic Studies, Ministry Of Defence, official web, 22, Accessed on 4 April 2020. https://publicaciones.defensa.gob.es/media/downloadable/files/links/c/e/ce_162_b.pdf
20. Torey L. McMurdo, 2012. „The Economics of Overthrow, The United States, Britain, and the Hidden Justification of Operation TPAJAX“, 15-16, Accessed on 4 April 2020. <https://www.cia.gov/library/center-for-the-study-ofintelligence/csi-publications/csi-studies/studies/vol.-56-no.-2/pdfs/McMurdo-The%20Economics%20of%20Overthrow.pdf>
21. https://archive.nytimes.com/www.nytimes.com/library/world/mideast/041600iran-cia-index.html?_r=1
22. The Central Intelligence Agency, 2001. Nazi War Crimes Disclosure Act, Accessed on 4 April 2020. https://www.cia.gov/library/readingroom/docs/GERMAN%20INTELLIGENCE%20SERVICE%20%28WWII%29%2C%20%20VOL.%201_0003.pdf
23. The National Security Archive, George Washington university, Accessed on 4 April 2020. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB4/docs/doc01.pdf>

ომის ჟურნალისტიკა და მისი სპეციფიკა ჟურნალ „არსენალის“
ფოკუსში

**PECULIARITY OF WAR REPORTING ACCORDING TO
MAGAZINE “ARSENALI”**

ნატალია პატარკაცაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის
სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის ჟურნალისტიკის
მიმართულების სტუდენტი.

Natalia Patarkatsasvhili _ Ivane Javakhishvili Tbilisi State University, Journalism_Junior;

2. ანი დეკანოსიძე _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო
უნივერსიტეტის ბაკალავრიატის, III კურსის ჟურნალისტიკის მიმართულების სტუდენტი.

Ani Dekanosidze- Ivane Javakhishvili Tbilisi State University, Journalism_Junior

აბსტრაქტი: ჩვენ მიერ წარმოდგენილი ნაშრომი მეტად აქტუალურ თემატიკას ეხება. მასში წარმოჩენილია თანამედროვე ქართული მედიის მუშაობის სპეციფიკა საომარი მოქმედებებისა და კონფლიქტური სიტუაციების გაშუქებისას. სამხედრო ჟურნალისტიკის განვითარების ტენდენციებზე თვალის მიდევნებით, შევეცადეთ ნათლად გვეჩვენებინა ქართველი ჟურნალისტების პროფესიონალიზმის პრობლემები, რამაც არაერთგზის იჩინა თავი კონფლიქტური ზონებიდან ინფორმაციის მოპოვება – გაშუქების პროცესში.

უნდა შევნიშნოთ, რომ საქართველოს გეოპოლიტიკური მდებარეობიდან, წარსულიდან და დღევანდელიდან გამომდინარე, მნიშვნელოვანია სამხედრო თემების გაშუქება და საზოგადოებამდე საჭირო და აუცილებელი სამხედრო ინფორმაციის მიტანა. უახლოესმა წარსულმა, კერძოდ 2008 წლის აგვისტოს ომმა, ნათლად აჩვენა ის ხარვეზები, რომლებიც დღეს კონფლიქტებზე მომუშავე ჟურნალისტთა საქმიანობას ახლავს. სამწუხაროდ, ქართული მედია სამხედრო შინაარსის გადაცემებისა თუ ჟურნალ-გაზეთების ნაკლებობას განიცდის, მაშინ როდესაც სამხედრო აღმშენებლობა ქვეყნის ერთ-ერთი უპირველესი ამოცანა უნდა იყოს. შესაბამისად, მოსახლეობის ცნობიერების დონის ამაღლება და საქართველოსა თუ მსოფლიოში მიმდინარე სამხედრო მდგომარეობის შესახებ ინფორმაციის სისტემატურად გავრცელება უმნიშვნელოვანესია.

ANNOTATION: THE ARTICLE PRESENTED BY US DEALS WITH VERY IMPORTANT ISSUES. IT PRESENTS THE SPECIFICS OF MODERN GEORGIAN MEDIA IN COVERAGE OF HOSTILITIES AND CONFLICT SITUATIONS. FOLLOWING TO THIS THEME WE HAVE TRIED TO SHOW THE PROBLEMS OF PROFESSIONALISM.

DUE TO GEORGIA'S GEOPOLITICAL LOCATION IT IS IMPORTANT TO COVER MILITARY ISSUES AND PROVIDE THE NECESSARY MILITARY INFORMATION TO THE PUBLIC. THE RECENT PAST, PARTICULARLY THE RUSSO-GEORGIAN WAR 2008, HAS CLEARLY SHOWN THE WEAKNESSES OF WAR CORRESPONDENTS' WORKS.

