SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL4 No3
DECEMBER 2019

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 34 - 47 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

МЕТОД КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ СТРУКТУРЫ СОЦИАЛЬНОЙ СЕТИ ДЛЯ ЗАДАЧ ИССЛЕДОВАНИЯ ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ

Александр Уличев, Елизавета Мелешко, Виталий Хох
Центральноукраинский национальный технический университет, Кропивницкий, Украина

АННОТАЦИЯ. В данной работе исследовались методы моделирования структуры социальных сетей, а также был предложен метод компьютерного моделирования сегмента социальной сети с заданным количеством кластеров для задач исследования процессов распространения информационных воздействий. Была создана компьютерная модель для генерации сегмента социальной сети с разными структурными свойствами для моделирования и исследования процессов распространения информационных влияний. Разработанная компьютерная модель позволяет исследовать: как влияет структурная позиция субъекта влияния на его эффективность в распространении информации, как влияет структура сети на ее робастность по отношению к внешним информационным воздействиям, через сколько времени субъект информационного влияния сможет воздействовать на заданное количество узлов.

КЛЮЧЕВЫЕ СЛОВА: социальная сеть, информационная безопасность, теория графов, компьютерное моделирование, информационные влияния

THE COMPUTER SIMULATION METHOD OF A SOCIAL NETWORK STRUCTURE FOR THE RESEARCH OF DISSEMINATION PROCESSES OF INFORMATIONAL INFLUENCES

Oleksandr Ulichev, Yelyzaveta Meleshko, Vitaliy Khokh
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

ABSTRACT. In this paper, the simulation methods of a social network structure were researched and also the computer simulation method of a social network segment with a given number of clusters for the research of dissemination processes of informational influences was proposed. The computer model to generate a social network segment with different structural properties for modeling and researching processes of disseminating information influences was created. The developed computer model allows one to research: how a structural position of a subject of influence affects his efficiency in the dissemination of information, how the network structure affects its robustness with respect to external information influences, after how much time a subject of information influence can affect a given number of nodes.

KEYWORDS: social network, information security, graph theory, computer simulation, information influence

ВВЕДЕНИЕ. Моделирование социальных сетей – это важная научная задача, которая используется для исследования социальных процессов, например, процесса распространения информации и/или информационных воздействий, процесса формирования репутации участников социальной сети, процесса информационного управления и противоборства, и т.д.

С точки зрения информационной безопасности важными вопросами, на которые может помочь найти ответы компьютерное моделирование, являются такие: как влияет структурная позиция субъекта влияния на его эффективность в распространении информационных влияний, как влияет структура сети на ее робастность по отношению к внешним информационным воздействиям, через сколько времени субъект информационного влияния сможет воздействовать на заданное количество узлов.

В целом моделирование социальных сетей в первую очередь используется для осуществления [1]:

– анализа структуры сети (например, поиска лидеров мнений, поиска скрытых сообществ и скрытых связей и т.д.);

– исследования социальных процессов (например, распространение слухов и т.д.).

– исследования процесса формирования и развития социальной сети (например, исследование влияния репутации участников социальной сети на динамику изменения ее структуры во времени).

Наиболее часто для моделирования социальных сетей используют графовые модели [1, 2].

Социальную сеть можно представить в виде графа:

$$G = (V, E), \tag{1}$$

где V – вершины графа, представленные участниками (и, возможно, объектами социальной сети, такими как сообщения, комментарии, «лайки» и т.д.); E – ребра графа, представленные связями различного типа между участниками и объектами сети.

В данной работе вершинами графа будут пользователи социальной сети, а ребрами – социальные связи между ними, которые предполагают возможность обменом информационными сообщениями.

Исследователи выделяют следующие графовые модели социальных сетей [2, 3]:

1. **Обычные графовые модели.** Задаются матрицей смежности G, размерностью, $n \times n$, где n – число участников сети.

2. **Стохастические блоковые модели.** Задаются матрицей смежности G, размерностью $n \times n$, где n – число блоков участников сети. Элемент $g_{ij} \in [0; 1]$ показывает плотность связей между участниками сети, принадлежащими блоку i, и участниками, принадлежащих блоку j. При этом граф не содержит ребер и вершин, показывающих связи участников сети внутри одного блока.

3. **Вероятностные графовые модели.** Задаются матрицей смежности G, размерностью $n \times n$, де n – число участников сети. Элемент $g_{ij} \in [0;1]$ показывает вероятность взаимодействия участника i и участника j в течении определенного периода времени.

Для исследования социальных процессов необходимо моделировать динамическую социальную сеть. Моделью динамической сети может быть **динамический граф** [4]. Динамический граф D, представляет собой

последовательность классических графов G_k, переход между которыми описывается различными графовыми операциями $\varphi(G_k) = G_{k+1}$.

Графовые операции можно разделить на базовые и сложные [4]. К базовым операциям относятся: добавление/удаление ребра, добавление/удаление вершины. Любую сложную графовую операцию можно описать последовательностью базовых графов операций. Операция, осуществляющая переход от графа G_k к графу G_{k+1} может быть как базовой так и сложной. Для построения динамического графа можно использовать множество графовых операций $\Phi = \{\varphi^t\}$. Последовательность графов $G_1, G_2, G_3, \ldots G_m$ называется траекторией динамического графа [4].

Для анализа динамических графов применяются методы извлечения ассоциативных правил и методы анализа частотных моделей, для прогнозирования изменений в динамическом графе могут использоваться иерархические, вероятностные и реляционные модели, модели основаны на свойствах социальных сетей и модели основаны на свойствах участников сети [2, 4].

Кроме графовых моделей для моделирования социальных сетей могут применяться клеточные автоматы, цепи Маркова, модели Изинга, модели просачивания и заражения, модели независимых каскадов, модели с порогами, модели основанные на теории игр [5], агентные модели [6] и т. Данные модели позволяют исследовать распространение информационных воздействий в социальных сетях, влиятельность участников сети и т.д., и могут применятся в комбинации с графовыми методами.

Целью статьи является разработка метода компьютерного моделирования структуры сегмента социальной сети с заданным количеством кластеров, который в дальнейшем можно использовать для моделирования и исследования процессов распространения информационных воздействий в социальных сетях.

ОСНОВНОЙ МАТЕРИАЛ

При моделировании социальной сети следует учитывать, что ее структура состоит из различных типов кластеров [3, 7, 8]. Различными исследователями выделен ряд типов кластеров социальной сети с характерными конфигурациями. Среди них стоит выделить в частности следующие: группа, лидерская группа, клика.

Предлагается представлять социальную сеть как набор определенных подграфов – типов кластеров и рассматривать ее с точки зрения сетевого подхода [9, 10, 11] с учетом определенных ограничений.

Дадим определения некоторым избранным типам кластеров.

Группа (Г) – граф с таким набором связей, что каждые два узла связаны напрямую или через другие узлы. В литературе такое подмножество часто называют – «целостная сеть» [12]. Схематически граф типа «Группа» представлен на рис. 1.

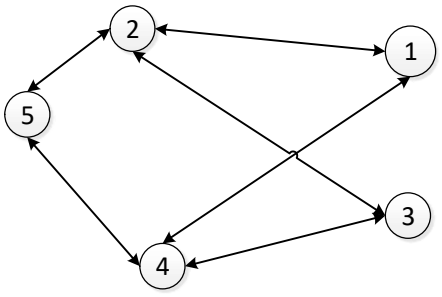

Рис. 1. Подграф социальной сети типа «Группа»

Клика (К) – граф в котором каждый узел связан с каждым, или, другими словами – все вершины графа смежные (рис. 2).

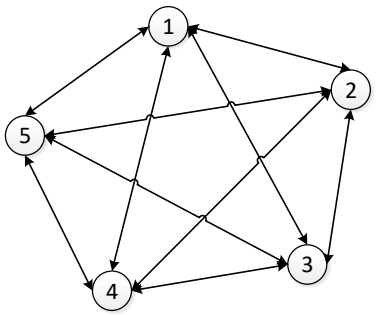

Рис. 2. Подграф социальной сети типа «Клика»

Такие кластеры в социальных сетях представляют интерес с точки зрения анализа информационной безопасности сети. В частности, в исследовании [13] указывается, что кластеры типа «клика» являются наиболее устойчивыми и активными, с точки зрения информационного обмена и влияния на окружающие узлы (другие субъекты сети). Теоретически в пределах клики могут формироваться противоположные идеи, но на практике, в большинстве случаев, «клика» объединяет единомышленников с общими интересами и идеями. Участники клики, обычно общаются и вне сети, их связи достаточно устойчивы и стабильны. Уровень информационного воздействия на порядки выше в отличие от кластеров, где основным носителем идеи есть отдельный субъект, так как в случае «клики» носителем и активным распространителем идеи выступает целый кластер, отображается и на количестве связей с внешними (по отношению к клике) узлами и на плотности информационного обмена. В исследовании [13] указывается и на возможность оценки возраста (зрелости) сети (как давно она сформировалась). Наличие клик с большим количеством узлов говорит о достаточно долгом существовании сети. Поиск клик и их анализ является одной из основных задач структурного анализа сетей.

«Смягченный» вариант клики называют К-плекс (понятие введено авторами [11]) – в таком графе не все, но подавляющее большинство узлов связаны между собой.

Лидерская группа (ЛГ) – подвид группы с одним или несколькими влиятельными узлами-лидерами, лидеры имеют связи со всеми другими узлами группы (рис. 3).

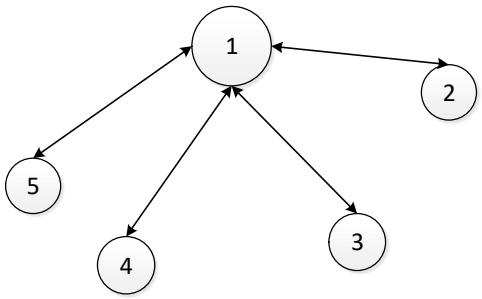

Рис. 3. Подграф социальной сети типа «Лидерская группа»

«ЛГ» фактически является подвидом «Г» с точки зрения теории графов, но существенно отличается с точки зрения структуры построения коммуникаций и развития. Такие подгруппы образуются при наличии в кластере явного лидера.

Под структурой сети можно понимать не только топологические особенности размещения узлов в графе и имеющиеся связи. В исследованиях можно встретить и другие классификации сетей, основанные на их структуре. Так в [14] приводится классификация Хефлина Ч., где сети структурируются на основе поведенческих моделей *актора* (субъекта сети) и возможностей, которые предоставляет ему та или иная сеть:

1. A-сеть. Позволяет актору обозначить и выстроить свое пребывание в социальной сети как определенной вполне реальной социальной единице с возможностью построения устойчивой социальной группы.
2. B-сеть. Позволяет актору обозначить и выстроить свое пребывание в социальной сети как определенной вполне реальной социальной единице без возможности построения устойчивой социальной группы.
3. C-сеть. Позволяет актору сформировать новые отношения внутри A и B сетей.
4. D-сеть. Вспомогательная сеть, предоставляющая инструментарий для построения и расширения функциональных возможностей отношений между акторами в сети Интернет.

При этом автор классификации отмечает не только особенности отдельного типа сети, но и решающую роль позиции субъекта в сети (пользователь, модератор, администратор и т.д.), которая влияет в дальнейшем на все информационные процессы.

Встречаются классификации на основе критериев доминантности (вес лидера и количество доминирующих лидеров) и коммуникативности (плотность связей и информационного обмена). Понятно, что все эти классификации коррелируются между собой. Сеть, относящаяся к определенной группе по критериям доминантности и коммуникативности, будет иметь и характерные наборы кластеров с их внутренней структурой.

На ряду с другими критериями структура носит определяющий характер для социальной сети и влияет на все процессы, происходящие в ходе ее функционирования и информационного обмена внутри. Структурный анализ сетей является актуальной задачей. Данная задача очень многогранна, для исследований могут использоваться различные подходы, методы и средства.

Подходы к генерации структуры социальной сети в значительной степени определяется задачами, которые ставятся перед компьютерной моделью сети. В случае данного конкретного исследования важными возможностями модели социальной сети являются следующие: наличие индивидуальных характеристик узлов и их поведенческих стратегий во время распространения информации.

Учитывая исследования других авторов и результаты обзора источников по анализу сетевых структур, для генерирования структуры сегмента социальной сети предлагается использовать набор базовых кластеров, а конкретные примеры сегментов реализовать как комбинацию выбраны следующие типы кластеров: группа, клика, лидерская группа. Кроме этого следует отметить, что в модели рассматриваются двунаправленные связи. То есть, если существует связь $V_i \rightarrow V_j$, то существует и $V_j \rightarrow V_i$.

Известно множество различных способов компьютерного представления графов, одним из способов является представление их в виде матриц смежности. Такой способ является достаточно удобным для программной реализации, а также для дальнейшей обработки и анализа, поэтому он и был использован.

Приведем примеры формального описания выбранных типов кластеров.

Формальное описание кластера типа «Группа» может выглядеть так:

$$G_{grupa} = (V_n | \forall\, V_i, V_j : i, j, k_i \leq n \; \exists \, \{E_{ik1}, E_{k1,k2}, E_{k2,k3} .. E_{kn,j}\}). \quad (2)$$

Фактически группа является связным графом, матрица смежности может иметь различный вид (зависит от плотности связей), а обязательным является условие связности – существование пути между любыми выбранными вершинами кластера.

Формальное описание кластера типа «Клика»:

$$G_{clika} = (V_n | \forall\, V_i, V_j : i, j \le n \;\exists\; E_{ij}). \quad (3)$$

Матрица смежности для клики будет иметь вид (рис. 4):

i\j	**1**	**2**	**3**	**…**	**n**
1	0	1	1	1	1
2	1	0	1	1	1
3	1	1	0	1	1
…	1	1	1	0	1
n	1	1	1	1	0

Рис. 4. Матрица смежности для кластера типа «Клика»

Формальное описание кластера типа «Лидерская группа»:

$$G_{lid\_grupa} = (V_n | \exists\, i \le n, \forall j \le n \;\exists\; E_{ij}). \quad (4)$$

Матрица смежности для лидерской группы будет характеризоваться наличием колонки и строки полностью заполненных значением 1 (кроме диагонального элемента), матрица будет иметь вид (рис. 5):

i\j	1	**2**	3	…	n
1	0	1	***x***	***x***	***x***
2	1	0	1	1	1
3	***x***	1	0	***x***	***x***
…	***x***	1	***x***	0	***x***
n	***x***	1	***x***	***x***	0

Рис. 5. Матрица смежности для кластера типа «Лидерская группа»

Здесь узел с индексом 2 является лидером группы, элементы *x* в матрице смежности означают, что на их месте могут как быть ребра (значение 1), так и не быть (значение 0).

В разрабатываемой компьютерной модели матрицы смежности кластеров сегмента сети генерируются автоматически, а также существует возможность внесения изменений в них в ручном режиме.

Предложенный подход к генерированию структуры сети позволяет генерировать сегменты сетей с достаточно разнообразной топологией, а возможность внесения корректив в ручном режиме обеспечивает возможность локально изменять ее структуру и приближать сеть в модели к реальной структуре социальной сети, которая является объектом исследования.

В данной работе генерация структуры социальной сети базируется на создании комбинации из некоторого количества параметризованных кластеров.

В базовом наборе кластеров предлагается использовать все три типа кластеров: группа, лидерская группа, клика. Основным параметром при генерации кластера является количество узлов. В качестве дополнительного параметра присутствует процент узлов кластера с высоким уровнем информационного сопротивления.

Для возможности редактирования структуры социальной сети и с целью получения сетей с заранее заданной структурой в программную реализацию компьютерной модели добавлена возможность добавления/удаления узлов и добавления/изъятия связей.

Так как базовым элементом социальной сети является узел, а компьютерная разрабатываемая модель базируется на объектном подходе, стоит начать рассмотрение модели именно с него.

Узел социальной сети в разрабатываемой модели характеризуется определенным набором параметров, определяющих его поведение и текущее состояние. В модели узел описывается следующими характеристиками:

$$V_i =< Av_i,\ Rv_i,\ O\alpha v_i,\ I\alpha v_i, \{Vj_i\} >, \tag{5}$$

где Av_i – (Active) активность пользователя V_i, количество активных диалогов (обращений к другим пользователям) за одну итерацию модели; Rv_i – (Reputation) репутация пользователя V_i, влияние информационного посыла, сила убеждения; $O\alpha v_i$ – (Opposite) информационное сопротивление пользователя V_i, критичность по отношению к идее, которая распространяется; $I\alpha v_i$ – (Involvement) степень вовлеченности в идею пользователя V_i, уровень доверия; $\{Vj_i\}$ – множество контактов, узлов с которыми существует информационный обмен у узла V_i.