UNFORTUNATELY, THE GEORGIAN MEDIA SUFFERS FROM A LACK OF MILITARY CONTENT OR MAGAZINES AND NEWSPAPERS, WHILE MILITARY RECONSTRUCTION SHOULD BE ONE OF THE COUNTRY'S TOP PRIORITIES. THEREFORE, RAISING THE LEVEL OF AWARENESS OF THE POPULATION AND SYSTEMATICALLY REPORTING INFORMATION ABOUT THE CURRENT MILITARY SITUATION IN GEORGIA AND THE WORLD IS THE MOST IMPORTANT.

საკვანძო სიტყვები: ცნობიერების ამაღლება, ინფორმაცია, საინფორმაციო ომი, ომის ჟურნალისტიკა, სამხედრო შეიარაღება, ჟურნალი „არსენალი“.

ომის ჟურნალისტიკა და მისი სპეციფიკა ჟურნალ „არსენალის“ ფოკუსში

რამდენადაც ომი ცივილიზაციისა და სამყაროს მუდმივად თანმდევი მოვლენაა სამხედრო სფერო და, შესაბამისად, სამხედრო ჟურნალისტიკაც დროსთან ერთად იხვეწება და სულ უფრო აქტუალური ხდება. საუკუნეების განმავლობაში საქართველოს ომის თვალსაზრისით უამრავი გამოცდილება დაუგროვდა, რომლებიც 2008 წლის

საქართველო-რუსეთის ომმა „დაავიწვინა“. ამდენად, ომის ჟურნალისტიკის განვითარების მნიშვნელობა დღითიდღე იზრდება. რასაკვირველია, ომის ჟურნალისტიკა არსებითად არ განსხვავდება ჟურნალისტიკის ძირითადი პრინციპებისგან, როგორც სამოქალაქო ისე სამხედრო ჟურნალისტიკისთვის უმთავრესია 1983 წელს, პარიზში, საერთაშორისო და რეგიონულ ჟურნალისტთა ასოციაციის მიერ ჩამოყალიბებულ პრინციპებთან თანხვედრა, რომელთაგანაც პირველი და ჩვენი აზრით, ყველაზე მნიშვნელოვანია შემდეგი: „ხალხსა და ინდივიდებს აქვთ უფლება მიიღონ ობიექტური სურათი რეალობისა ისევე, როგორც ნებისმიერი მედიასაშუალებით თვითგამოხატვის შესაძლებლობა.“ ამდენად, ომის გაშუქების დროს ჟურნალისტმა რეალური სურათის ჩვენება უნდა დაისახოს მიზნად, მისი მთავარი მიზანი უნდა იყოს ინფორმაციის მიწოდება საზოგადოებისთვის ყველანაირი ემოციებისა და შეფასებების გარეშე. მიუხედავად იმისა, რომ კარგად გვესმის და ვიაზრებთ კონფლიქტურ სიტუაციებში მუშაობის სირთულეს, მიგვაჩნია, რომ ობიექტურობა ეს არის ის უმთავრესი თვისება, რომელიც კრიტიკულ სიტუაციებშიც კი არ უნდა დაკარგოს ჟურნალისტმა.

სანამ უშუალოდ ჟურნალ „არსენალის“ განხილვაზე გადავალთ ჩვენ გვინდა გავიხსენოთ ის ხარვეზები, რომლებიც 2008 წლის ომის მიმდინარეობისას ჟურნალისტთა საქმიანობაში გამოვლინდა. კერძოდ :

- 2008 წლის 8 აგვისტოს, შუადღეს სოფელ მეღვრევისის შესახვევთან მდგარმა ერთ-ერთმა ქართულმა ტელეარხმა პირდაპირი ჩართვა სწორედ მაშინ დაიწყო, როდესაც გზაზე ცხინვალისკენ მიმავალი ქართული სამხედრო კოლონა გამოჩნდა .

- რუსთავი 2-ის საომარი მოქმედებებისას მომზადებულ მასალაში, კერძოდ, ნანუკა ჟორჯოლიანის სიუჟეტში ისმის შემახილები : „ წავედით...სად წავედით???“ „წელა ტანკი“, როდესაც ტანკი საერთოდ არ ყოფილა იქ.

- მოდელირებული ქრონიკა, როდესაც მოვლენების ინსცენირებას შეეცადნენ ჟურნალისტები და რუსული ჯარი საქართველოს ტერიტორიაზე კიდევ ერთხელ „შემოიყვანეს“.

- ტელეკომპანია “რუსთავი-2” ინფორმაციას ავრცელებდა, თითქოს ქართული არმია ცხინვალის 70%-ს აკონტროლებდა, დანარჩენ 30%-ში კი გაწმენდითი ოპერაციები მიმდინარეობდა.

ეს იმ უხეში შეცდომების მცირე ჩამონათვალია, რომლებმაც ჟურნალისტური საქმიანობის შესრულების პროცესში იჩინეს თავი. საკითხავია რა იყო ამის გამომწვევი მიზეზი? ჩვენი აზრით, ამის უმთავრესი მიზეზი არასათანადო მომზადება და ომის ჟურნალისტიკაში მოქმედი წესების არცოდნა იყო. ქართული მედია ინფორმაციას სეგმენტურად და ფრაგმენტულად გადმოსცემდა, უამრავი მშვიადობიანი მოქალაქე აგვისტოს მოვლენებს ერთადერთი რამის გამო შეეწირა - მათ საფრთხის შესახებ ინფორმაცია არ ჰქონდათ, ეს ხალხი სახლებში დარჩა, და ტელევიზორებს უყურებდა. ყველაზე დიდი შეცდომა, რომელიც ქართულმა მედიასაშუალებებმა დაუშვეს იყო ჩვენი ჯარების მოძრაობისა თუ განლაგების პირდაპირი ეთერით გაშუქება, მაშინ

,როდესაც რუსეთს თავისუფლად შეეძლო სწორედ ქართული მედიების საშუალებით , უბრალოდ ტელევიზორის ჩართვით ჩვენი სამხედრო სტრატეგიებისა და ძალის შესახებ ინფორმაციის მიღება და,შესაბამისად,ჩვენს წინააღმდეგ გამოყენება.აქვე გვინდა შეგახსენოთ მსგავსი ფაქტი,რომელიც უახლოეს წარსულში 2017 წელს გადაგვხვდა თავს,კერძოდ,ბერი გაბრიელ სალოსის ქუჩაზე მომხდარი ტერორისტული აქტი,რომლის დროსაც რამდენიმე საათის განმავლობაში მედიაშუალებები პირდაპირი ეთერით გადასცემდნენ სპეცრაზმის განლაგებისა და მოძრაობის შესახებ ინფორმაციას, რაც ხელმისაწვდომი იყო,როგორც მოსახლეობისათვის ,ისე შენობაში გამაგრებული ტერორისტებისთვის.მიუხედავად იმისა,რომ ეს ხარვეზი მალევე გამოსწორდა და შემდგომში უკვე 20 წუთის დაგვიანებით გადაიცემოდა ინფორმაცია,მაინც შეგვიძლია დავასკვნათ,რომ 2008 წლის ომში დაშვებული ხარვეზების აღმოფხვრა დღემდე ვერ მოხერხდა. არსებობს ომის დროს ჟურნალისტების მოქმედების ძირითადი პრინციპები და სავარაუდო სამოქმედო გეგმაც თეორიის სახით,რომლის განხორციელება არცთუ ისე ეფექტიანად შეძლებს ჟურნალისტებმა ჩვენ მიერ განხილულ ბოლო ორ შემთხვევაში.აღსანიშნავი და სამწუხაროა ის ფაქტი,რომ ქართულმა მედიამ 3 ჟურნალისტი დაკარგა, აგრეთვე ომმა იმსხვერპლა ჰოლანდიელი ტელეოპერატორი სტან სტორიმანსი.

მოსახლეობის ცნობიერების დონის ამაღლება და მსოფლიოში მიმდინარე სამხედრო მდგომარეობის შესახებ ინფორმაციის სისტემატურად გავრცელება უმნიშვნელოვანესია , შესაბამისად ჩვენ გვინდა განვიხილოთ საქართველოში მოქმედი ერთადერთი სამხედრო თემატიკის ჟურნალ „არსენალის“ 2018 წლის თორმეტივე ნომერი და გამოვკვეთოთ ის ტენდენციები,რომლებიც თემატური თვალსაზრისით ჭარბობს ამ წლის ნომრებში.