Узел в разрабатываемой компьютерной модели представлен отдельным классом и имеет следующий вид (листинг 1):

Листинг 1. Класс, описывающий узел модели социальной сети.

```
public sealed class User
    {

        /// <summary>
/// Базовые характеристики узла сети
        ///  Активность узла (количество сообщений за 1 итерацию)
        /// </summary>
        public int Activity { get; set; }//(A) Active
        /// Информационное сопротивление (недоверчивость) //(Op) Opposite
        /// </summary>
        public int Opposite { get; set; }
        /// <summary>
        /// Репутация//(R) Reputation
        /// </summary>
        public int Reputation { get; set; }
        /// <summary>
        /// Вовлеченность в идею //(I) Involvement
        /// </summary>
        public int Involvement { get; set; }//
///  Графическое представление
        public double PointX { get; set; }
        public double PointY { get; set; }
        private Ellipse ellipse;
        public Ellipse Ellipse
        {
            get { return ellipse; }
```

```
            set { ellipse = value; }
        }//Точка
        public string Name { get; set; } //имя пользователя
        public List<User> FriendsList = new List<User>(); // список
контактов        /// <summary>
///  Дополнительные сервисные поля
        public int Level { get; set; }
        /// <summary>
        public List<User>ForTree = new List<User>();
        public int NumberFromMatrix { get; set; }// Порядковый номер в
матрице
       }
```

Конкретные значения полей узел получает в момент добавления к сети в зависимости от параметров, заданных при генерации кластера, конкретной роли узла и других факторов.

Далее рассмотрим метод генерирования одного из кластеров на примере лидерской группы. Лидерская группа характерна наличием узла, имеющего связи со всеми другими узлами сети.

Данный метод предусматривает несколько составляющих этапов:

1 Этап. Создание массива точек, которые будут определять визуальное положение узлов на экране;

2 Этап. Создание самих узлов (определение индивидуальных параметров) и добавления их в общий массив узлов сети;

3 Этап. Установление структурных особенностей в соответствии с выбранным типом кластера (создание связей между узлами);

4 Этап. Внесение изменений в матрицу смежности.

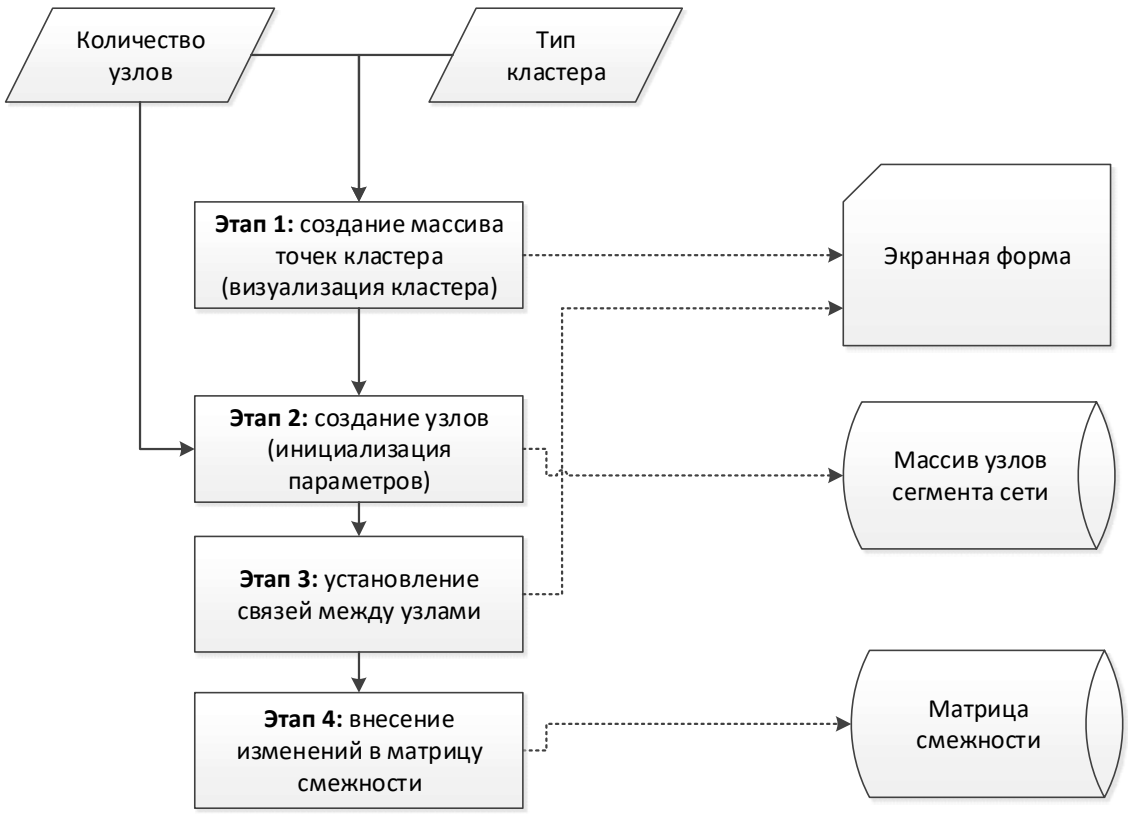

Рис. 6. Этапы метода генерации структуры социальной сети

Каждый тип кластера в конструкторе имеет ограничения на количество узлов сверху, при установке параметров пользователь может задать значение данного параметра (int countUsers) в предложенных конструктором пределах. Кроме количества узлов в метод передается центральная точка, которая определяет место размещения кластера на экране, положение других узлов кластера рассчитывается относительно данной точки.

Отдельно стоит охарактеризовать лидера группы. Логично предположить, что узел, который является лидером группы, имеет достаточно высокий уровень репутации (возможно самый высокий уровень, относительно других узлов группы). В противном случае он не может быть лидером группы. Так как лидер группы имеет наибольшее количество связей и для поддержания своего статуса должен постоянно общаться с другими членами группы, его уровень активности должен быть достаточно высоким. А информационное сопротивление должно быть не ниже среднего с точки зрения лидерской позиции в группе.

Другие узлы, если не задан параметр высокого информационного сопротивления в кластере, получают случайные значения этого параметра в допустимых пределах. Тем самым реализуется равномерное распределение характеристик по сети. Вовлеченность в идеи до первой итерации модели у всех узлов кроме генератора равно нулю. Так как положение генератора определяется уже после создания структуры сети, то этот параметр при генерации независим от типа кластера, а также для отдельно (вручную) добавленных узлов всегда равен нулю.

Формулы, используемые для начальной инициализации параметров *i*-го узла в кластере, представлены ниже:

$$\begin{gathered} Active(V_i) = random(1, KK), \\ Reputation\ (V_i) = random(1, 90), \\ Opposite\ (V_i) = random(10, 800), \\ Involvement\ (V_i) = 0, \end{gathered} \tag{6}$$

где V_i – узел группы не из числа лидеров, KK – количество контактов узла V_i.

Для узла, который является лидером группы, учитывая вышеописанные рассуждения, значения параметров активности, репутации и сопротивления несколько выше по сравнению с другими узлами в кластере:

$$\begin{gathered} Active(V_l) = [0.7 * KK], \\ Reputation\ (V_l) = 100 - \text{random}\ (20), \\ Opposite\ (V_l) = 00 + \text{random}\ (500), \\ Involvement\ (V_i) = 0, \end{gathered} \tag{7}$$

где V_l – лидер группы, KK – количество контактов лидера группы V_l.

Листинг 2. Метод добавления в сеть кластера типа «Лидерская группа».

```
internal void AddLiderGroup(Point point_, int countUsers ){
// Проверка нахождения центральной точки, представляющей узел, в допустимых
пределах на экране
    if (point_.Y > 90 && point_.Y < 620){
// Буферный массив точек, отвечающих узлам
      Point[] masPointBuf = new[]{
// Создание точек, инициализация координат смещения
        new Point(0, 0),
```

```
        new Point(10, 10),
        new Point(20, 10),
        new Point(20, 20),
        new Point(30, 10),
...
      };
// Создание массива точек в соответствии с указанным количеством узлов
      Point[] masPoint = new Point[countUsers];
// Цикл присвоении местоположение каждому узлу
      for (int i = 0; i < countUsers; i++){
        masPoint[i] = masPointBuf[i];
      }

      var      userList      =      GenarateUserList(point_,      masPoint,
UserList.Count).ToList();// Создание списка узлов кластера

// Определение случайного узла, которому присваивается роль лидера группы
      Random random = new Random();
      int lider = random.Next(0, countUsers);

// Установление значений характеристик узлов
      for (int i = 0; i < userList.Count; i++){
        if (i==lider){
        for (int j = 0; j < countUsers; j++){
// Если узел лидер группы
          if (i!=j){
            userList[i].FriendsList.Add(userList[j]);
            userList[j].FriendsList.Add(userList[i]);
            userList[i].Activity = (int) 0.7*countUsers;
            userList[i].Opposite = 500 + random(500);
            userList[i].Involvement = 0;
            userList[i].Reputation = 100 - random(20);
          }
        }
        }
        else{
        int count = random.Next(0, 2);
        for (int j = 0; j < count; j++){
          int user = random.Next(0, countUsers);
          if   (i   !=   user   &&   !userList[i].FriendsList.Any(x=>x.Name==
userList[user].Name)){
            userList[i].FriendsList.Add(userList[user]);
            userList[user].FriendsList.Add(userList[i]);
            userList[i].Activity              =              random.Next(1,
userList[user].FriendsList.countUsers);
            userList[i].Opposite = random.Next(10,800);
            userList[i].Involvement = 0;
            userList[i].Reputation = random.Next(1,90);
          }
        }
        }
       AddMatrix (userList[i]); // внесение изменений в матрицы смежности
      }
// добавление списка узлов кластера в общий список узлов сети
      UserList.AddRange(userList);
      }
    }
```

С точки зрения пользователя разрабатываемой компьютерной модели, который проводит на ней эксперименты, процесс добавления кластера заключается в выборе его

типа, установлении количества узлов (рис. 7) и выборе местоположения центральной точки кластера на рабочем поле, на котором визуализируется структура сгенерированной социальной сети.

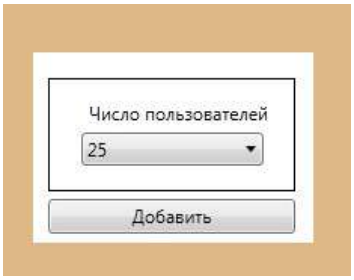

Рис. 7. Окно установки количества узлов

После отработки этого метода пользователь видит размещение кластера на рабочем поле и может выбирать разные режимы его отображения (рис. 8).

а) **б)** **в)**

Рис. 8. Различные режимы отображения кластера: (а) исходное отображение узлов кластера, (б) кластер в режиме отображения всех связей, (в) отображение связей выбранного кластера (в данном случае лидер группы)

Аналогично, с точностью до структурных особенностей типа кластера, работают методы генерирования других типов кластеров.

Пример сгенерированного сегмента социальной сети в разрабатываемой компьютерной модели приведен на рис. 9.

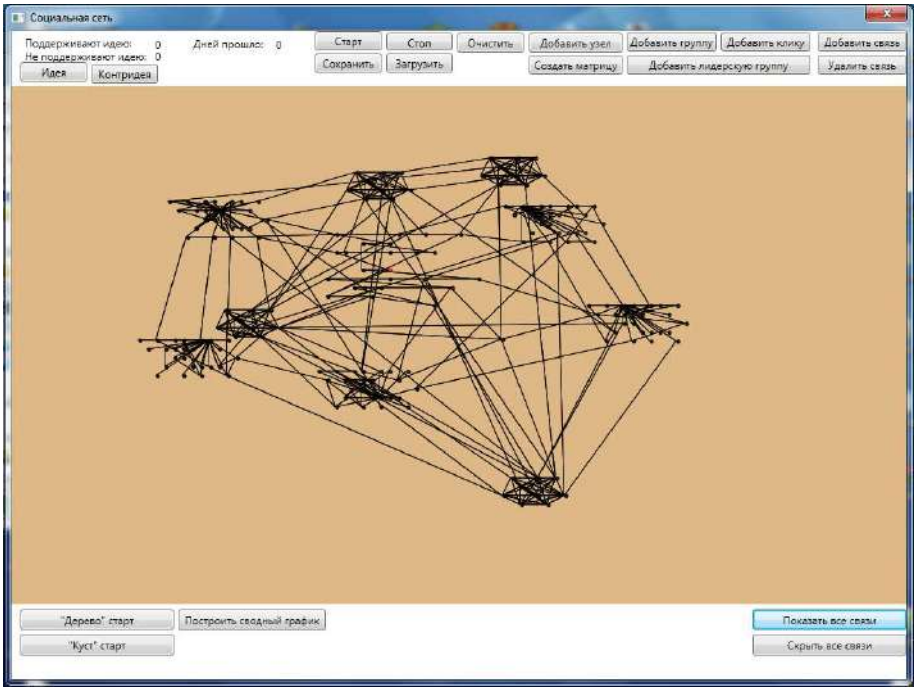

Рис. 9. Пример сегмента сети, сгенерированного в компьютерной модели

Процесс информационного обмена в модели происходит в виде итераций, где каждая отдельно взятая итерация соответствует определенному временному промежутку (например, 1 итерация = 1 день).

Вовлеченность в α-идею отдельного узла определяется аддитивным принципом. Показатель вовлеченности равнен сумме накопленных α-посылов на текущую итерацию:

$$I\alpha v_j = \sum_{m=1}^{x} \sum_{i=1}^{n} k_{ij} * \alpha_i, \tag{8}$$

где $I\alpha v_j$ – уровень вовлеченности j-го узла в α-идею, x – текущая итерация моделирования, n – количество контактов j-го узла, α_i – сообщение от i-го узла, фиксирует наличие сообщения, значение параметра определяется как:

$$\alpha_i = \begin{cases} 1, \ \alpha - \text{сообщение от } V_i \text{ было} \\ 0, \ \alpha - \text{сообщение от } V_i \text{ не было} \end{cases}, \tag{9}$$

где k_{ij} – коэффициент информационного воздействия, определяется соотношением:

$$k_{ij} = \frac{Rv_i}{Op\alpha v_j}, \tag{10}$$

где Rv_i – репутация узла V_i, $Op\alpha v_j$ – уровень недоверия j-го узла к α-идеи.

Поведение и вовлеченность к идее определяется параметром $I\alpha v_j$, при превышении определенного порогового значения узел считается вовлеченным в идею. Этим разрабатываемая модель похожа на пороговые модели. Классические пороговые модели рассматривают линейную функцию накопления воздействия.

Так как уровень доверия (недоверия) в модели уже закреплен к конкретной идеи, то информационный вес узла (ИВ) предлагается определять, как коэффициент, получаемый по отношению:

$$ИВ = Репутация / Недоверие. \quad (11)$$

В случае наличия в сети распространителей контридеи к α-идеи, необходимо учитывать их влияние, и тогда формула (7) примет вид:

$$I\alpha v_j = \sum_{m=1}^{x}(\sum_{i=1}^{n} k_{ij} * \alpha_i + \sum_{i=1}^{n} k_{ij} * (-\alpha_i)). \quad (12)$$

При наличии распространителей контридеи функция вовлеченности перестает быть монотонной и может убывать в случае, если узел получает сообщения с контридеей. В данном случае также определяется уровень вовлеченности распространителя контридеи – пороговое значение (отрицательное) после которого узел становится контргенератором, распространять контридею узел начинает после снижения значения вовлеченности ниже определенного уровня: $I\alpha v_i < -0.5Ig$.

Для упрощения восприятия результатов, а также их анализа в модель, кроме графического отображения динамики вовлеченности в идею в сети, добавлена возможность получения динамического графика, отражающего количество вовлеченных в идею узлов на каждой итерации. График позволяет сравнивать скорость роста вовлеченности, для сравнения эффективности разных стратегий распространения информации. На рисунке 10 представлены структура сегмента социальной сети и график количества вовлеченных в α-идею узлов во времени.

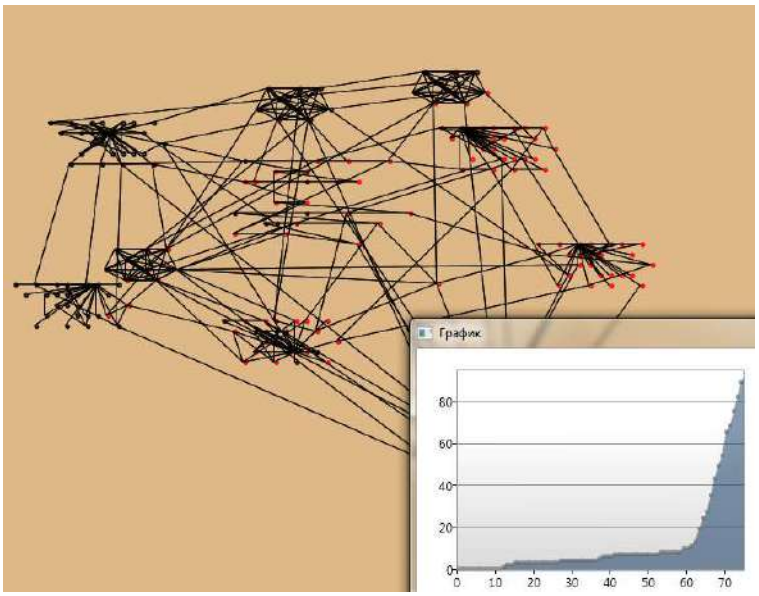

Рис. 10. Графическое отображение состояния социальной сети на *i*-й итерации модели

На разработанной компьютерной модели можно проводить моделирование процессов распространения информации и информационных воздействий с применением различных стратегий субъектов распространения информации [15].

ВЫВОДЫ

В этой работе проведено исследование существующих методов моделирования структуры социальных сетей и их сегментов. Разработан метод компьютерного моделирования сегмента социальной сети для исследования распространения информационных воздействий. Реализована компьютерная модель для генерирования сегмента социальной сети, в которой можно проводить эксперименты для исследования различных стратегий распространения информационных воздействий.