ჩვენი ისტორია

2018 წლის თორმეტივე ნომერში გამოყოფილი ეს რუბრიკა ეხება რუსეთის „ჰიბრიდულ ომს“ საქართველოს რესპუბლიკის წინააღმდეგ. ნომრებში თანმიმდევრულად ვეცნობით საბჭოთა კავშირის კარგად დაგეგმილ პოლიტიკას-ფარული სატელეფონო მოსმენებით, ჩვენი ქვეყნის შეიარაღების სრული შესწავლით, ბოლშევიკების ეკონომიკური ომის და სამხედრო დაზვერვის სრულ ანალიზს. საინტერესოა, რომ რუბრიკა ამ ომის პერიოდში გამოჩენილი გენერლების პიროვნებებთან ერთად მათ ტაქტიკებსაც გვაცნობენ, ჟურნალისტური თვალსაზრისით ერთ-ერთი ყველაზე საინტერესო ნაწილი კი ერთი ფაქტის ყველა არსებული ვერსიის წარმოდგენაა მკითხველისთვის. მაგალითად: 1919 წლის 13 სექტემბრის ტერაქტის ქართული და საბჭოთა საგარეო დაზვერვის ვერსიები. ჟურნალისტები გვაწვდიან ორ არსებულ ვერსიას, რომელთა შორისაც „არჩევანის გაკეთება“ უკვე ჩვენზეა. ეს მიუკერძოებელი ტენდენციაა და შესაბამისად, ფაქტის ორივე და არსებულ კონტექსტში წარმოჩენა აღნიშნულ სტატიაზე მომუშავე ჟურნალისტების პროფესიონალიზმს უსვამს ხაზს. ფაქტობრივად, ესაა რუბრიკა, რომელიც ჩვენი ქვეყნის თავს გამოვლილი წინა საუკუნის ომის მსვლელობას ნათლად გვიხატავს, შესაბამისად, მკითხველს საშუალება ეძლევა „ძველი“

და „ახალი“ ომის მსვლელობის შედეგების, რადგან მტერი რეალურად არ შეცვლილა, წინა საუკუნეში თუ იყო საბჭოთა კავშირი, 2008 წელს იყო რუსეთი.

რა თქმა უნდა, შეუძლებელია არსენალის 2018 წლის ნომერზე საუბარი აგვისტოს ომის გარეშე, რომელსაც ჟურნალმა მერვე ნომერში 7 რუბრიკა მიუძღვნა. ამ ნომერში ომის წინმსწრები პერიოდიდან დაწყებული ომის შემდგომი პერიოდით დამთავრებული ყველა დეტალი და ნიუანსია განხილული. პირველი რუბრიკა რუსეთის მომზადების, კერძოდ, ჩრდილო კავკასიის სამხედრო ოლქის სწავლების „კავკაზ 2008“ ის შესახებ უყვება მკითხველს. კარგადაა განხილული ყველა ის დეტალი, რომელიც გვარწმუნებს რომ 2008 წლის აგვისტოს ომი წინასწარ კარგად იყო დაგეგმილი. როგორც აღმოჩნდა რუს ჯარისკაცებს დაურიგეს ფურცლები სახელწოდებით „იცნობდე შენს მტერს“, რომელშიც მოცემული იყო საქართველოს არმიის შემადგენლობა, შეიარაღება, მისი ძლიერი და სუსტი მხარეები. რუბრიკა თანამიმდევრულად მიყვება ომის მსვლელობას - ფაქტობრივად აცოცხლებს 10 წლის წინანდელ საქართველოს, განსაკუთრებით კი გორს. ჟურნალის აღნიშნულ ნომერში ხუთდღიანი ომის თითოეული დღის დეტალური განხილვაა მოცემული. როგორც ჩვენი, ისე რუსეთის ყველა ქმედების დაწვრილებით აღწერას თან ახლავს შესაბამისი ფოტოსურათები-ტანკების, რაკეტების, ბომბდამშენების და ა.შ. რეალურად ესაა ომის მსვლელობის სრულყოფილი გაშუქების თვალსაჩინო მაგალითი, რომელიც ომში მონაწილე ოფიცრების ინტერვიუებითაა გაჯერებული. როგორც ჟურნალის ტური პროდუქტი ინფორმაციული თვალსაზრისით საკმაოდ კარგია, ფაქტებს თან კომენტარებიც ახლავს, რომლებიც სრულყოფს, ამდიდრებს აღწერილს და გამიჯნულია ერთმანეთისაგან. ახალ თაობას, რომელსაც ბუნდოვნად, ან საერთოდ არ ახსოვს 2008 წლის ომი, სრულყოფილი წარმოდგენა ექმნება თუ რა ხდებოდა და როგორ მიმდინარეობდა ხუთდღიანი ომი, რა ტიპის არტილერიას იყენებდა ორივე მხარე, რა უძღოდა წინ ამ კონფლიქტს და რეალურად, რა შედეგების წინაშე აღმოვჩნდით ჩვენ.