СПИСОК ЛИТЕРАТУРЫ

[1] Гусарова, Н.Ф. (2016) “Анализ социальных сетей. Основные понятия и метрики”, *СПб: Университет ИТМО,* 67 стр.

[2] Батура, Т.В. (2013) “Модели и методы анализа компьютерных социальных сетей”, *Программные продукты и системы, №3,* URL: https://cyberleninka.ru/article/n/modeli-i-metody-analiza-kompyuternyh-sotsialnyh-setey

[3] Чураков, А.Н. (2001) “Анализ социальных сетей”, *Социологические исследования, №1,* С. 109-121.

[4] Кочкаров, А.А, Сенникова, Л.И.,. Кочкаров, Р.А (2015) “Некоторые особенности применения динамических графов для конструирования алгоритмов взаимодействия подвижных абонентов”, *Известия ЮФУ. Технические науки, №1(162),* URL: https://cyberleninka.ru/article/n/nekotorye-osobennosti-primeneniya-dinamicheskih-grafov-dlya-konstruirovaniya-algoritmov-vzaimodeystviya-podvizhnyh-abonentov

[5] Губанов, Д.А., Новиков, Д.А., Чхартишвили, А.Г. (2010), “Социальные сети: модели информационного влияния, управления и противоборства – Второе издание”, *Москва: Издательство физико-математической литературы,* 228 стр.

[6] Haidai, B., Artiukh, R., Malyeyeva, O. (2018), “Analysis and modelling the preferences of social networks users”, *Innovative technologies and scientific solutions for industries, No 1 (3),* P. 5-12. DOI: https://doi.org/10.30837/2522-9818.2018.3.005.

[7]Евин, И.А. (2010), “Введение с теорию сложных сетей”, *Компьютерные исследования и моделирование, Том 2, № 2,* С. 121-141.

[8] Меликов, С., Мусатов, Д., Савватеев, А. (2013), “Моделирование социальных сетей”, URL: https://kpfu.ru/docs/F117464271/MMS_socnet_cities.pdf

[9] Сазанов, В.М. (2010), “Социальные сети как новая общественная сфера. Системный анализ и прогноз.”, *Москва, Лаборатория СВМ,* 180 стр.

[10] Hogan, B. (2007), “Analysing social networks via the Internet”, 13 p., URL: https://pdfs.semanticscholar.org/be39/06ca5bfc196581aeaa957cc9287179819bc1.pdf

[11] Seidman, S.B., Foster, B.L. (1978), “A graph-theoretic generalization of the clique concept”, *Journal of Mathematical Sociology*, №6(1), 139–154.

[12] Wellman, B., Hogan, B., Berg, K et al. (2006), “Connected lives: The project”, *The networked neighborhood*, pp. 161–216.

[13] Komusiewicz, C. (2016), “Multivariate algorithmics for finding cohesive subnetworks”, *Jena, a, Germany, Friedrich-Schiller University of Jena, 24 p., URL: https://pdfs.semanticscholar.org/2def/ce3c6f915a4d2bd64412c9a15b4f3bed9f09.pdf*

[14] Тоискин, В.С., Красильников, В.В. (2010) “Классификация социальных сетей интернет как элементов социальных структур”, *Заочные электронные конференции*, URL: www.econf.rae.ru/pdf/2012/10/1688.pdf.

[15] Уличев, А.С., Мелешко, Е.В. (2018), “Программное моделирование распространения информационно-психологических воздействий в виртуальных социальных сетях“, *Харьков: Современные информационные системы, Т.2, №2*, С. 35-39, – URL: http://nbuv.gov.ua/UJRN/adinsys_2018_2_2_8 (на украинском)

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 48 - 52 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

СТЕГАНОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В ФАЙЛАХ ФОРМАТА OFFICE OPEN XML С ПОМОЩЬЮ ЦВЕТОВОЙ МОДЕЛИ RGB

STEGANOGRAPHIC INFORMATION PROTECTION IN OFFICE OPEN XML FORMAT FILES USING RGB COLOR MODEL

Babenko Yuriy, PhD student, Taras Shevchenko National University of Kyiv, Kiev, Ukraine.
Babenko Mykhailo, PhD in Engineering Science, Associate Professor, Dniprovsk State Technical University, Kamyanske, Ukraine.

АННОТАЦИЯ. В данной статье рассмотрены алгоритмические особенности реализации методов текстовой стеганографии для скрытой передачи данных. Представлен алгоритм, основанный на модификации цветовых параметров символов текста, а именно применении метода наименьшего значащего бита к цветовым RGB каналам текстовых символов файла формата Microsoft Office Word с расширением DOCX. Разработано программное обеспечение, реализующее данный алгоритм, с возможностью вложения / извлечения скрытой информации.

КЛЮЧЕВЫЕ СЛОВА: стеганография, формат OFFICE OPEN XML, метод наименьшего значащего бита, цветовая модель RGB

ABSTRACT. This article describes the algorithmic features of the implementation of text steganography methods for hidden data transmission. An algorithm based on a modification of the color parameters of the text characters is presented. The least significant bit method is applied to the RGB color channels of text characters in a Microsoft Office Word file format with the .docx extension. Software implementation of algorithm has been developed. Software can embed / extract hidden information.

KEYWORDS: steganography, OFFICE OPEN XML format, The least significant bit method, RGB color model

Введение. Рассматривая способы защиты информации, наряду с криптографическими методами уместно обратить внимание на стеганографические методы. Сам термин «стеганография» означает скрытое сообщение, которое полностью исключает возможность узнать о его существовании третьему лицу. И если, образно говоря, криптография делает понятное непонятным, то стеганография делает видимое невидимым (иногда и в прямом смысле слова). Достигается это «растворением» скрываемой информации среди других данных значительно большего объема.

Компьютерная стеганография основывается на двух основных принципах [1]. Во-первых, файлы с оцифрованными изображениями, а также аудио- и видеофайлы можно определенной мерой изменить без потери их функциональности. Во-вторых, возможности человека различать незначительные изменения звука или цвета довольно ограниченные. Стеганографические методы дают возможность заменить несущественные части данных нужной информацией. Это означает, что семейное фото может

содержать информацию коммерческого характера, а файл с любимой мелодией – секретное сообщение.

Чаще всего стеганография применяется для создания цифровых водяных знаков, которые, в отличие от обычных, можно проявить, лишь используя необходимое программное обеспечение. Цифровые водяные знаки записываются в виде псевдослучайных последовательностей сигналов шума, которые сгенерированы на базе секретных ключей. Такие знаки обеспечивают аутентичность или неприкосновенность документа, дают возможность идентифицировать владельца или автора, проверить права пользователя или дистрибьютора, даже в том случае, когда файл был обработан.

Существующие алгоритмы встраивания секретной информации разделяют на несколько групп:

1. Те, которые работают с самым цифровым сигналом.
2. «Впаивание» секретной информации. В этом случае происходит наложение изображения, звука или текста, которые необходимо спрятать, сверх оригинала. Довольно часто применяется для встраивания ЦВЗ (цифровой водяной знак).
3. Использование возможностей файловых форматов. Сюда относится вложение информации в метаданные или в другие зарезервированные поля файла, которые обычно не используются.

Контейнером могут служить любые данные (файлы) достаточно большого объема, например графические или звуковые. Их структура проста и, как правило, обладает большой избыточностью, позволяющей вместить значительный объем дополнительной информации. Однако текстовые файлы все же более распространены, и их структура широко известна.

Поскольку мы будем встраивать скрытые данные в текстовый файл, рассмотрим методы, с помощью которых это можно реализовать. Для скрытия конфиденциальных сообщений в тексте (так называемая текстовая стеганография – *text steganography*) используется или обычная избыточность письменной речи, или же форматы представления текста.

Наиболее сложным объектом для скрытия данных по многим причинам является электронная (файловая) версия текста. В отличие от текстового файла его "жесткая" копия (например, бумажная) может быть обработана как высокоструктурированное изображение и поэтому является относительно легко поддающейся разнообразным методам скрытия, таким как незначительные изменения формата текстовых шаблонов, регулирование расстояния между определенными парами символов (кернинг), расстояния между строками и т.п. В значительной степени такая ситуация вызвана относительным дефицитом в текстовом файле избыточной информации, особенно в сравнении с графическими или, например, звуковыми файлами. В то время как в большинстве случаев существует возможность внести незаметные глазу и неощутимые на слух модификации в изображение и звук, даже дополнительная буква или знак пунктуации в тексте могут быть легко распознаны случайным читателем.

Скрытие данных в тексте требует поиска таких модификаций, которые были бы незаметными подавляющему большинству читателей. Обычно рассматривают три группы методов, которые получили наибольшее распространение при встраивании скрываемых данных в текст [2]:

- методы произвольного интервала, которые осуществляют встраивание путем манипуляции с пробельными символами (свободным местом на печатной полосе);
- синтаксические методы;

- лексические методы;
- семантические методы, в основу алгоритмов которых положено манипулирование словами, зависимое от скрываемых бит данных.

Наибольшее распространение получили следующие методы текстовой стеганографии:

1. Метод изменения порядка следования маркеров конца строки CR/LF. Использует индифферентность подавляющего числа средств отображения текстовой информации к порядку следования символов перевода строки (CR) и возврата каретки (LF), ограничивающих строку текста. Традиционный порядок следования CR/LF соответствует 0, а инвертированный LF/CR означает 1.
2. Метод хвостовых пробелов. Предполагает дописывание в конце коротких строк (менее 225 символов; значение 225 выбрано достаточно произвольно) от 0 до 15 пробелов, кодирующих значение полубайта.
3. Метод знаков одинакового начертания. Предполагает подмену (бит 1) или отказ от такой подмены (бит 0) русского символа латинским того же начертания.
4. Изменение количества промежутков. Будем считать, что один промежуток отвечает биту «0», а два – «1». Программа получает любой текст в качестве контейнера и вкладывает в него сообщение, заменяя его биты на соответствующее количество промежутков. Важную роль здесь также играет и способ кодирования символов. Нужно получить код символов оптимальной длины, и чтобы при этом двойной промежуток встречался по возможности меньше раз.
5. Метод изменения межстрочного расстояния, или line-shift coding. В его стандартной реализации предлагается скрывать стегосообщение в изменении высоты межстрочных интервалов.
6. Word-shift coding. Изменяется расстояние между словами текста. Суть метода заключается в том, что берется текст с разными расстояниями между словами. Выделяется максимальное и минимальное расстояние, которые обозначаются соответственно 1 и 0, а другие расстояния увеличивают или уменьшают до размеров выделенных.
7. Feature coding. Внесение специфических изменений в очертания отдельных букв.

Рассмотренные выше методы довольно легко встраиваются в любой текст, независимо от его содержания, назначение и языка. Однако они имеют несколько существенных недостатков: обладают малой пропускной способностью и могут быть выявлены для электронного документа путем изменения параметров размера и начертания шрифта.

Поэтому мы будем использовать другой метод, который имеет название LSB (Least Significant Bit, наименьший значащий бит). Суть заключается в замене наименее значащих бит контейнера на биты сообщения, которое необходимо спрятать [3]. Младший значащий бит несет в себе меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, НЗБ – это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов контейнера битами секретного сообщения. Поскольку возможности человеческого глаза различать оттенки одного и того самого цвета довольно ограниченные, такая замена будет незаметной для человека.

Именно на базе метода LSB и будет реализован алгоритм сокрытия тайной информации в цветовых RGB каналах текстовых символов файла формата Microsoft Office Word с расширением DOCX, которому посвящена эта работа.

Постановка задачи. Разработать программное обеспечение, с помощью которого можно будет спрятать тайную информацию таким образом, чтобы о ее существовании не узнал кто-нибудь другой. Также необходимо обеспечить возможность вытягивания секретного сообщения из контейнера, в котором оно уже скрыто. В качестве контейнера (или хранилища) для тайных данных мы будем использовать файл формата Microsoft Office Word с расширением DOCX. Почему именно DOCX, а не, например, DOC или TXT? На это есть несколько важных причин.

Во-первых, файл с расширением DOCX, в отличие от DOC, представляет собой zip-архив с XML-документами, который можно распаковать и получить всю необходимую информацию: текст, изображения, таблицы и т.п. Благодаря этому довольно легко вкладывать и получать скрытые в нем данные. Формат файла основан на Open XML, подробно описанный в стандарте ECMA-376: Office Open XML File Formats, и использует сжатие по алгоритму ZIP для уменьшения размера файла. Данный архив содержит два типа файлов – файлы формата XML с расширениями xml и rels и медиафайлы, например, изображения. Логически файл состоит из трех видов элементов: типов, частей и связей. Типы – это список сущностей, встречающихся в документе, например, типов медиафайлов или частей документов, части – это отдельные части документа, для каждой части документа создан отдельный файл формата XML. Между частями документа устанавливаются связи. Таким образом, можно сказать, что файл формата docx представляет собой набор сжатых файлов формата XML, причем все текстовое содержимое электронного документа Microsoft Word формата DOCX находится в одном XML файле, а именно в document.xml. Файл document.xml представляет собой XML файл в элементной форме, где каждому элементу обычно соответствует один атрибут.

Во-вторых, DOCX – наиболее популярный и массовый формат, и его частое использование не будет вызвать ни у кого сомнений на предмет вложенных в нем данных, что несомненно является большим плюсом его использования при стеганографической защите.

В-третьих, размер DOCX-файла значительно меньше, чем его аналога с расширением DOC. Особенно это заметно в файлах, которые содержат большое количество изображений или графиков.

Результаты работы. Как было уже сказано раньше, человеческий глаз не в состоянии отличить незначительные оттенки одного и того же цвета. Этим можно удачно воспользоваться при построении алгоритма вложения тайных данных в контейнер. Суть этого алгоритма заключается в следующем. У нас есть сообщения, которое необходимо спрятать в документ с расширением DOCX. При этом сам документ должен уже содержать в себе текстовую информацию. От объема этой информации будет зависеть объем тех данных, которые мы сможем в него вложить. Чем больше текста содержит документ, тем больше данных мы сможем в него спрятать. Тайное сообщение мы будем вкладывать в RGB каналы цвета каждого текстового символа из этого файла. Для этого нам сначала необходимо «разобрать» документ Word, получить из него все необходимые данные: текст и информацию о цветах каждого из символов в формате RGB. Потом полученные составляющие цвета

нужно перевести в двоичную систему счисления и заменить младшие биты составных цвета битами нашего сообщения. Более детально объясним это на примере:

Это 1 байт нашего сообщения:

10 101 010

Это RGB цвета одного символа:

R: 11110**00**

G: 00001**000**

B: 11001**000**

Заменив 2 младших бита в канале R и 3 младших биты в каналах G и B, получим следующий результат:

R: 11110**10**

G: 00001**101**

B: 11001**010**

Данная операция не внесет в цвет заметных человеческому глазу искажений. Вместе с тем она поможет нам вложить ровно 1 байт нашего сообщения в цвет каждого символа входного файла. Т.е. максимальное количество байт (или символов), которые мы можем спрятать, будет равно количеству символов документа с расширением DOCX, включая промежутки, табуляции, символы возврата каретки и абзаца.

Аналогичным образом выполняется и вытягивание данных из контейнера. Для того, чтобы получить сообщение, нужно, как и в первом случае, «разобрать» документ Word, получить цвета текстовых символов в формате RGB и прочитать необходимое количество последних бит каждого канала. Они и будут составлять один байт (или символ) скрытых данных. Проделав эти действия для всех других цветов, мы получим полностью текст секретного сообщения.

Авторами разработано программное обеспечение, которое реализует вышеописанный алгоритм. Также реализован собственный парсер docx-документов, который в отличие от уже существующих, полностью удовлетворяет требованиям задачи и включает в себя лишь необходимые функции, такие как считывание текста с сохранением форматирования, считывание цветов символов, которые используются в файле, и т.п.

Выводы. На базе метода LSB с использованием цветовой модели RGB построен алгоритм вложения скрытых данных в документ Microsoft Word с расширением DOCX.

Разработано программное обеспечение на языке C#, реализующее данный алгоритм, с возможностью вложения/извлечения скрытой информации. Программа функционирует в средах ОС семейства Windows. Для разработки программного обеспечения использовался пакет Microsoft Visual Studio.net 2017.

Результаты, полученные в этой работе, будут полезны в научно-технической сфере и сфере защиты данных.

Список использованной литературы

1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. - М.: «Солон-Пресс», 2009. - 272 с.

2. А Конахович Г.Ф. Компьютерная стеганография. Теория и практика. / Г.Ф.Конахович, А.Ю.Пузыренко. - К.: "Мк-Пресс", 2006. - 288 с.

3. .Домарев В.А. Безопасность информационных технологий. Системный подход / В.В.Домарев . - К.: ООО "ТИД "ДС", 2004 .- 992 с.

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 53 - 66 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ISRAEL CYBER SECURITY SYSTEM

Leri Saraidarov, PhD student of the Faculty of Law
and International Relations of Georgian Technical University.

ABSTRACT. There is no doubt that the national security problems exist in any country, regardless of the governors and regime conditions, however in democratic states, especially for the countries in war situations where, along with others the terrorist threats are increased. Ensuring the security of the country is a priority and it is of particular importance.

In the State of Israel, special attention is paid to information security- one of its key areas and components - cyber security and cyber defense. As you know, in the cybernetic age, with the development and availability of technologies, are increasing the number and extent of threats and challenges.