განხილული რუბრიკები 2018 წლის ყველა ნომერში მეორდებოდა, ამიტომ სამართლიანად მივიჩნით მათი გამოყოფა და უფრო დეტალურად განხილვა, თუმცა ამ რუბრიკების გარდა სხვადასხვა ნომერებში იყო დროებითი რუბრიკებიც საინტერესო და აქტუალური თემების შესახებ, სწორედ ერთ-ერთი ასეთი იყო ტერორიზმი- ოცდამეერთე საუკუნის ყველაზე მწვავე თემა, რომელიც აჰმეთ ჩატაევს და 2017 წლის 22 ნოემბრის ბერი სალოსის ქუჩაზე მომხდარ ტერორისტულ აქტს ეხება. სტატიაში დეტალურადაა აღწერილი ჩატაევის მიერ განვლილი გზა თბილისში ჩატარებულ ოპერაციამდე. გარდა იმისა, რომ სტატია ინფორმაციული თვალსაზრისით საკმაოდ საინტერესო და სრულყოფილია, აღსანიშნავია ისიც რომ დაცულია ჟურნალის ტური ეთიკის ნორმები, რომელსაც უნდა ვიცავდეთ ტერორიზმის გაშუქებისას. კერძოდ, ჟურნალისტები ყველანაირად ერიდებიან რომანტიზების ტენდენციას, რაც სამწუხაროდ ტელევიზიების მიერ შექმნილ რეპორტაჟებში გამოიკვეთა (იმედი, რუსთავი2).

ასევე აღსანიშნავია რუბრიკები, რომლებშიც განხილულია საქართველოს პოლიტიკური და სამხედრო ურთიერთობები სხვა ქვეყნებთან. მაგალითად: ჩვენი ურთიერთობა გერმანიასთან და მის როლი ჩვენი ქვეყნის NATO-ში გაწევრიანებასთან

დაკავშირებით. ბოლოს გვინდა გამოვყოთ ყველაზე ემოციური რუბრიკა ვეტერანების შესახებ, რომლებშიც ვეცნობით ომში მონაწილე ადამიანებს და დაწვრილებით ვისმენთ მათ ისტორიებს.

ჟურნალ „არსენალის“ 2018 წლის ნომრების განხილვის შემდეგ გამოიკვეთა ძირითადი თემები, რომლებიც პროცენტული მაჩვენებლების მიხედვით შემდეგნაირად გადანაწილდა.

საბოლოოდ, გვინდა შემოგთავაზოთ იმ რეკომენდაციების მცირე ჩამონათვალი, რომელთა გათვალისწინებაც ჟურნალისტებს ხელს შეუწყობს, რომ ომისა თუ კრიზისული სიტუაციების გაშუქებისას იმუშაონ უსაფრთხოდ და ეფექტიანად.

- აუცილებელია საინფორმაციო თავშესაფრის არსებობა, რომელიც სათანადოდ გამაგრებული და შესაფერისად მოწყობილი იქნება-თავისი სარეზერვო და პირველადი დახმარების პუნქტებით. საჭიროების შემთხვევაში უკან დახევის გეგმა და სათანადო მარშრუტის არსებობაც აუცილებელია.

- არცერთი რეპორტაჟი, მიუხედავად მისი მნიშვნელობისა, არ ღირს ჟურნალისტის სიცოცხლის ან ფიზიკური ზიანის ფასად.

- საჭიროა ჟურნალისტებს ჰქონდეთ სპეციალური აღჭურვილობა, მუზარადი და ჯავშანჭილეთი, რომელსაც აუცილებლად უნდა ჰქონდეს წარწერა Press ან TV, ისინი არცერთ შემთხვევაში არ უნდა იყოს ხაკისფერი.

- არცერთ შემთხვევაში ოპერატორი არ უნდა ამოეფაროს კედელს და სანგრიდან თავაწეულმა არ უნდა დაიწყოს გადაღება, რადგან ამ დროს კამერა იარაღის ასოციაციას იწვევს და შესაძლოა ვერ მოხერხდეს ჟურნალისტისა და მეომარის ერთმანეთისგან გარჩევა.

სამწუხაროდ ამ რეკომენდაციებს დასავლური ქვეყნების ჟურნალისტები უფრო მისდევენ, ვიდრე ქართველები, რის გამოც სავალალო შედეგების წინაშეც ხშირად აღმოვჩენილვართ. გასათვალისწინებელია ის ფაქტი, რომ ჟურნალისტთა საქმიანობა საკმაოდ საპასუხისმგებლოა, განსაკუთრებით კი კრიზისული სიტუაციებისა და ომის გაშუქების დროს, შესაბამისად, ვისურვებდით, რომ ამ მიმართულებით ქცევის კოდექსის შემუშავება და ჟურნალისტთა სპეციალური გადამზადება მოხდეს.