In Israel, a number of public and private sector agencies and organizations provide reliable and sustainable cyber threats and risks including the special services, police and defense units, as well as highly rated startups and information security companies.

To summarize, it has to be said, the foundation for success is a multitude of highly qualified specialists, years of work experience, innovative approaches, the development of modern technologies and the inevitable dilemma of forming an advanced leader and a protected state.

KEYWORDS: Cyber security, security services, fight cyber threats, startups in cyber security, government agencies.

ისრაელის კიბერუსაფრთხოების სისტემა

ლერი სარაიდაროვი, საქართველოს ტექნიკური უნივერსიტეტის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის დოქტორანტი.

რეზიუმე. უდავოა, რომ ეროვნული უშიშროების უზრუნველყოფის პრობლემა არსებობს ნებისმიერ ქვეყანაში, მიუხედავად მმართველობისა და რეჟიმის პირობებისა, თუმცა დემოკრატიულ სახელმწიფოებში, მით უმეტეს საომარ მდგომარეობაში მყოფ ქვეყნებში, სადაც სხვა საფრთხეებთან ერთად მომეტებულია ასევე ტერორისტული საფრთხეები, ქვეყნის უშიშროების უზრუნველყოფა პრიორიტეტულია და მას ენიჭება განსაკუთრებული მნიშვნელობა.

ისრაელის სახელმწიფოში განსაკუთრებული ყურადღება ეთმობა საინფორმაციო უსაფრთხოებასა და მის ერთ-ერთ მნიშვნელოვან მიმართულებას და კომპონენტს- კიბერუსაფრთხოებას და კიბერთავდაცვას. მოგეხსენებათ, კიბერნეტიკულ ერაში, ტექნოლოგიების

განვითარებასთან და ხელმისაწვდომობასთან ერთად იზრდება საფრთხეებისა და გამოწვევების რაოდენობა და მოცულობა.

ისრაელში კიბერსაფრთხეებთან და რისკებთან საიმედო და მდგრად გამკლავებას უზრუნველყოფს არაერთი სახელმწიფო და კერძო სექტორში მომუშავე სამსახური თუ ორგანიზაცია. მათ შორის სპეცსამსახურების, პოლიციის და თავდაცვის ძალების დანაყოფები, ასევე მაღალრეიტინგული სტარტაპ და საინფორმაციო უსაფრთხოების სფეროში მომსახურე კომპანიები.

შესაჯამებლად უნდა ითქვას, რომ ისრაელის კიბერუსაფრთხოების სფეროში მიღწეული წარმატების საფუძველს წარმოადგენს მაღალკვალიფიციური სპეციალისტების მრავალრცხოვანი შტატი, მრავალწლიანი სამუშაო გამოცდილება, ნოვატორული მიდგომები, თანამედროვე ტექნოლოგიების განვითარება და მოწინავე-ლიდერ და დაცულ სახელმწიფოდ ჩამოყალიბების გაუნელებელი ჟინი.

საკვანძო სიტყვები: კიბერუსაფრთხეობა, სპეცსამსახურები, კიბერსაფრთხეებთან ბრძოლა, სტარტაპი კიბერუსაფრთხოებაში, სახელმწიფო უწყებები.

უდავოა, რომ ეროვნული უშიშროების[1] უზრუნველყოფის პრობლემა არსებობს ნებისმიერ ქვეყანაში, მიუხედავად მმართველობისა და რეჟიმის პირობებისა, თუმცა დემოკრატიულ სახელმწიფოებში, მით უმეტეს საომარ მდგომარეობაში მყოფ ქვეყნებში, სადაც სხვა საფრთხეებთან ერთად მომეტებულია ასევე ტერორისტული საფრთხეები, ქვეყნის უშიშროების უზრუნველყოფა პრიორიტეტულია და მას ენიჭება განსაკუთრებული მნიშვნელობა. ბალანსის დაცვა ქვეყნის უშიშროების ნიშნულსა და დემოკრატიული პრინციპების რეალიზაციის ხელშეწყობას შორის მსგავსი ტიპის ქვეყნებში დიდ სირთულეებთან არის დაკავშირებული.

ზოგადად, ქვეყნის ეროვნული უშიშროების უზრუნველყოფის სისტემა დაფუძნებულია და აერთიანებს სახელმწიფო ორგანოებს, ძალებს-პოტენციალის სახით, სხვადასხვა სახის რესურსებსა და საშუალებებს, რომელთა გამოყენება და ფუნქციონირება ხორციელდება ქვეყანაში მოქმედი და აღიარებული სამართლებრივი აქტების შესაბამისად. სახელმწიფოში უშიშროების პრიორიტეტულ მიმართულებებს წარმოადგენს პიროვნების, საზოგადოების და სახელმწიფოს პოლიტიკური, სამართლებრივი, ორგანიზაციული, ეკონომიკური, სამხედრო და სხვა მსგავსი ხასიათის უსაფრთხოება. სისტემის ძირითად ფუნქციას განეკუთვნება ეროვნული უშიშროების წინაშე მდგარი საფრთხეების თაობაზე ინფორმაციის მოპოვება, შეფასება, იდენტიფიცირება, მათზე რეაგირება, კონკრეტულ მოქმედებათა ორგანიზება, რათა აღმოფხვრილ, ნეიტრალიზებულ და მინიმუმამდე იქნას დაყვანილი საფრთხეებისა და რისკების რაოდენობა [1, 26-35].

[1] ეროვნული უშიშროება-მდგომარეობა, როდესაც ქვეყანაში უზრუნველყოფილია პიროვნების, საზოგადოების და სახელმწიფოს დაცულობა შიდა და გარე საფრთხეებისაგან, ასევე უზრუნველყოფილია კონსტიტუციური უფლებების რეალიზაცია, მოსახლეობის ცხოვრების მაღალი დონე, ქვეყნის სუვერენიტეტი, ტერიტორიული მთლიანობა, მდგრადი განვითარება, სახელმწიფოსა და მოსახლეობის თავდაცვა და უშიშროება.

ცხადია, რომ ისრაელისთვის, მისი ოფიციალურად დამოუკიდებელ სახელმწიფოდ გამოცხადების დღიდან ეროვნული უშიშროების სისტემის სიმტკიცის უზრუნველყოფა წარმოადგენს სახელმწიფო პოლიტიკის პრიორიტეტულ მიმართულებას. ცალკეული ყურადღება ექცევა ეროვნული უშიშროების უზრუნველსაყოფად სპეცსამსახურებისა და სამართალდამცავი ორგანოების მიერ გამოყენებულ საშუალებებს, მეთოდებსა და ინსტრუმენტებს.

„უშიშროების“ ცნებას სამართლებრივ და სამეცნიერო ლიტერატურაში დათმობილი აქვს საკმაოდ ბევრი გამოკვლევა[2], თუმცა მეცნიერებს შორის დღემდე ვერ მოხერხდა საერთო აზრის ფორმირება ამ ფენომენთან მიმართებაში, თუ რა უნდა და რა შეიძლება ჩაითვალოს სახელმწიფო უშიშროების განმსაზღვრელ ფაქტორებად შიდა და საგარეო დონეზე [2,5].

წინამდებარე სტატიაში გვსურს, საუბარი წარვმართოთ საინფორმაციო უსაფრთხოების ერთ-ერთი მთავარი მიმართულების-კიბერუსაფრთხოების აქტუალურ საკითხებზე.

კიბერუსაფრთხოების სფეროს განვითარება ისრაელის სახელმწიფოსთვის განსაკუთრებით პრიორიტეტულია და მნიშვნელოვანი, გამომდინარე იქიდან, რომ იგი წარმოადგენს ყველაზე კომპიუტერიზებულ ქვეყანას ახლო აღმოსავლეთში. მაღალი ტექნოლოგიების წარმატებული ფლობა და მათი განვითარება თავისთავად პირდაპირპროპორციულია ამ სფეროში მოსალოდნელი საფრთხეებისა და რისკების.

ისრაელის სახელმწიფოში განსაკუთრებული ყურადღება ეთმობა საინფორმაციო უსაფრთხოებასა[3] და მის ერთ-ერთ მნიშვნელოვან მიმართულებას და კომპონენტს-

[2] კამათი „უსაფრთხოების“ ცნებასთან დაკავშირებით მომდინარეობის შუა საუკუნეების ხანიდან. მაგალითისთვის იტალიელი ფილოსოფოსი და პოლიტიკური მოღვაწე ნიკოლო მაკიაველი აღნიშნავდა, რომ სახელმწიფოს საფრთხე შესაძლოა შეექმნას ორი მხრიდან-ქვეშევრდომი და სხვა სახელმწიფოთა მხრიდან. მისი აზრით, საგარეო საფრთხეებთან გამკლავება შესაძლებელია ძლიერი არმიისა და თავდადებული ჯარისკაცების ხარჯზე, ამასთან შიდა საფრთხეები თავისთავად უვნებელყოფდება, ვინაიდან მშვიდობა შენარჩუნებულია ქვეყნის შიგნით. გერმანელი სოციოლოგი და პოლიტოლოგი კარლ დოიჩი უსაფრთხოებას განსაზღვრავდა, როგორც „დაცულობას, ძირითადი სასიცოცხლო ფასეულობების“. ფრანგი სამართალმცოდნე და საზოგადო მოღვაწე ჟორჟ ვედელი იხრებოდა იმ აზრისკენ, რომ უსაფრთხოება არის პრევენციული ღონისძიებების გატარება და საზოგადოების ან ცალკეული ჯგუფების მიმართ არსებული საფრთხეების აღმოფხვრა.

[3] საინფორმაციო უსაფრთხოება-ინფორმაციის, მომსახურებების, სისტემების და ტელეკომუნიკაციების დაცვა ნებისმიერი ფორმით. საინფორმაციო უსაფრთხოება მოიცავს ტექნიკურ უსაფრთხოებას, კერძო პირების ქმედებებს და ორგანიზაციულ პროცედურებს. საინფორმაციო უსაფრთხოების წინააღმდეგ მიმართული საფრთხეები მოიცავს პირადი საიდუმლოებების დარღვევას, ელექტრონულ ფოსტაზე უსარგებლო, რეკლამის მიზნით შეტყობინებების გამოგზავნას, სამრეწველო ჯაშუშობას, პირატულ კოპირებას, კომპიუტერულ ვირუსებს, ქსელურ ტერორიზმს და ელექტრონული ომის წარმოებას. ნებისმიერი ზემოთ ჩამოთვლილი საფრთხე შეიძლება ერთ წამში მთელს მსოფლიოში გავრცელდეს, საინფორმაციო ქსელების გავლით. ინფორმაციულ უსაფრთხოებაში იგულისხმება: ინფორმაციის კონფიდენციალურობის, მთლიანობის (ურღვევობის) და ხელმისაწვდომობის დაცვა.

კიბერუსაფრთხოებას[4] და კიბერთავდაცვას[5]. თვალნათელია, რომ კიბერნეტიკულ ეპოქაში, ტექნოლოგიების განვითარებასთან და ხელმისაწვდომობასთან ერთად იზრდება საფრთხეებისა და გამოწვევების რაოდენობა და მოცულობა. ტექნოლოგიებისა და ინფრასტუქტურის მოხერხებულ და კომფორტულ გამოყენებასთან ერთად იქმნება საკუთარი სისტემისა და კრიტიკული ინფორმაციული[6] მოწყობილობებისა და მატარებლების დაცულობის საშიშროება და პრობლემა, რაც ნებისმიერი ქვეყნისთვის უდავოდ პრიორიტეტულია და საკვანძო.

ისრაელი მსოფლიოში წარმოადგენს ერთ-ერთ წამყვან ქვეყანას, რომელსაც სოლიდური ინვესტირება უწევს კიბერ უსაფრთხოების სფეროში. სტარტაპ[7]-კომპანიების რეკორდული რაოდენობა, მოწინავე კიბერ არმია და განათლების სისტემის პროგრესირება, ამ ყველაფერმა ისრაელს, ხელი შეუწყო ინოვაციების ცენტრად ჩამოყალიბებაში და სახელმწიფო კიბერ სივრცის დაცულობის სფეროში წარმატების მიღწევაში.

ჯერ კიდევ 2002 წელს, კიბერ სივრცეში აქტიური დივერსიების დაწყებამდე, ისრაელის სახელმწიფომ მკაფიოდ განსაზღვრა ქვეყნისთვის პრიორიტეტული ინფორმაციული

---

[4] კიბერუსაფრთხოება (ინგლ. *Cybersecurity)* გაცილებით ფართო ცნებაა და მოიცავს კიბერთავდაცვასაც, იგი არა მარტო სახელმწიფო ქსელებისა და ინფრასტრუქტურის დაცულობასა და უსაფრთხოებას გულისხმობს, არამედ კერძო პირებისა და სექტორების მფლობელობასა და სარგებლობაში არსებული კიბერმოწყობილობების უსაფრთხოებას. ნებისმიერი არასანქცირებული მოქმედება კიბერსივრცეში შეიძლება მიჩნეულ იქნეს კიბერუსაფრთხოების საპირისპირო პროცედურად. კიბერუსაფრთხოება, როგორც ინფორმაციული უსაფრთხოების ერთ-ერთი მიმართულება, ძირითადად უკავშირდება ქსელებისა და პროგრამული უზრუნველყოფის თავდაცვითი და პრევენციული ღონისძიებების გატარებას, რათა თავიდან იქნეს აცილებული ან აღკვეთილი მიმდინარე კიბერაგრესია. ნებისმიერი თავდასხმა კიბერსივრცეში უკავშირდება კონფიდენციალურ ინფორმაციაზე ხელმისაწვდომობის მიღებას, მის დამახინჯებას, შეცვლას ან განადგურებას, ასევე მოპოვებული ინფორმაციის სანაცვლოდ ფულის გამოძალვას. კიბერუსაფრთხოება ასევე ითვალისწინებს კიბერჰიგიენას, სისტემაში შესასვლელი პაროლებისა და სხვა პირადი ინფორმაციების დაცულობას, პლასტიკური ბარათების და სხვა ფულად საკრედიტო ინფორმაციების დაცულობასა და გაუხმაურებლობას, უსაფრთხოების პოლიტიკის დაგეგმვასა და გატარებას.

[5] კიბერთავდაცვა-(ინგლ. *Cyberwarfare)* ჩრდილო-ატლანტიკური ხელშეკრულების ორგანიზაციამ ტერმინი „კიბერუსაფრთხოება“ შეცვალა ტერმინით „კიბერთავდაცვა“, რაც შესაძლოა, უკავშირდებოდეს ვაშინგტონის (ჩრდილო-ატლანტიკური ხელშეკრულება, ვაშინგტონი, კოლუმბიის ოლქი - 4 აპრილი, 1949 წ.) შეთანხმების მე-5 მუხლის ამოქმედებას, რომელიც ითვალისწინებს აგრესიის გამომვლენი სახელმწიფოს მიმართ ფიზიკური ძალის გამოყენების შესაძლებლობას [12]. ხშირად კიბერთავდაცვას-კიბერწინააღმდეგობასაც უწოდებენ, კიბერომს, წინააღმდეგობის გაწევას კიბერნეტიკულ სივრცეში, ინტერნეტ სივრცეში კომპიუტერული წინააღმდეგობის გაწევა. საინფორმაციო ომის ერთ-ერთი სახეობა. მიმართულია კომპიუტერული სისტემების დესტაბილიზაციისკენ და წვდომის მისაღებად სახელმწიფო დაწესებულებების, ფინანსური და საქმიანი ცენტრების ქსელებზე და დაცულ ინფრასტრუქტურაზე, უწესრიგობისა და ქაოსის გამოსაწვევად ქვეყანაში, რომელსაც ინტერნეტზე და კიბერსივრცეზე მინდობილი აქვთ ყოველდღიური ცხოვრება და საქმიანობა. კიბერწინააღმდეგობა შეიძლება გამოიხატებოდეს ვანდალიზმში, პროპაგანდაში, ჯაშუშობაში, უშუალო თავდასხმებში კომპიუტერულ სისტემებსა და სერვერებზე.

[6] კრიტიკული ინფრასტრუქტურა-იურიდიული პირების, სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის.

[7] სტარტაპი-არის დროებითი ორგანიზაცია, რომელიც ეძებს მაღალი მოგების პოტენციალის მქონე ბიზნეს მოდელს და აქვს ექსპონენტური ზრდის პოტენციალი.

უსაფრთხოებისა და დაცულობის საკითხი და მისი უზრუნველყოფა ეროვნულ დონეზე დაავალა შიდა უშიშროების სამსახურს „შაბაქს[8]“ (შინ-ბეთს). გადაწყვეტილება გამოდგა შედეგიანი, მისი რეალიზების შემდეგ ისრაელის კრიტიკული ინფრასტრუქტურა ანგარიშგასაწევ თავდასხმას აღარ დაქვემდებარებია, მიუხედავად ყოველდღიური უმნიშვნელო კიბერ შეტევებისა, რომელთა ინტენსივობა უშედეგობის გამო იყო მზარდი [3, 22-34].

დღევანდელი მდგომარეობით ქვეყნის კიბერ უსაფრთხოებაზე პასუხისმგებლობა აღებული აქვს ისრაელის ეროვნულ კიბერ-დირექტორატს (INCD[9]), რომელიც აერთიანებს წარსულში კიბერ უსაფრთხოებისა და ტექნოლოგიური დაცვის სფეროებში ცალ-ცალკე მოქმედ ორ (INCB[10] და NCSA[11]) სამთავრობო დაწესებულებას. მიუხედავად კომპეტენციების გამიჯვნისა, ინფორმაციული უსაფრთხოების უზრუნველყოფის ვალდებულება შეინარჩუნა „შაბაქმაც“.

2010 წელს ისრაელის პრემიერ-მინისტრმა, ქვეყანის რეალური საფრთხეების წინაშე აღმოჩენის შემდეგ, შექმნა სპეციალური ჯგუფი, „კიბერ ინიციატივის“ სახელით ცნობილი, რომელსაც დაევალა ეროვნული კიბერ პროგრამის შემუშავება. ჯგუფის მიერ შემუშავებული რეკომენდაციების მიხედვით, სასურველი გახდა შექმნილიყო ეროვნული კიბერ ბიურო და სამოქალაქო სექტორის უსაფრთხოების აღმასრულებელი ორგანო [4, 47-53].

2011 წელს ისრაელის მთავრობის დადგენილების შესაბამისად, ეროვნულ დონეზე სამოქალაქო კიბერუსაფრთხეობის განმტკიცების მიზნით შეიქმნა ისრაელის ეროვნული კიბერ ბიურო (INCB). მის კომპეტენციაში შევიდა ქვეყნის პრემიერ-მინისტრისთვის და მთავრობის შემადგენლობაში შემავალი სხვა სამინისტროებისთვის კონსულტაციების გაწევა და დახმარების აღმოჩენა ხსენებულ სფეროში. აღნიშნულ ორგანოს დავალებული ჰქონდა ეროვნული კიბერუსაფრთხოების პოლიტიკის გატარება ქვეყნის მთელ ტერიტორიაზე. კიბერთავდასხმების აცილებისა და განეიტრალების მიზნით ბიუროს ასევე უნდა ეზრუნა ნაციონალური ინფრასტუქტურის გაუმჯობესებაზე და მათი დაცულობის ამაღლებაზე, რათა უზუნველყოფილიყო ნორმალური და უსაფრთხო ცხოვრება ისრაელის სახელმწიფოში. ამავდოულად ბიუროს ამოცანათა რიგს განეკუთვნებოდა თავდაცვითი ღონისძიებების განვითარება და ეროვნული

[8] შაბაქი-იგივე შინ-ბეთ (ივრთ. שב"כ - שירות הביטחון הכלל -შირუთ ხა ბითახონ ხა კლალი)-ქვეყნის პრემიერ-მინისტრის დაქვემდებარებაში არსებული უსაფრთხოების სპეციალური სამსახური, შიდა უსაფრთხოების უზრუნველმყოფი, სამსახურის ერთ-ერთი მიმართულებაა კონტრდაზვერვითი საქმიანობა.

[9] INCD-Israel National Cyber Directorate-ისრაელის ეროვნული კიბერდირექტორატი, ქვეყნის პრემიერ-მინისტრის კანცელარიის მმართველობაში შემავალი ორი ორგანოს გაერთიანების შედეგად 2018 წელს შექმნილი სამსახური, რომელიც უზრუნველყოფს სახელმწიფო და კერძო სტრუქტურებში კიბერუსაფრთხოების პოლიტიკის რეალიზაციას და დაცვას.

[10] INCB-Israel National Cyber Bureau-ისრაელის ეროვნული კიბერბიურო, 2018 წლამდე მოქმედი ორგანო, შეუერთდა NCSA-ს, შედეგად შეიქმნა INCD.

[11] NCSA- National Cyber Security Authority-ეროვნული კიბერუსაფრთხოების ორგანო, ისრაელის პრემიერ-მინისტრის კაბინეტს დაქვემდებარებული ორგანო 2016-2018 წლებში, რომელიც უზრუნველყოფდა ქვეყნის სამოქალაქო კიბერსივრცის დაცვას. 2017 წლის დასასრულს ორგანო გაუერთიანდა NCSA-ს, რომელიც ასევე მოქცეული იყო პრემიერ-მინისტრის კანცელარიის მმართველობის ქვეშ და შეიქმნა ერთიანი ეროვნული კიბერბიურო. ბიურომ აიღო ქვეყნის პრემიერ-მინისტრის საკონსულტაციო ვალდებულება კიბერპოლიტიკის საკითხებში.

ძალისხმევის გაძლიერება კიბერნეტიკული მიმართულებით, საბოლოო ჯამში კი ისრაელის კიბერუსაფრთხოების სფეროში ლიდერ სახელმწიფოდ გადაქცევის ხელშეწყობა.

2015 წლის თებერვალში INCB მოახდინა გარღვევა, კერძოდ, შეიმუშავა მთავრობის ორი დადგენილება (N2443 და N2444) კიბერუსაფრთხეობის სფეროში და შექმნა საფუძველი ეროვნული კიბერუსაფრთხეობის სტრატეგიის მნიშვნელოვანი ელემენტების რეალიზაციის. ასევე, ერთ-ერთი ამ დაგენილების საფუძველზე შეიქმნა კიბერუსაფრთხეობის სფეროში, ეროვნულ დონეზე მომუშავე მეორე ორგანიზაცია (NCSA) [4, 59-64].

NCSA-ს პასუხისმგებლობა აღებული ჰქონდა ქვეყნის კიბერსივრცის დაცვაზე, ყველა ოპერატიულ-დაცვითი ღონისძიებების რეალიზაციისა და ექსპლუატაციის საფუძველზე, რათა ეროვნულ დონეზე განხორციელებულიყო სრული და უწყვეტი რეაგირება კიბერშეტევებთან მიმართებაში. გარდა სხვა დაკისრებული ამოცანებისა, ორგანოს თავისი ქოლგის ქვეშ მოქცეული ჰქონდა ისრაელის სერტი (IL-SERT), ასევე მის კომპეტენციას განეკუთვნებოდა ქვეყნის კიბერთავდასხმებთან მედეგობისა და მათთან გამკლავების მზაობის გაზრდაზე ზრუნვა.

IL-CERT[12]-მა (ისრაელის კომპიუტერულ შემთხვევებზე რეაგირების ჯგუფი), სხვა ქვეყნების ანალოგიური დანაყოფების მსგავსად, პასუხისმგებლობა აიღო ეროვნული კიბერუსაფრთხეობის სფეროში ინციდენტების მართვასა და მოქმედებათა კოორდინაციაზე, პროაქტიულ და პრევენციულ ღონისძიებებზე მათ წარმოშობამდე, ინფორმაციის გაცვლასა და საზოგადოების ინფორმირებაზე ინფორმაციის უსაფრთხოებისა და კონფიდენციალურობის დაცვის სფეროში. ჯგუფი ახორციელებს მსგავსი ღონიძიებების გამოკვლევას, მათ შეფასებას, ასევე საზოგადოებისთვის პერიოდულად აქვეყნებს ინფორმაციას, თუ რა ხერხებითა და მეთოდებით, დაცვის რომელი საშუალებებით არის შესაძლებელი მოსალოდნელ საფრთხეებთან და ინციდენტებთან გამკლავება და თავიდან აცილება [13].

რაც შეეხება ეროვნული კიბერუსაფრთხოების დირექტორატს (INCD), იგი უშუალოდ ფუნქციონირებს და მოქმედებს პრემიერ-მინისტრის ხელმძღვანელობის ქვეშ და წარმოადგენს უსაფრთხოების ოპერატიულ, არასაიდუმლო ორგანოს, რომელსაც დავალებული აქვს ისრაელის სამოქალაქო კიბერსივრცის მონიტორიგი სხვადასხვა ინსტუმენტებისა და საშუალებების დახმარებით, რათა უზრუნველყოფილ იქნას სრულყოფილი და საიმედო დაცვა. ისრაელის სამხედრო ძალები, სპეციალური სამსახურებისა და დანაყოფების ფუნქციონირების საფუძველზე პასუხისმგებლობას იზიარებენ სამხედრო კიბერსექტორში ინფორმაციის და ინფრასტუქტურის დაცულობასთან დაკავშირებით. მათთან ერთად კოორდინირებულ საქმიანობას ეწევიან ისრაელის სხვადასხვა სახელმწიფო სამსახურები, მათ შორის უშიშროების სააგენტო, რომელიც ორიენტირებულია ტერორისტული და კიბერტერორისტული საფრთხეების განეიტრალებაზე, პოლიცია, რომელიც აწარმოებს ბრძოლა კიბერდანაშაულთან წინააღმდეგ [4, 70].

ხსენებული უწყებებისა და სამსახურების კოორდინირებული მუშაობა გარკვეულ ასპექტებში იძლევა ეროვნული ძალისხმევის წარმატებული სინქრონიზაციის საშუალებას კიბერ უსაფრთხეობისა და კიბერსივრცის დაცულობის სფეროში, რაც ქვეყნისთვის ძალიან მნიშვნელოვანია.

[12] **I**srael'S **C**omputer **E**mergency **R**esponse **T**EAM-ისრაელის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი. https://il-cert.org.il/. დღეს უკვე დამოუკიდებელი პროფესიული ორგანიზაცია.

უნდა აღინიშნოს, რომ გარდა სახელმწიფო უწყებებისა, ისრაელის კიბერსივრცის დაცვაში მონაწილეობას იღებენ ისრაელში ოპერირებადი კომპანიებიც, მათ შორის ცნობილი კომპანია „რაფაელი“[13]. „რაფაელი“, როგორც კიბერუსაფრთხოების ერთ-ერთი წამყვანი და თანამედროვე ცენტრის მფლობელი, გარდა სამხედრო მრეწველობისა, წარმოადგენს ისრაელის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფის მთავარ ქვეკონტრაქტორს [19]. ჯგუფის საქმიანობას ისრაელის სახელმწიფოში დიდი ხნის ისტორია არა აქვს, თუმცა, გამოცდილების სიმწირის მიუხედავად იგი უკვე წარმოადგენს გიგანტურ სამთავრობო ცენტრს კიბერუსაფრთხეობის სფეროში მძლავრი საფრთხეების აღმოჩენის, მონიტორინგისა და გაუვნებელყოფის კუთხით ეროვნულ დონეზე. აქვე უნდა აღინიშნოს, კონცერნი „რაფაელი“ ასევე წარმოადგენს კომპანია „მატრიქსის“[14] ქვეკონტრაქტორს, რომელმაც გაიმარჯვა სახელმწიფო ბანკის მიერ შემუშავებულ კონკურსში ქსელების კიბერუსაფრთხოების უზრუნველყოფის სფეროში. ქსელის დანიშნულებას წარმოადგენს ბანკების მიერ რისკების შეფასებისა და კონკურენციის გაზრდის მიზნით ორგანიზაციებს შორის სამომხმარებლო კრედიტების თაობაზე ერთმანეთის ინფორმირება [5, 50-60].

გარდა კომპანია „რაფაელისა“, კიბერუსაფრთხოების სფეროში საქმიანობით დაკავებულია ისრაელის სტრარტაპ კორპორაცია SCADAfence[15] სკადაფენსი, რომელიც უზრუნველყოფს საერთაშორისო გლობალური ქსელებით[16] მოსარგებლე მრეწველობითა და პროდუქციის წარმოებით დაკავებული კომპანიების კორპორატიული ქსელების პროგრამულ მხარდაჭერას და მათ უსაფრთხოებას. თვალნათელია, რომ თანამედროვე ეპოქაში ხსენებული ტიპის ორგანიზაციების ქსელები უფრო დაუცველები გახდნენ კიბერთავდასხმების მიმართ, რის გამოც SCADAfence-ის მომსახურებით დაინტერესებული კომპანიების რიცხვი დღითიდღე იზრდება. ასეთ კომპანიებს ძირითადად წარმოადგენენ სოლიდური საავტომობილო, ფარმაცევტული, ქიმიური და ენერგეტიკულ სფეროში მომუშავე საწარმოები.

აღნიშვნის ღირსია ასევე ის ფაქტი, რომ 2016 წლის დასაწყისში ისრაელის ეკონომიკისა და მრეწველობის სამინისტროს და კიბერბიუროს ერთობლივი ძალისხმევით ფუნქციონირება დაიწყო პროგრამა KIDMA (ივრთ. კიდმა-აბრევიატურა კიბერუსაფრთხოების სფეროში კვლევების

[13] რაფაელი-Rafael ისრაელის კომპანია, რომელიც აწარმოებს შეიარაღებას, საჰაერო თავდაცვით და რაკეტსაწინააღმდეგო ტექნიკას, ასევე წარმატებით ოპერირებს კიბერუსაფრთხოების სფეროში, არის შეიარაღების მსხვილი ექსპორტიორი. ორგანიზაცია დაარსდა 1948 წელს, თავდაპირველად ეწოდა Hemed. შემდგომში შეიცვალა სახელწოდება Emet. 1958 წელს კომპანიამ ისევ შეიცვალა სახელწოდება და ეწოდა Rafael. კომპანიის ერთ-ერთი წარმატებული პროექტია ჰაერსსაწინააღმდეგო, რაკეტთავდაცვითი კომპლექსი „რკინის გუმბათი“, (ივრთ. კიფათ ბარზელ).

[14] მატრიქსი-ისრაელის წამყვანი კომპანია 2000 წლიდან, რომელის საქმიანობს ტექნოლოგიების დანერგვისა და პროგრამული უზრუნველყოფის სფეროში, გააჩნია სახელმწიფო და კერძო სექტორებთან დიდხნიანი გამოცდილება კიბერუსაფროების პროგრამული პროდუქტების მიწოდებისა და პროგრამული უზრუნველყოფის მიმართულებით. ასევე ფინანსურ და საბანკო სექტორთან წარმატებული ურთიერთობის სოლიდური სტაჟი.

[15] SCADAfence-კიბერუსაფრთხოების ერთადერთი პლატფორმა, რომელიც შექმნილია რთული, მსხვილმასშტაბიანი ქსელების ოპერაციული ტექნოლოგიების უწყვეტი და შეუფერხებელი მუშაობისთვის.

[16] გლობალური ქსელი (WAN – Wide Area Network)- ქსელი, რომელიც აერთიანებს სხვადასხვა ქალაქების, რეგიონების და სახელმწიფოების კომპიუტერებს.

განვითარება) მეორე დონემ[17] [18]. პროგრამის იდეას წარმოადგენდა ის, რომ შენარჩუნებულიყო ისრაელის კიბერუსაფრთხოების სფეროში ლიდერის როლი და საერთაშორისო ბაზარზე აწეული ყოფილიყო კონკურენციის ნიშნული. სწორედ მსგავსი პროგრამების დანერგვისა და განვითარების ხარჯზე აღწევენ ებრაული კომპანიები წარმატებებს საერთაშორისო ინდუსტრიაში[18], რომელთაგან ორი (ForeScout Technologies-IT Security და Ability Inc- Mobile Security) შევიდა NASDAQ (ნასდაქში)[19], რამდენიმემ კი მიიღო ათეულობითი მილიონი დოლარი ინვესტიციის სახით [6, 89-90].

2017 წლის იანვარსა და თებერვალში, ისრაელის ქალაქ თელ-ავივში გაიმართა საერთაშორისო გამოფენა Cybertech 2017, რომელიც ეხებოდა კონკურსს უსაფრთოების სფეროში საუკეთესო სტარტაპის გამოვლენის მიზნით. კონკურსის შედეგად საუკეთესო სტარტაპად დასახელდა ისრაელის ინოვაციური ტექნოლოგია Aperio Systems, რომელსაც გააჩნია შესაძლებლობა მოახდინოს სისტემაში საეჭვო აქტივობის იდენტიფიცირება, ავტომატურად გააგზავნოს შეტყობინება და დამოუკიდებლად მოახდინოს ქმედების კორექტირება მნიშვნელოვან ობიექტებზე ინფრასტუქტურის დაზიანების მცდელობის დროს. (იქნება ეს წყალმომარაგების თუ ელექტროქსელების ობიექტი) [4, 66].

ამჟამად გვსურს, საუბარი განვაგრძოთ კიბერ უსაფრთხოების სფეროში მომსახურე სამართალდამცავ უწყებებზე.

2012 წელს ისრაელის პოლიციის სამმართველოში „ლახავი-433[20]“ შეიქმნა კიბერდანაშაულთან ბრძოლის დანაყოფი, რომელსაც ფუნქციურად განესაზღვრა კიბერნეტიკის სფეროში ჩადენილი დანაშაულების გამოძიება. გარდა იმისა, რომ ისრაელი არკეთილმოსურნე ქვეყნების მხრიდან ყოველდღიურად განიცდის კიბერ თუ სხვა სახის აგრესიას, ასევე თვალშისაცემი სიხშირით გამოირჩევა სოციალურ ქსელებსა თუ სხვა მომიჯნავე სფეროებში არაავტორიზებული და უკანონო შეღწევისა და თავდასხმის ფაქტები. ეს შეიძლება იყო პირადი დაცული სივრციდან ინფორმაციისა და ფულადი თანხის მოპარვა, სახელგამტეხი ინფორმაციის გავრცელება, დაშანტაჟება, მუქარა (ბულინგი), ბანკომატებიდან და საბანკო ანგარიშებიდან ფულადი სახსრებისა და პერსონალური ინფორმაციის მართლსაწინააღმდეგო დაუფლება, უკანონო ვაჭრობა ინტერნეტსივრცეში და სხვა. სწორედ მსგავსი დანაშაულების გამოძიება და მათი პრევენცია

[17] 2012 წლიდან ისრაელში ფუნქციონირებს სპეციალური პროგრამა KIDMA, რომელიც საბიუჯეტო დაფინანსებაზე მყოფ კომპანიებს კიბერპროდუქტის შექმნაში სთავაზობს მომსახურებას აღნიშნულ სფეროში. პროგრამა 3 წელიწადში ერთხელ იღებს ფინანსურ მხარდაჭერას 26 მლნ. აშშ დოლარის ოდენობით.