ბიბლიოგრაფია

1. ჟურნალ „არსენალის“ 2018 წლის 12 ნომერი

2. ვარდიაშვილი, ზურაბ. 2012 „ომის პირველი მსხვერპლი - სიმართლე”.
Liberali. ბოლო ნახვა 30.02.20 <http://liberali.ge/articles/view/2601/salome.ge>

„რუტკიტი“, როგორც კიბერდანაშაულის იარაღი“
"Rootkit" as a weapon of cybercrime "

1. ნათია ფილაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო
უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი.
Natia Pilashvili_ Ivane Javakhishvili Tbilisi State University, Sociology_Junior;

2. მარიამ კიკლიაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო
უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი.
Mariam Kikliashvili_ Ivane Javakhishvili Tbilisi State University, Sociology_Junior

ანოტაცია: XXI საუკუნეში, სწრაფი ტექნოლოგიური პროგრესის პარალელურად, გამოუვლენელი და გაუხსნელი დანაშაულების ყველაზე მზარდი ტენდენცია კიბერდანაშაულის კუთხით აღინიშნება, რომელსაც ხშირად „მომავლის დანაშაულსაც“ უწოდებენ. მავნე პროგრამები, რომლებიც კიბერდანაშაულის ერთ-ერთი მთავარი მექანიზმია, თითოეულ ჩვენგანს მათ მსხვერპლად ადვილად გვაქცევს. სწორედ, ერთ-ერთ ასეთ მავნე პროგრამას წარმოადგენს „რუტკიტი“, რომლის საშუალებითაც მსოფლიოში 60 000-მდე ადამიანი დაზარალდა.

ANNOTATION: In the 21st century, in parallel with rapid technological progress, the increasing trend of unsolved and inexcusable crimes is marked by cybercrime, often referred to as "the crime of the future." Malicious software, one of the key mechanisms of cybercrime, makes it easy for us to be victims of it. One of these Malware programs is "Rootkit", about 60,000 people around the world have been affected by this.

საკვანძო სიტყვები: კიბერსივრცე, კიბერდანაშაული, დისტანციური მართვის მექანიზმი(RAT), მალვარი(Malware), „რუტკიტი“;

„რუტკიტი“, როგორც კიბერდანაშაულის იარაღი“

კიბერსივრცე ეს არის ინფორმაციულ - ტექნოლოგიური ინფრასტრუქტურის ურთიერთდაკავშირებული კომპლექსი, რომელიც თავის თავში აერთიანებს კომპიუტერულ სისტემებს, ინტერნეტის გლობალურ და ტელესაკომუნიკაციო ქსელებს. კიბერსივრცეში არსებული მდგომარეობა დღითიდღე უფრო შემამფოთებელი ხდება. კარგად შესრულებულ კიბერშეტევას შეუძლია, როგორც გავლენის მოხდენა, ასევე ზიანის მიყენება ნებისმიერ სექტორზე. მისი საშუალებით შესაძლებელია ყველა დონეზე სახელმწიფო სტრუქტურების

პარალიზება. კიბერსივრცეში უსაფრთხოების უზრუნველყოფა მთელ რიგ სირთულეებთან არის დაკავშირებული.

ისეთი პროგრამები, როგორებიცაა „Malware“, „Riskware“ და „Spyware“ ქსელურ სისტემაში მიიჩნევიან განსაკუთრებით დიდი საფრთხის გამომწვევად. ამ საზიანო პროგრამების ეფექტი მოიცავს: კომპიუტერული სისტემის მწყობრიდან გამოყვანას, მომხმარებელთა კონფიდენციალური ინფორმაციის მიღებასა და მათ გამოყენებას უკანონო მიზნებისათვის.

მაღვეარი („Malware“) წარმოადგენს ინტრავირუსულ პროგრამას. იგი მოიცავს კომპიუტერულ ვირუსებს, “ტროიანებს” (“ტროას ცხენი”), “რუტკიტებს”, “კილოგერებს”, “ედვეარს”, “რენსომვეარს”, “ვორმებს”, “სპაივეარს”, საზიანო “BHO”-სა და სხვა საზიანო პროგრამებს. მათმა არსებობამ საჭირო გახადა ისეთ დამცავ პროგრამათა შექმნა, როგორც არის ანტიმაღვეარები და ანტივირუსები. აღნიშნული პროგრამები აქტიურად გამოიყენება კერძო მომხმარებელთა მიერ, კომპიუტერების, პირადი ინფორმაციისა და მათზე უნებართვო წვდომისაგან თავის დასაცავად.