[18] ბრიუს ოსტის (NASDAQ-ის ხელმძღვანელის მოადგილე) განცხადებით, მაღალი ტექნოლოგიების ყოველი მე-5 კომპანია, რომელიც მონაწილეობს ფასთა კოტირებაში ნიუ-იორკის ბირჟაზე-NASDAQ, არის ისრაელის მოქმედი ან ყოფილი კომპანია. ბირჟაზე მონაწილე ებრაულ კომპანიათაგან-80 არის სახელმწიფო [17].

[19] ნასდაქი-(NASDAQ, მომდინარეობს აკრონიმიდან National Association of Securities Dealers Automated Quotations — ფასიან ქაღალდთა დილერების ავტომატური კოტირებების ეროვნული ასოციაცია) — აშშ-ის ელექტრონული სააქციო ბირჟა. დაფუძნდა ფასიან ქაღალდთა დილერების ეროვნული ასოციაციის (NASD) მიერ. კორპორაციის ამჟამინდელი აღმასრულებელი დირექტორია რობერტ გრიფილდი.

[20] ლახავი-443-(იგრთ. ბასრი, მახვილი) יחידת להב 433, (იეხუდათ ლაახავ არბა შალოშ შალოშ)- ისრაელის პოლიციაში 2008 წელს შეიქმნილი სპეციალური დანაყოფი, რომელშიც გაერთიანდა 5 სამართალდამცავი ორგანო. დანაყოფის კომპეტენციას განეკუთვნება ნაციონალური მასშტაბის დანაშაულებათა გამოძიება, კერძოდ, კორუფციისა და სხვა განსაკუთრებით მძიმე და მძიმე კატეგორიი დანაშაულებათა გამოძიება.

ევალება პოლიციის აღნიშნულ დანაყოფს, რომელიც სტუქტურულად ექვემდებარება ისრაელის პოლიციის ერთ-ერთ ყველაზე პრესტიჟულ და ავტორიტეტულ სამმართველოს ლახავი 433 [7, 83-87].

პოლიციური დანაყოფის პარალელურად ისრაელის სახელმწიფო პროკურატურაში 2015 წელს გენერალური პროკურორის გადაწყვეტილებით შეიქმნა კიბერდანაშაულთან ბრძოლის განყოფილება, სადაც კონცენტრირებულ იქნა კიბერდანაშაულთან და კიბერტერორიზმთან გამკლავებისთვის და ბრძოლისთვის აუცილებელი ყველა საშუალება და ძალისხმევა. დასახელებული დანაყოფის შექმნის გადაწყვეტილება მიღებულ იქნა კიბერდირექტორატთან კონსულტაციის საფუძველზე, რა დროსაც გამოიკვეთა მისი არსებობის აუცილებლობა. სამსახურის პროფილურ საქმიანობას განეკუთვნება: კიბერდანაშაულის და რადიოელექტრონული დაზვერვის (SIGINT) [21] სფერო, ციფრული მტკიცებულებების მოპოვება, მიყურადება და კავშირგაბმულობის არხებიდან მონაცემების მოპოვება. პროკურატურის ახლად შექმნილი დანაყოფი საპროცესო ზედამხედველობას უწევს პოლიციის კიბერდანაშაულთან ბრძოლის სამსახურის და იუსტიციის სამინისტროს ტექნოლოგიებისა და ინფორმაციების საქმეთა სამმართველოს წარმოებაში არსებულ საქმეებს [8-25].

გარდა დასახელებული უწყებებისა და კომპანიებისა, კიბერსაფრთხეებთან ბრძოლის სოლიდური გამოცდილება გააჩნიათ სამხედრო სექტორს დაქვემდებარებულ და სპეციალური დანიშნულების მქონე სამსახურებს.

ისრაელის თავდაცვის არმიის გენერალური შტაბის სტრუქტურულ ქვედანაყოფს წარმოადგენს სამხედრო დაზვერვის სამმართველო „ამანი“[22], რომელიც დაკავებულია საგარეო დაზვერვის წარმოებით, იგი „შაბაქთან“ და „მოსადთან[23]“ ერთად შედის ისრაელის ძირითად სპეცსამსახურთა სამეულში. სწორედ მის დაქვემდებარებაშია რადიოელექტრონული დაზვერვის დანაყოფი 8200 (ივრთ. იეხიდა შმონა მათაიმ, 8200 יחידה) [14], რომელიც დაკავებულია რადიოელქტრონული ინფორმაციის შეგროვებითა და დეშიფრაციით, ასევე სხვა ოპერაციებით. დასახელებულ დანაყოფს, გარდა დაზვერვის მნიშვნელოვანი ფუნქციისა, დავალებული აქვს კიბერუსაფრთხოების უზრუნველყოფა რადიოელექტრონულ სასიგნალო დონეზე [9, 63; 10, 50].

სამხედრო სექტორში, კიბერუსაფრთხოების უზრუნველყოფას, გარდა ხსენებული დანაყოფისა, ახორციელებს ისრაელის თავდაცვის არმიის სახმელეთო ჯარების ზროა ხა იაბაშა) შემადგენლობაში 2017 წელს შექმნილი კიბერთავდაცვის მიმართულება ანაფ საიბერ . ახალი მიმართულება ექვემდებარება სახმელეთო ჯარების კავშირგაბმულობის შტაბს მახლექეთ ტიკშუვ).

---

[21] Sigint-signal intelligence-რადიოელექტრონული დაზვერვა-სადაზვერვო საქმიანობის ერთ-ერთი მიმართულება, შესაბამისი ტექნოლოგიების გამოყენებით მიწოდებული სიგნალების გადაჭერა და მოპოვებული ინფრომაციის ანალიზი. რადიოელექტრონული დაზვერვა მოიცავს რადიო (comint), რადიოტექნიკურ (elint), რადიოლოკაციურ (radint) დაზვერვას.

[22] ამანი-(ივრთ. אמ"ן ივრთ-დან המודיעין חגא אגאפ ხა მოადინ — დაზვერვის სამმართველო), ისრაელის თავდაცვის არმიის გენერალური შტაბის სტრუქტურული ქვედანაყოფი.

[23] მოსადი-(ივრთ. ჰამოსად ლემოდიინ ულეთაფკიდიმ მეიუხადიმ, დაზვერვისა და სპეციალური დანიშნულების ორგანო). ისრაელის სადაზვერვო სამსახური, დაკავებულია საგარეო სადაზვერვო საქმიანობით, წარმოადგენს ერთ-ერთ წარმატებულ სპეცსამსახურს მსოფლიოში.

აღნიშნულ მიმართულებას აქვს სხვა დასახელებაც: „ანაფ სევერ“ სევერ-სვივათ რეშეთ საიბერ (ანუ ქსელური სივრცე, ინგლისურენოვანი სიტყვა „საიბერის“ ივრითიზაცია.) ახალი სამსახურის ამოცანას წარმოადგენს ყველა სახეობის შეირაღების და სახმელეთო ჯარების სამხედრო ტექნიკის დაცვის უზრუველყოფა თავდასხმისგან და მათზე კონტროლის მოპოვებისგან. დანაყოფს დაევალა არა მარტო სარგებლობაში არსებული სისტემების დაცვა, არამედ შემუშავებისა და საგამოცდო ეტაპზე არსებული სისტემებისა და ტექნიკის დაცვაც. მიმართულება შედგება რამდენიმე სექტორისგან: მათ შორის (მადორი), რომელიც პასუხისმგებელია დაცვითი საშუალებების შექმნაზე, მათ საბრძოლო ტექნიკაში დანერგვაზე, მიმართულება კომპლექტდება გენერალური შტაბის კავშირგაბმულობის მთავარი სამმართველოს (ანაფ ხა ტიკშუვ) შემადგენლობიდან. გარდა მოხსენიებული მიმართულებისა, ახლადშექმნილი სამსახურის შემადგენლობაში სამმართველოების სახით შედის სისტემების დაცვის (ხატივათ ხა-ხაგანა), კიბერუსაფრთხოების (ხატივათ ხა საიბერ) და კომპიუტერული ქვედანაყოფების (მაარახ ხა-მიხშუვ) მიმართულებები [4, 43].

ალბათ, სიახლეს არ წარმოადგენს, რომ ისრაელის სპეცსამსახურები ითვლებიან ერთ-ერთ ყველაზე ეფექტურ და ეფექტიან სამსახურებად მსოფლიოში. ინტერნეტის განვითარებასთან ერთად, მათი საქმიანობის სფეროს დაემატა კიბერუსაფრთხოების უზრუნველყოფა. როგორც უკვე აღვნიშნეთ, კიბერნეტიკული განყოფილება „შაბაქში“ შეიქმნა საუკუნის დასაწყისში, თავიდან მის ამოცანას წარმოადგენდა ისრაელის ქსელების გამოყენებით ინფორმაციის უსაფრთხო და საიმედო გადაცემა. თუმცა კომპიუტერიზაციის სწრაფმა განვითარებამ, ვირტუალური სივრცის ტოტალურმა გაფართოებამ გამოიწვია მასშტაბური, სტრუქტურული ცვლილებების საჭიროება.

კიბერინდუსტრიასა და კიბერუსაფრთხოებაში მოწინავე ქვეყნის ადგილის დაკავება უდავოდ დიდ ძალისხმევასთან და ინტელექტუალური და ეკონომიკური რესურსების მოხმარებასთან არის დაკავშირებული. ხშირად პროფესიონალიზმი და წარმატებულობა ხდება ნეგატიური ეჭვის საბაბი. ისრაელის შემთხვევაში სახელმწიფო, რომელიც წარმატებულად ფლობს თანამედროვე მაღალ ტექნოლოგიებს და თავად ეწევა მათ ინდუსტრიას, მიიჩნევა საფრთხის წარმომშობ ქვეყნად. ისრაელი არაერთხელ იქნა დადანაშაულებული კიბერთავდასხმების განხორციელებაში, მაშინ, როდესაც იგი თავად არის არაკეთილმოსურნე ქვეყნების მხრიდან სისტემატიური თავდასხმებისა და აგრესიის მსხვერპლი.

2011 წელს თეირანმა ისრაელი დაადანაშაულა ზღვის ფსკერის საბურღი დანადგარებისა და მოწყობილობების მწყობრიდან გამოყვანის მიზნით კიბერთავდასხმაში. ისრაელი, სხვა ქვეყნებთან ერთად მიეკუთვნება იმ სახელმწიფოთა რიცხვს, რომელიც ეჭვმიტანილია ირანის ბირთვული პროგრამის მიმართ კიბერაგრესიისა და თავდასხმების განხორციელებაში. დადანაშაულების საფუძვლად მიიჩნეულია ის ფაქტი, რომ ჩვეულებრივი სამხედრო შეტევების განხორციელება რთულია პოლიტიკური მიზეზების გამო, ამიტომ ისინი მიმართავენ კიბერშეტევებს [15].

აღნიშნულ ბრალდებას წინ უსწრებდა 2010 წელს კიბერსივრცეში ახალი ვირუსის „სტაქსნეტის“ (STAXNET) გამოჩენა, რომლის ავტორობაში ამერიკის შეერთებულ შტატებთან ერთად სახელდებოდა ისრაელი. ვირუსმა უზარმაზარი საფრთხე შეუქმნა ბირთვულ და ინდუსტრიულ ობიექტებს. გავრცელებული ცნობების თანახმად „სტაქსნეტი“[24] შეიჭრა ირანის

[24] სტაქსნეტ-კომპიუტერული ვირუსი, რომელიც აზიანებს ოპერაციული სისტემა „ვინდოუსის“ მართვის ქვეშ არსებულ კომპიუტერულ სისტემებს. აღმოჩენილია 2010 წელს, მისი შეღწევა განხორციელდა არამარტო კომპიუტერულ სისტემებში, არამედ სამრეწველო სისტემებში, რომელიც იმართებოდა ავტომატიზირებული პროცესების მეშვეობით.

ბუშერის[25] ბირთვული ელექტროსადგურის საკომპიუტერო სისტემაში და შეაფერხა მისი ნორმალური მუშაობის რეჟიმი.

ისრაელისა და ამერიკის შეერთებული შტატების კოალიცია დასახელდა ასევე 2012 წელს ჩატარებული იმ კვლევის შედეგად, რომელიც უკავშირდებოდა „სტაქსნეტისგან“განსხვავებული, თუმცა გაცილებით მოქნილი ვირუსის „ფლეიმის“ Flame შემუშავებას. იგი, მისი წინამორბედის მსგავსად, მიზნად ისახავდა ირანის ბირთვული პროგრამის ფუნქციონირების შეფერხებას და სისტემიდან ინფორმაციის ხელმისაწვდომობის უზრუნველყოფას [5, 13-25].

უნდა აღინიშნოს, რომ, გარდა ისრაელის მხრიდან აგრესიის მომდინარეობის თაობაზე ბრალდებებისა, თვით ისრაელიც ხშირად დაქვემდებარებია აქტიურ კიბერშეტევებს, მათ შორის პალესტინის მხრიდან, უშუალოდ ღაზას სექტორიდან. „ქსელის ჯიხადისტები“ ცდილობენ, კიბერთავდასხმებით შეაეფერხონ ებრაული მოსახლეობის ნორმალური და სტაბილური ცხოვრება და წარმოშვან შიში, თუმცა ამის საშუალებას არ იძლევიან ებრაული სპეცსამსახურები, რომლებიც მყისიერ და ეფექტიან რეაგირებას ახდენენ აგრესიასთან და აგრესორთან მიმართბაში. სარაკეტო ავიადარტყმებით ისრაელის მხარემ გაუსწორა ანგარიში მიმდინარე წლის მაისში „ხამასის“ დაჯგუფებას, დადგინდა თავდასხმის მომდინარეობის ლოკაცია, რომლის მიმართაც განხორციელდა თავდასხმა. ისრაელის რეაქცია, მიიჩნევა ისტორიაში პირველ ფაქტად, როდესაც ქვეყანამ აქტიური კონფლიქტის დროს ხაკერულ თავდასხმაზე რეაგირება მოახდინა სამხედრო მოქმედებებით [11, 64-67].

ისრაელისთვის, გარდა ღაზას სექტორიდან მომდინარე კიბერსაფრთხეებისა, მნიშვნელოვან გარემოებად მიიჩნევა კიბერაგრესია ირანისა და სხვა არაბული სახელმწიფოების მხრიდან. ამ უკანასკნელთა ხაკერპოტენციალი მიმართულია ისრაელის მიმართ ინტენსიურ კიბერთავდასხმებზე, რათა დაასუსტონ ობიექტი სახელმწიფოს კიბერმედეგობა, შეარყიონ ქვეყნის პოლიტიკური და ეკონომიკური მდგრადობა, ნეგატიური ცვლილებები შეიტანონ მოსახლეობის ყოველდღიურ ცხოვრებაში და გამოიწვიონ მათი დაშინება, რაც საბოლოო ჯამში შექმნის დაუცველობის სინდრომის საფრთხეებს საზოგადოებაში.

თანამედროვე ეპოქაში მარტივ ჭეშმარიტებას წარმოადგენს ის ფაქტი, რომ ქვეყნის სიძლიერე და განვითარება დამოკიდებულია მის უშიშროებასა და დაცულობაზე. ჩვენს შემთხვევაში, ისრაელი, წარმოადგენს სწორედ იმ სახელმწიფოს, რომელისთვისაც უშიშროება და დაცულობა პრირიტეული მიმართულებებია. მის წინაშე მდგარი საფრთხეები და გამოწვევები მართლაც რომ საგულისხმოა და საყურადღებო. არაბული სახელმწიფების არაკეთილგანწყობა და ყოველდღიური აგრესია ისრაელისთვის სოლიდურ თავსატეხს წარმოადგენს. დაპირისპირებულ მხარეებს შორის კონფლიქტი ათული წლებია, რაც გრძელდება, ამ ყველაფერს თანამედროვე ეპოქაში დაემატა კიბერაგრესია და მათი საშუალებებით შპიონაჟი, ინფორმაციის დატაცება, ინფრასტრუქტურის დაზიანება, მოსახლეობის დაშინება, სადაზვერვო ღონისძიებების და ტერორის მეთოდების გამოყენება კიბერსივრცეში. ვინაიდან ისრაელისთვის ეროვნული უშიშროება და თავდაცვა პრიორიტეტულია, ქვეყანა თანამედროვე გამოწვევებსა და საფრთხეებს უმკლავდება მაღალი ტექნოლოგიების გამოყენებით. ისრაელის მოქმედებებზე დაკვირვებით შეგვიძლია, გამოვიცნოთ ქვეყნის წარმატების ფორმულა.

[25] ბუშერი-ქალაქი ირანში, რომლის მახლობლად მდებარეობს ირანის ბირთვული რეაქტორი.

ისრაელის სკოლებში დაწყებით კლასებში სწავლობენ კითხვას, წერას და კოდირებას. ქვეყანაში არსებობს ბაღები, სადაც ასწავლიან კომპიუტერთან და რობოტოტექნიკასთან[26] მუშაობას. მე-4 კლასიდან მოსწავლეები აქტიურად სწავლობენ პროგრამირებას, განსაკუთრებული ნიჭით დაჯილდოებული უფროსკლასელები კი დაშიფრვის ტექნოლოგიას და „შავქუდიან ხაკერობასთან“[27] ბრძოლის მეთოდებს.

ისრაელი მიზანმიმართულად იყენებს არმიას, როგორც საკადრო რეზერვს, რათა უზრუნველყოს კიბერუსაფრთხოების სფერო კვალიფიციური სამუშაო რესურებით. ვინაიდან ქვეყანაში სამხედრო სავალდებულო სამსახური საყოველთაო სახისაა, სამხედრო დაზვერვის სამსახურს საშუალება ეძლევა შეარჩოს სამხედრო მოსამსახურეთაგან ყველაზე წარმატებული ახალგაზრდები. არის შემთხვევები, როდესაც ახალგაზრდები ითხოვენ სამხედრო სამსახურის გადავადებას სპეციალობის მისაღებად. მას შემდეგ, რაც მიიღებენ ტექნიკურ ხარისხს, ირიცხებიან სამხედრო სავალდებულო სამსახურში სპეციალობის მიხედვით, სადაც უწევთ მსახური დაახლოვებით 3-4 წლის განმავლობაში, რომლის პარალელურადაც იმაღლებენ კვალიფიკაციას და იძენენ გამოცდილებას.

რამდენადაც ისრაელის კიბერუსაფრთხეობის ინფრასტრუქტურა წარმოადგენს თვალსაჩინო ლიდერს მსოფლიო ინდუსტრიაში, საერთაშორისო კომპანიები ისწრაფვიან ებრაულ სახელმწიფოსთან თანამშრომლობისკენ. 2016 წელს ისრაელის პრემიერ-მინისტრმა ბენიამინ ნეთანიაჰუმ გაეროს გენერალურ ასამბლეაზე განაცხადა: „ისრაელის მოსახლეობა შეადგენს მსოფლიო მოსახლეობის[28] 1%-ის მეათედს[29] (ანუ საერთო რაოდენობის მეათასედი), მიუხედავად ამისა, ჩვენ შევძელით და წინა წელს მოვიზიდეთ მსოფლიო კერძო ინვესტიციების 20% კიბერუსაფრთხოების სფეროში. მე მსურს, გაიაზროთ ეს რიცხვი. ისრაელის წვლილი კიბერუსაფრთხოებაში სოლიდურია და ანგარიშგასაწევი. ისრაელი წარმოადგენს გლობალურ კიბერძალას. ისრაელს შეუძლია, შემოგთავაზოთ აუცილებელი დახმარება, თუ ხაკერები ორიენტირებულნი იქნებიან თქვენს ბანკებზე, თვითმფრინავებზე, ელექტრო ქსელებსა თუ ნებისმიერ სხვა კავშირში მყოფ ინფრასტუქტურაზე“ [21].

აღნიშნულის გათვალისწინებით, გასაკვირი არ უნდა იყოს, რომ უმსხვილესმა ტრანსნაციონალურმა კორპორაციებმა, მათ შორის Microsoft, Google, Apple, Cisco, IBM, Intel, HP, Siemens, General Electric, Philips Medical, PayPal დააფუძნეს საკუთარი კვლევითი და კიბერნეტიკული განვითარების ცენტრები ისრაელში.

ორგანიზაცია Start-Up Nation Central მონაცემების მიხედვით, 2018 წელს ისრაელის ექსპორტის საერთო მოცულობამ კიბერუსაფრთხოების ინდუსტრიაში შეადგინა 3,8 მლრდ. აშშ დოლარი, აღნიშნული დარგის კომპანიებმა კი მიიღეს ინვესტიცია 815 მლნ. აშშ დოლარის ოდენობით საწარმოო და პირადი კაპიტალის სახით.

---

[26] რობოტოტექნიკა-გამოყენებითი მეცნიერება, რომელიც დაკავებულია ავტომატიზირებული ტექნიკური სისტემების შემუშავებით და მიიჩნევა მნიშვნელოვან ტექნიკურ საფუძვლად წარმოების განსავითარებლად.

[27] შავქუდიანი ხაკინგი-არაეთიკური ხაკინგი-უნებართვო შეღწევა კომპიუტერულ ქსელში, პირადი სარგებლის მიღების, მუქარის ან შანტაჟის მიზნით. ტერმინის ავტორი-რიჩარდ სტოლმენი.

[28] მსოფლიო მოსახლეობის რიცხოვნობა შეადგენს თითქმის 8 მლრდ-ს. 7 763 035 301 ადამიანი. ისრაელის მოსახლეობა 8 670 110. https://countrymeters.info/ru/World#population_2019

[29] 1%-ანუ მე-100.

კვლევითი ცენტრის „Cyber Security Ventures“ მონაცემების მიხედვით, ისრაელის 9 კომპანია შედის ტოპ-100-ულში, მსოფლიოში ყველაზე წარმატებული და შემოსავლიანი კომპანიების რიგებში კიბერუსაფრთხოების სფეროში. მაგალითისთვის კომპანია „Check Point Software“ იკავებს სარეგიტინგო მეოთხე ადგილს საბაზრო ღირებულებით 15 მლრდ. აშშ დოლარით.

ისრაელს, სტარტაპ-ინდუსტრიის წარმატებული განვითარების გამო, უწოდებენ მეორე სილიკონის ველს[30]. სტრატაპების ინდუსტრიაში ერთ-ერთი გამოცდილი და მაღალრეიტინგული ბრენდია „Startup Nation“, უცნაური რეალობაა ის ფაქტი, რომ ისრაელის სამხედრო დაზვერვის დანაყოფს 8200-ს, ეწოდა „საიდუმლო სტარტაპ-მანქანა“. ეს კი გამომდინარე იქიდან, რომ მრავალი ვალმოხდილი სამხედრო, რომელიც მსახურობდა ზემოხსენებულ დანაყოფში, გახდა მაღალანაზღაურებადი სტრატაპების ავტორი.

აღნიშვნის ღირსია ასევე ის ფაქტი, რომ 2018 წლის 30 ნოემბერს, არგენტინაში პირველად გაიმართა G-20[31] ქვეყნების რიგით მე-13 საერთაშორისო სამიტი. არგენტინის თავდაცვის სამინისტროს წარმომადგენლებმა სამიტის გამართვამდე ერთ წლით ადრე ებრაელ კოლეგებთან ხელი მოაწერეს 5 მლნ. დოლარის ღირებულების კონტრაქტს, რომელიც ითვალისწინებდა მომსახურების გაწევას კიბერუსაფრთხეობისა და კიბერდაცვის სფეროში G-20-ის სამიტზე. მომსახურების ფარგლებში გათვალისწინებული იყო ინფორმაციული უსაფრთხოების სფეროში საგანგებო სიტუაციებსა და კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფების ჩანერგვა [16].

საბოლოო ჯამში შეგვიძლია, დადასტურებით ვიმსჯელოთ, რომ ისრაელის კიბერუსაფრთხოების სფეროში მიღწეული წარმატების საფუძველს წარმოადგენს მაღალკავალიფიციური სპეციალისტების მრავალრიცხოვანი შტატი, მრავალწლიანი სამუშაო გამოცდილება, ნოვატორული მიდგომები, თანამედროვე ტექნოლოგიების განვითარება და მოწინავე-ლიდერ და დაცულ სახელმწიფოდ ჩამოყალიბების დაუოკებელი ჟინი.

მუდმივი მისწრაფება თვითგადარჩენისკენ, აქტივიზაციას უწევს ისრაელიანთა ერთადერთ ბუნებრივ რესურსს-მათ ინტელექტს. მათ არ სცხვენიათ შეკითხვების და ექსპერიმენტების, არ ეშინიათ წარუმატებლობის, უბრალოდ ისინი სწრაფად იწყებენ მოქმედებას და არ კარგავენ დროს ფიქრსა და ეჭვებში.

[30] სილიკონის ველი-Silicon Valley (სილიკონის ველი კაჟისგან მიღებული ნაერთის, სილიციუმის გამო ეწოდა, რომელიც მიკროსქემებში ფუძეშრედ გამოიყენება)-მაღალტექნოლოგიური ზონაა, სადაც მაღალტექნოლოგიური ინდუსტრიის ობიექტებია განლაგებული. მის ძირითად ამოცანას მეცნიერული იდეების პრაქტიკაში დანერგვის დროის შემცირება წარმოადგენს. "სილიკონ ველის" მსგავს ზონებს გააჩნიათ სპეციალური ინფრასტრუქტურა: შენობა-ნაგებობები, ტელეკომუნიკაცია, სპეციალური საგადასახადო და საბაჟო შეღავათები და ა.შ."სილიკონის ველის" დედაქალაქად არაოფიციალურად ქალაქ სან-ხოსეს (კალიფორნიის ქალაქი) მოიხსენიებენ.

[31] დიდი ოცეული (ინგლ. Group of Twenty, G-20) საერთაშორისო ფორუმის ფორმატი, როდესაც ერთმანეთს ფინანსთა მინისტრები და ცენტრალური ბანკების ხელმძღვანელები ხვდებიან. 2009 წელს უმაღლეს დონეზე მიღებული გადაწყვეტილების მიხედვით, დიდი ოცეული მსოფლიო ეკონომიკის მთავარი სტრატეგიული ეკონომიკის ფორუმია. დიდი ოდეული აერთიანებს მსოფლიოში ეკონომიკურად წამყვან და სწრაფად განვითარებად ქვეყნებს [20]. https://www.g20.org/index.php/en/g20

გამოყენებული ლიტერატურის ჩამონათვალი

1. გვენეტაძე ეპიფანე. „საერთაშორისო უშიშროების ასპექტები“, თბილისი, 2017 წ.
2. Цитович Я.В., Понятие «национальная безопасность» и особенности ее обеспечения (на примере Государства Израиль) Россия, Москва; 2019 г
3. Казанин М.В., Военный и гражданский аспекты кибербезопасности Израиля. 2018 г.
4. Гельман З. Кибербезопасность по-израильски, Тель-Авив, 2019 г.
5. Диогенес Ю, Озкайя Э: Кибербезопасность. Стратегии атак и обороны. Перевод: Беликов Д. изд. ДМК-Пресс, 2020 г.
6. Демидов О. и Касенова М. Кибербезопасность и управление интернетом: Москва. изд Статут, 2013 г.
7. Север А. «Моссад» и другие спецслужбы Израиля. 2011 г.
8. Седов С. Сионизм: ставка на террор.–изд. Москва, 1984 г.
9. Дегтярев К. Энциклопедия спецслужб. – Москва., 2008 г.
10. Блехман Р. Мосад, Аман, Шабак, или Возмездие по-еврейски Уцененный товар (№1), 2008г.
11. Бирюк В. Секретные операции XX века: Из истории спецслужб. – СПб., 2003 г.

ინტერნეტ რესურსები

12. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=ka
13. https://il-cert.org.il/
14. https://he.wikipedia.org/wiki/%D7%99%D7%97%D7%99%D7%93%D7%94_8200
15. https://www.gov.il/en/departments/news/119en
16. https://www.7kanal.co.il/News/News.aspx/205594
17. https://shofar7.com/2015/05/17/20-%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D0%B9-%D0%BA%D0%BE%D1%82%D0%B8%D1%80%D1%83%D1%8E%D1%89%D0%B8%D1%85%D1%81%D1%8F-%D0%B2-nasdaq-%D0%B8%D0%B7%D1%80%D0%B0%D0%B8%D0%BB%D1%8C%D1%81/
18. https://mfa.gov.il/mfa/innovativeisrael/sciencetech/pages/israel-launches-kidma-2-cyber-security-program-21-dec-2015.aspx
19. https://www.rafael.co.il/worlds/cyber-security/
20. https://www.g20.org/index.php/en/g20
21. https://mfa.gov.il/MFARUS/PressRoom/2016/Pages/PM-Netanyahu-speech-at-UNGA-22-9-16.aspx

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 67 - 70 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

„THE KNIGHT IN THE PANTHER'S SKIN''-INSTRUMENT OF 20TH CENTURY'S INFORMATION WARFARE'

,,ვეფხისტყაოსანი''- მე-20 საუკუნის საინფორმაციო ომის იარაღი ''

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

Natalia Patarkatsasvhili Ivane Javakhishvili Tbilisi State University, Journalism_Junior;

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

Ani Dekanosidze Ivane Javakhishvili Tbilisi State University, Journalism_Junior;

ანოტაცია: 21-ე საუკუნის მთავარ ,,მონაპოვრად'' თანამედროვე მსოფლიო სწორედ საინფრომაციო ომს მიიჩნევს. თუმცა ცოტამ თუ იცის, რომ სტალინი, ჯერ კიდევ ამ ტერმინის დანიშნულების გაგებამდე, აქტიურად იყენებდა სასურველი ინფორმაციის გავრცელეების სხვადასხვა ტექნიკებს, მათ შორის ხელოვნებას და ამ გზით, არაერთი საინფრომაციო ომის მოგებაც შეძლო. ამდენად, ვფიქრობთ, რომ საზოგადოებისთვის საინტერესო იქნება ,,დიდი ბელადის'' ფარული გეგმების და მისი პროპაგანდისტული მანქანის მოუშაობის სქემის გაცნობა.

Annotation: The modern world considers information warfare as the ,,achievement'' of 21st century, but little the world knows, that Stalin, before this word was even used, was spreading his ,,own'' information by different technics, he was even using an art and by this way was wining different wars. So, we think, that finding out new information about Stalin's plans and propagandistic machines will be interesting for society.

საკვანძო სიტყვები: საინფორმაციო ომი, ხელოვნება, სტალინი, ,,ვეფხისტყაოსანი'', პროპაგანდა, მე-20 საუკუნე.

,,ვეფხისტყაოსნის'' ღირებულებითი არსებობის მომავალი თაობებისათვის გადაცემა ისეთივე მნიშვნელოვანია, როგორც ჭადრაკში პაიკისთვის დაფის ბოლოში გასვლა, იმისათვის რომ აღსდგეს როგორც ძლიერი, სასურველი და მნიშვნელოვანი ფიგურა. ამის მისაღწევად კი საჭიროა მოთამაშემ კარგად იცოდეს თამაშის წესები, როგორც ჩანს, თამაშის ამ წესებს საოცრად ფლობდა დიდი ბელადი, მასაც ხომ იგივე მიზანი ჰქონდა! საკუთარი სახელის რესტავრაცია, გაძლიერება და თამაშის მთავარ მოქმედ ფიგურად

გადაქცევა არა მხოლოდ საბჭოთა კავშირში, არამედ მთელს მსოფლიოში, მან კი ამისთვის ყველაზე ჭკვიანურ გზას, ხელოვნებას მიმართა, დროსაც გაუსწრო და 21-ე საუკუნის მონაპოვარი-საინფორმაციო ომი გამოიყენა.

საკუთარი სახელისა და ვინაობის უკვდავსაყოფად სტალინმა სწორედ ხელოვნების დიდი ნიმუშის, მეთორმეტე საუკუნეში შექმნილი, ქართველი ერისთვის ღირებულებითი, მხატრული თუ შინაარსობრივი მნიშვნელობის განძის, ,,ვეფხისტყაოსნის'' გამოყენება გადაწყვიტა. 1941 წელს მოსკოვში გამოქვეყნდა შალვა ნუცუბიძის მიერ შესრულებული ,,ვეფხისტყაოსნის'' სრული, პოეტური რუსული თარგმანი. ეს ერთობ ჩვეულებრივი ფაქტია, რომელშიც არც სტალინის სახელი ფიგურირებს და შესაბამისად არც მისი მიზნები, მაგრამ ამ ფაქტს ,,არაჩვეულებრივს'' ის საარქივო დოკუმენტები, მიმოწერები თუ მოგონებები ხდის, რომლის გაცნობის საშუალებასაც თამარ ბელქანიას წიგნი ,,სტალინური კულტУРА!'' გვაძლევს. ერთი შეხედვით ჩვეულებრივი ფაქტის უკან დიდი პოლიტიკური მიზნები, საოცრად და შეფარვით განხორციელებული პროპაგანდა და დიდი ბელადის მრავალმხრივი ნიჭიერება იმალება განხორციელებული საინფორმაციო ომის საშუალებით.

მისი მიზანი მარტივი იყო, ომის მოსაგებად სასურველი ინფორმაციის გავრცელება, რათა მსოფლიოს დაენახა და დარწმუნებულიყო, რომ დიდი ბელადი უდიდესი ცივილიზაციისა და კულტურის მქონე ქვეყნის შვილი იყო, რაც ყველანაირ კითხვის ნიშანს გააქრობდა მისი წარმოშობისა და ვინაობის შესახებ. მიზანი მიიღწა, მაგრამ როგორ?