„რუტკიტი“ არის პროგრამა, რომელიც ცდილობს თავის არსებობას მაღავს უსაფრთხოების პროგრამებისგან თავის აცილების გზით. კომპიუტერში შეღწევის შემდეგ, იგი საიდუმლო კონტროლის საშუალებას აძლევს დისტანციურ მომხმარებელს კომპიუტერის ოპერაციული სისტემაზე. მისი მიზანი არაა საკუთარი თავის რეპლიკაცია. ჰაკერები მას იყენებენ კომპიუტერული სისტემის დისტანციურ მართვის მექანიზმად (RAT – Remote Administration Tool). პროგრამა შეიძლება კომპიუტერზე იყოს, თუმცა ჩვენ ამის შესახებ არაფერი ვიცოდეთ. მიზანი მარტივია, კომპიუტერული მოწყობილობათა გამოყენება, როგორც ფინანსური, ასევე სხვა ტიპის მოგების მისაღებად.

ტერმინი „rootkit“ არის "root" („Unix“ - ის მსგავსი ოპერაციული სისტემების პრივილეგირებული ანგარიშის ტრადიციული სახელი) და სიტყვა "kit"-ის (პროგრამული კომპონენტები, რომლებიც ახორციელებენ ამ ხელსაწყოს) ნაერთი.

„რუტკიტი“ შესაძლოა სპამების სახითაც იყოს წარმოდგენილი და დამალული იყოს ნებისმიერ ფაილში, განსაკუთრებით კი არალიცენზირებულ პროგრამებში. „რუტკიტის“ ამოცნობა ანტივირუსისთვის ფაქტობრივად შეუძლებელია. ის ანტივირუსს მარტივად უვლის გვერდს და ოპერაციულ სისტემაში ფარულად იდებს ბინას, საიდანაც ჰაკერს მისთვის სასურველ ინფორმაციას აწვდის.

ყოველწლიურად, 60,000-მდე ადამიანი ხდება „რუტკიტის“ მსხვერპლი. სპამებით შემოტევის ყველაზე დიდი მაჩვენებელი კორპორაციებში, გასულ წლებში ფიქსირდებოდა ევროპისა და ამერიკის რეგიონში, თუმცა ბოლო პერიოდში აზია დაწინაურდა.

ლეინ დევისმა და სტივენ დეიკმა შექმნეს ყველაზე ძველი და ცნობილი „რუტკიტი“ 1990 წელს „Sun Microsystems 'SunOS UNIX“ ოპერაციული სისტემისთვის. „Windows NT“

ოპერაციული სისტემისთვის პირველი მავნე „რუტკიტი“ გამოჩნდა 1999 წელს, რომელიც შექმნა გრეგ ჰოგლუნდმა.

2005 წელს, პროგრამული უზრუნველყოფის ინჟინერმა მარკ რასინოვიჩმა შექმნა „რუტკიტის“ გამოვლენის ინსტრუმენტი „RootkitRevealer“, რის შემდეგაც აღმოაჩინა „რუტკიტი“ მის ერთ-ერთ კომპიუტერზე. მომხდარმა სკანდალმა საზოგადოების ცნობიერების ამაღლება გამოიწვია „რუტკიტის“ შესახებ.

„რუტკიტის“ ორი ძირითადი ტიპია: მომხმარებლის რეჟიმის(“User-mode”) „რუტკიტი“ და ბირთვის რეჟიმის(“Kernel-mode”) „რუტკიტი“. მომხმარებლის რეჟიმის(“User-mode”) „რუტკიტი“ თავსდება კომპიუტერის ოპერაციულ სისტემაში, როგორც პროგრამები. ისინი ახორციელებენ თავიანთ მიზანს აპარატზე მუშაობის პროცესში მეხსიერების გადაწერით, რომელსაც პროგრამა იყენებს. ბირთვის რეჟიმის(“Kernel-mode”) „რუტკიტი“ მუშაობს კომპიუტერის ოპერაციული სისტემის ყველაზე დაბალ დონეზე და თავდამსხმელს ანიჭებს ყველაზე ძლიერ პრივილეგიებს კომპიუტერში. ბირთვის რეჟიმის(“Kernel-mode”) „რუტკიტის“ დამონტაჟების შემდეგ, თავდამსხმელს აქვს სრული კონტროლი კომპიუტერულ სისტემაზე და შესაბამისად, შეუძლია ნებისმიერი მოქმედების განხორციელება საკუთარი მიზნებისთვის. ბირთვის რეჟიმის (“Kernel-mode”) „რუტკიტი“, როგორც წესი, უფრო რთული აღმოსაჩენი და აღმოსაფხვრელია, ვიდრე მომხმარებლის რეჟიმის(“User-mode”) „რუტკიტი“ და უფრო ნაკლებადაა გავრცელებული.

ბოლო წლების განმავლობაში, წარმოიქმნა მობილური „რუტკიტის“ ახალი კლასი, სმარტფონებზე, კონკრეტულად Android მოწყობილობებზე შეტევებისთვის.

კარგად ცნობილი „რუტკიტის“ მაგალითებია:

„Machiavelli“ - პირველი “რუტკიტი”, რომელიც მიზანში იღებს “Mac OS X”-ის ოპერაციულ სისტემას და გამოჩნდა 2009 წელს. ეს “რუტკიტი” ქმნის ზარების დაფარულ სისტემას.

„Zeus” - რომელიც პირველად იდენტიფიცირდა 2007 წლის ივლისში და ფარულად იპარავდა საბანკო ინფორმაციას მოხმარებლების კომპიუტერული სისტემებიდან.

“Stuxnet” - პირველი ცნობილი “რუტკიტი” სამრეწველო კონტროლ-სისტემებისთვის.

“Flame” - კომპიუტერის „მავნე პროგრამა“, რომელიც აღმოაჩინეს 2012 წელს. თავს ესხმის კომპიუტერებს, რომლებიც მუშაობენ “Windows OS” კომპიუტერულ სისტემაზე. მას შეუძლია ჩაიწეროს ხმა, შექმნას „სკრინშოტები“ (“screenshots”) და გააკონტროლოს კლავიატურაზე წვდომა.

დღეს ჩვენი ყოველდღიური ცხოვრება უშუალოდ დაკავშირებულია ციფრულ ტექნოლოგიასთან, რაც მნიშვნელოვნად ზრდის კიბერდანაშაულების რიცხვს. ყოველი ახალი შემთხვევა უნდა იყოს ჩვენთვის მაგალითი, რომ გამოვიჩინოთ უფრო მეტი სიფრთხილე

ინტერნეტ სივრცეში ყოფნისას და არ გავხდეთ „ჩვენივე ნებით“ ჰაკერებისა და მავნე პროგრამების შემდეგი მსხვერპლი.

საჭიროა პრევენციული ღონისძიებების აქტიური გატარება. „მნიშვნელოვანია მაღალი სტანდარტების შეტევების პრევენციის სენსორული სისტემების დანერგვა, ფართო მასშტაბის კიბერკონტრაზვერვის გეგმისა და თავდაცვითი სტრატეგიების შემუშავება. ამ თვალსაზრისით პრიორიტეტულია უწყებათაშორისი კოორდინაცია და კომუნიკაცია. მნიშვნელოვანია ქვეყნის შიგნით საკანონმდებლო ბაზის არა მარტო შემუშავება, არამედ აღსრულება. ამ პრობლემასთან გამკლავება ასევე საჭიროებს მჭიდრო საერთაშორისო თანამშრომლობას.“¹

ბიბლიოგრაფია

1. "What is a rootkit and how to remove it" Written by Serge Malenkovich on March 28, 2013
https://www.kaspersky.com/blog/rootkit/1508/?fbclid=IwAR3fQU_Cldd3WgxwKome2IJ7n_nO-Fj62IDPv2Kobkl-A3T26zh3qx7MbFQ
2. "ROOTKIT: WHAT IS A ROOTKIT?
Rootkit: What Is a Rootkit, Scanners, Detection and Removal Software"
https://www.veracode.com/security/rootkit?fbclid=IwAR0hx_sd739-mYTSA8Q4u8R48BTrIA-OF-7_z832CaHaQnir_1F2hB-3M
3. "What is Malware? How Malware Works & How to Remove It" by Joseph Regan on July 11, 2019
https://www.avg.com/en/signal/what-is-malware?fbclid=IwAR1up9OviyqJypGSZeKYi_j8UtryCh89ZFiaPAC3JNN1EH1kjWjtTkzSeYA
4. სისხლის სამართლის კერძო ნაწილი. წიგნი 2. მ.ლეკვეიშვილი, ნ.თოდუა და გ.მამულაშვილი. გამომცემლობა „მერიდიანი“, თბ. 2017

¹ სისხლის სამართლის კერძო ნაწილი. წიგნი 2. მ.ლეკვეიშვილი, ნ.თოდუა და გ.მამულაშვილი. გამომცემლობა „მერიდიანი“, თბ. 2017, გვ 145;