როგორც ზემოთ აღვნიშნეთ, ,,ვეფხისტყაოსანი'' ფილოსოფოსმა, ლიტერატურათმცოდნე, თბილისის სახელმწიფო უნივერსიტეტის ერთ-ერთმა დამაარსებელმა, მთარგმნელმა და საზოგადო მოღვაწე შალვა ნუცუბიძემ თარგმნა, თარგმნის შესახებ დეტალებს სწორედ მის მიერ, 27 წლის შემდეგ დაწერილი წერილიდან ვიგებთ. მისი დაკავება საკმაოდ საეჭვო გარემოებებში მომხდარა, დაკავებიდან გარკვეული დროის შემდეგ კი, სტალინს მისთვის ,,ვეფხისტყაოსნის'' თარგმნა დროის კონკრეტულ ვადაში მოუთხოვია. წერილიდანვე ვიგებთ, რომ ყოველ შაბათს მისი თარგმანები მიჰქონდათ და უკან შესწორებული ვარიანტები ბრუნდებოდა არც მეტი, არც ნაკლები დიდი ბელადის მიერ, აქ უკვე იკვეთება სტალინის დიდი ინტერესი ამ წიგნის მიმართ და ფაქტი, რომ ის უშუალოდ იღებს მონაწილეობას პოემის თარგმნაში. ერთობ მნიშვნელოვანი ფაქტიც უნდა აღვნიშნოთ , სტალინის მიერ ბერიასათვის ნათქვამ სიტყვებში, რომ ისევე არ არსებობს გალიაში მომღერალი შაშვი, როგორც კამერაში მომღერალი მგოსანი, და რომ რუსთაველის თარგმანის მისაღებად საჭირო იყო მგოსნის (ნუცუბიძის) გაშვება, წარმოდგენას გვიქმნის სტალინის, როგორც ხელოვნების არსის მცოდნეს შესახებ, მან კარგად იცის, რომ ღირებული, ფასეული ხელოვნება მხოლოდ თავისუფლების წიაღში იქმნება და სწორედ ხელოვნების საშუალებითაა შესაძლებელი მთავარი საინფორმაციო ომის მოგება.

ნუცუბიძემ თარგმნა დაასრულა, ნაშრომი კი სტალინის მაგიდაზე დასრულებისთანავე აღმოჩნდა. ბელადს მიზნის ძირითად ნაწილი უკვე ჰქონდა, ახლა მნიშვნელოვანი ინფორმაციული ხასიათის დეტალები იყო, რომელზე მუშაობაც, რა თქმა უნდა, საკუთარ თავზე აიღო, სატიტულო ფურცლის ტექსტი ჩაასწორა- „Перевод Шалвы

Нусубидзе „Перевод с грузинсского Шалва Нуцубидзе"-თი შეცვალა, სადაც საქართველოს ფიგურირებას პირველივე ფურცელზე გაუსვა ხაზი, პოემის სახელწოდების თარგმანიც საკუთარი ვერსიით შეცვალა და საბოლოოდ-,,Витязь в тигровой шкуре" დააწერა. მის მიერ წიგნის კონცებციის არსებობას ადასტურებს ისიც, რომ თავად ბელადმა განსაზღვრა ყდის დიზაინი, ორნამენტები, აბზაცები, სიტყვების წყობა და მიიღო თამბაქოსფერი, ხავერდოვანი ქსოვილის ორნამენტებით შემოსაზღვრული, შუაგულში შავ ფონზე რუსთაველის პორტრეტიანი ყდა. სამუშაოს მნიშვნელოვანი ნაწილი შესრულებული იყო, მაგრამ წინ მნიშვნელოვანი ეტაპი-ილუსტრირება იდგა. სტალინმა კარგად იცოდა, რომ ილუსტრაცია ყოველთვის ამდიდრებდა წაკითხულის შთაბეჭდილებას და ამიტომ მან ამაზეც იზრუნა. ცნობილია, რომ ბელადმა უპირატესობა უნგრელ ფერმწერსა და გრაფიკოსს მიხაილ ზიჩს მიანიჭა, ალბათ თვლიდა რომ ევროპა ევროპელის ნაშრომს უკეთესად აღიქვამდა, ეს ხომ მასათა დიდ ფენებზე, მათ შორის ევროპაზეც იყო გათვლილი. სტალინს მსოფლიოსთან გაჩაღებული ომი ყველაძე ძლიერი იარაღით, ინფორმაციით უნდა მოეგა, ამდენად უმნიშვნელოვანესი იყო ის ყველა გზავნილი, რომელსაც წიგნი მკითველს აწვდიდა. დიდი ბელადი მხოლოდ მხატვრების შერჩევით როდი შემოიფარგლა, ის თითოეულ ილუსტრაციას გაეცნო და თავისი შენიშვნები ლურჯი ფანქრითაც კი მიაწერა, რაც, რა თქმა უნდა, უსიტყვოდ დაკმაყოფილდა და საბოლოო სახეც სწორედ მისი სურვილებისა და შენიშვნების გათვალისწინებით მიიღო. აქ ყველაზე მნიშვნელოვანი ფაქტი, რასაც ნუცუბიძის წერილიდან ვიგებთ ისაა, რომ სტალინს არ სურდა საკუთარი სახელის სადმე, რაიმე ფორმით დაფიქსირება, რაც პირდაპირი მითითება იყო დიდი ბელადის. ნუცუბიძე ამავე წერილში თავის მოსაზრებას აფიქსირებს, რომ ბელადის ეს საქციელი მის მოკრძალებულობაზე მიუთითებდა და მას ზედმეტი დიდების მოხვეჭა აღარ სჭირდებოდა. სწორედ აქ ვლინდება სტალინის გეგმის წარმატების პირველი ნიშნები, მან საკუთარი სახელის ფიგურირების გარეშე შეძლო ფარული პიარის მექანიზმის ეფექტური ამუშავება, თავმდაბალი ბელადის სახელის რესტავრაცია ნუცუბიძის საშუალებით უპირველესად საქართველოში იწყებოდა. დიდი ბელადი ამ ერთი შეხედვით უმნიშვნელო, მაგრამ ერთობ მნიშვნელოვანი წიგნით შეძლებდა მკითხველის საკუთარი ინტერესებით მართვასა და მისთვის საჭირო ინფორმაციის ადრესატამდე ეფექტური გზით მიტანას. მან შეძლო კულტურული ძეგლის ინფორმციულ იარაღად გადაქცევა.

,,ვეფხისტყაოსნის'' საქმეში კიდევ ერთი, მნიშვნელოვანი პირის ფიგურირება იკვეთება, რომლის შესახებაც ინფორმაციას არქივში დაცული დოკუმენტებიდან ვიგებთ, ესაა გამორჩეული ბოლშევიკი და სტალინის მეგობარი, სერგო ქავთარაძე, რომლისთვისაც ბელადს ,,ვეფხისტყაოსნის'' მსოფლმხედველობის შესახებ ნარკვევის დაწერა დაუვალებია. ქავთარაძე დაწვრილებით აღწერს და საუბრობს არა მხოლოდ პოემის ესთეტიკურ, მხატრულ თუ შინაარსობრივ ღირებულებაზე, არამედ ეპოქაზე და ეპოქაში მიმდინარე რენესანსულ, პროგრესულ იდეებსა და პროცესებზე. ის ,,ვეფხისტყაოსანს'' განიხილავს როგორც აღმოსავლეთისა და დასავლეთის კულტურათა ,,ურთიერთქმედების პროდუქტს'', რომელიც მოიცავს ისეთ მაღალ ღირებულებით თემებს როგორიცებიცაა მეგობრობა, ქალის კულტი, სიყვარული, ჰუმანიზმი. საბოლოოდ, სერგო ქავთარაძის ნაშრომი ზუსტად

ემსახურება მიზანს, ესაა ბოლშევიკის მიერ, ობიექტურად დაწერილი ნარკვევი რომელიც მკითველში იწვევს აღტაცებასა და დიდ პატივისცემას არა მხოლოდ პოემის, არამედ იმ ეპოქის და ზოგადად ქვეყნის მიმართ სადაც ის შეიქმნა.

საბოლოოდ წიგნი ქვეყნდება, პროპაგანდისტული მექანიზმი მუშაობს, დიდი ბელადი მიზანს აღწევს და მისი სახელი სისხლიანი თუ ოქროს ასოებით მიანც იწერება ისტორიის უკვდავ ფურცლებზე.

საინფორმაციო ომი სტალინის სასარგებლოდ სრულდება, მსოფლიოს ბელადის სასურველი ინფორმაცია ჩუმად და შეფარვით, თუმცა ეფექტურად მიეწოდება. პროპაგანდისტული მანქანაც მუშაობს, ერთი საუკნით ადრე სტალინი ყველაზე მნიშვნელოვან და ყველაზე ძლიერ ფენომენს- საინფორმაციო ომს სათავისოდ იყენებს და მსოფლიოს თავს ,,დიდ ბელადად'' სთავაზობს.

ბიბლიოგრაფია

- თამარ ბელქანია -,,სტალინური კულტУРА!''
- შსს-ის არქივში დაცული დოკუმენტური მასალა

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 71 - 74 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

“DARKCOMET”-ის როლი სირიის კონფლიქტში“
„THE ROLE OF “DARKCOMET” IN THE SYRIAN CONFLICT“

ნათია ფილაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი.
Natia Pilashvili_ Ivane Javakhishvili Tbilisi State University, Sociology_Junior;
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. იმ შემთხვევაში კი როცა საქმე ეხება მასობრივ კონფლიქტებს, იგი უფრო მეტ მნიშვნელობას იძენს. სწორედ ამის ერთ-ერთი მაგალითია სირიის მთავრობის მიერ „DarkComet”-ის გამოყენებით სრული კონტროლის მოპოვება მის ოპონენტებზე და სასურველი ინფორმაციის მიღება მათსავე სამოქმედო გეგმებზე.

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. And when it comes to mass conflicts, it becomes even more important. One example of this is the Syrian government's use of „DarkComet“, to gain full control over its opponents and obtain desired information on their action plans.

საკვანძო სიტყვები: კიბერდანაშაული, კიბერშეტევა, დისტანციური მართვის მექნიზმი(RAT), „ტროიანი“, „ DarkComet”, „სირიის კონფლიქტი.

ტექნოლოგიურმა პროგრესმა უამრავი სიახლე შემატა საზოგადოებრივ ცხოვრებას, რასაც ბევრ დადებითთან ერთად უარყოფითი ასპექტებიც ახლავს თან. ინტერნეტის მეშვეობით ინფორმაციისა და მომსახურების მიღება-გავრცელების ხელმისაწვდომობამ ერთი მხრივ ცხოვრება გაგვიმარტივა, თუმცა მეორე მხრივ კიბერდამნაშავეთა რეალურ სამიზნე ობიექტებად გვაქცია. კიბერდამნაშავეთაგან წამოსული საფრთხეები შეგვიძლია 2 ნაწილად დავყოთ: პროგრამული საფრთხეები და ინტერნეტ-თაღლითობა.

პროგრამული საფრთხეები ძირითადად მავნე პროგრამებთან, უსადენო ინტერნეტ-კავშირთან(Wi-Fi), კიბერშეტევებთან, მზა ჩანაწერებთან(Cookies) და ვირტუალური ფულის გამომუშავებასთან არის დაკავშირებული. მავნე პროგრამა გულისხმობს კომპიუტერული კოდს ან აპლიკაციას, რომელსაც თქვენი მოწყობილობისთვის, იქნება ეს კომპიუტერი, მობილური ტელეფონი თუ ტაბლეტი, დიდი ზიანის მიყენება შეუძლია და ამავდროულად თქვენი პირადი ინფორმაციის მოპარვაც.

სწორედ ერთ-ერთ ასეთ მავნე პროგრამას წარმოადგენს ეგრეთწოდებული „ტროიანი“ იგივე „ტროას ცხენი“. მისი სახელწოდება მოდის ქალაქ ტროასთან დაკავშირებული ბერძნული ლეგენდიდან, რომლის თანახმადაც, ბერძნებმა ტროას ასაღებად ააგეს უზარმაზარი ხის ცხენი, შიგნით ჩასვეს ბერძენი ჯარისკაცები, ცხენი ტროას კარიბჭესთან დატოვეს, თვითონ კი ჯარი უკან გააბრუნეს, თითქოს დაზავებას აპირებდნენ. ტროელებმა ცხენი ღმერთების საჩუქრად მიიჩნიეს და ქალაქში შეაგორეს; ღამით, როდესაც ყველას ეძინა, მეომრები გადმოვიდნენ ცხენიდან, ბერძენ ჯარისკაცებს გაუხსნეს ქალაქის კარიბჭე და ტროა მიწასთან გაასწორეს. დღეს ტროას ცხენს გადატანითი მნიშვნელობით იყენებენ, როგორც მტრისგან მიძღვნილ „საჩუქარს“, რითაც იგი ცდილობს მოწინააღმდეგისთვის მახის დაგებას.

„ტროიანი“ მიეკუთვნება ისეთ მავნე კომპიუტერულ პროგრამას, რომელიც ერთი შეხედვით უვნებლად გამოიყურება, ან თავს ინიღბავს ყველასთვის კარგად ცნობილ პროგრამად, რადგან მომხმარებლები მათ ინსტალირებას არ ერიდებიან და საფრთხეს ნაკლებად ხედავენ, მაგალითად „Facebook“, რომელიც არაერთხელ გამხდარა ჰაკერების იარაღი. მსგავსი ხრიკებით რიგითი კომპიუტერის მომხმარებელები ადვილად ტყუვდებიან და საკუთარი ნებით საშუალებას აძლევენ „ტროას ცხენს“ შევიდეს მათ კომპიუტერულ სისტემაში. მის მიზანს არ წარმოადგენს საკუთარი თავის რეპლიკაცია. ჰაკერები მას კომპიუტერული სისტემის დისტანციურ მართვის მექანიზმად(RAT -Remote Administration Tool) იყენებენ .

ერთ-ერთი ყველაზე ცნობილი „ტროას ცხენი“ არის “DarkComet”. ის დისტანციური წვდომის ინსტრუმენტია, რომელიც შეიმუშავა ფრანგმა პროგრამისტმა ჟან-პიერ ლესუურმა, რითიც ცდილობდა პროგრამირებაში საკუთარი შესაძლებლობების წარმოჩენას და არანაირი სხვა მიზანი მას არ ამოძრავებდა. “DarkComet” საშუალებას აძლევს მომხმარებელს გააკონტროლოს სისტემა გრაფიკული ინტერფეისით(GUI – Graphical User Interface). მისი საშუალებით შესაძლებელია ფოტოების გადაღება ვებკამერიდან, საუბრის მოსმენა კომპიუტერთან მიერთებული მიკროფონიდან; მას

შეუძლია მოახდინოს დაინფიცირებული აპარატის სრული კონტროლიზება, როგორც ნებისმიერი ფაილის გადატანა დაინფიცირებულ აპარატზე, ისე ნებისმიერი დოკუმენტის მოპარვა. როგორც ბლოგი “Malwarebytes” გვეუბნება, პროგრამა “DarkComet”-ის შეძენა ჰაკერების ფორუმზე 2012 წელს შესაძლებელი იყო 25 ევროდ, რაც მის ფინანურ ხელმისაწვდომობაზე მიუთითებს. “DarkComet”-ის ფართო გავრცელება სწორედ 2012 წლიდან დაიწყო და ასოცირდება ისეთ ფართომასშტაბიან მოვლენასთან, როგორიცაა სირიის კონფლიქტი.

The Syrian Malware Team(SMT) წარმოადგენს სირიის მავნე პროგრამების სამთავრობო ჰაკერების ჯგუფს, რომელიც იყენებდა დისტანციური მართვის მექანიზმს(RAT). კიბერუსაფრთხოების ფირმის “FireEyes”-ის ცნობით ეს ჯგუფი პირველად გამოჩნდა 2011 წელს და აქტიური იყო 2014 წლის ივლისამდე. როგორც „ESG“(Environmental, Social, and Governance)-ის უსაფრთხოების მკვლევრებმა დაადგინეს „DarkComet“-ს მჭიდრო კავშირი ჰქონდა სირიის მთავრობასა და პოლიტიკურ დისიდენტებთან.

სირიის მთავრობა იყენებდა „DarkComet“-ის პროგრამას, რათა წვდომა ჰქონოდა ოპონენტების კომპიუტერულ სისტემაზე. მთავრობამ ის გამოიყენა, როგორც ჯაშუში. „არაბული გაზაფხულის“ მოძრაობისთვის კი ერთ-ერთი ყველაზე დამახასიათებელი ნიშანია ის, რომ ისინი იყენებენ ონლაინ სოციალურ ქსელებს და ძლიერ ეყრდნობიან ისეთ პროგრამას კომუნიკაციისთვის, როგორიცაა „Skype“. სიირის მთვარობამ „DarkComet“, სწორედ „Skype”-ის მეშვეობით გაავრცელა და შეძლო, რომ ერთი აქტივისტის დაკავებითა და მის პირად მონაცემებში შეღწევით, წვდომა ჰქონოდა მასთან კავშირში მყოფ აქტივისტებთან. ასევე სამთავრობო ჯგუფის წევრები, როგორც ქალი ანტისამთავრობო აქტივისტები უკავშირდებოდნენ მსხვერპლებს „Skype”-ით ან „Facebook”-ით, უგზავნიდნენ ქალის ფოტოს, რომელიც შეიცავდა მავნე პროგრამას. როდესაც ამ სურათს ხსნიდნენ, “DarkComet” აქტიურდებოდა მათ კომპიუტერზე და ფარულად აკავშირებდა სამთავრობო სისტემასთან. მთავრობის მიზანსაც სწორედ ეს წარმოადგენდა, მათ შეძლეს ანტისამთავრობო ჯგუფების სამოქმედო გეგმების გაშიფვრა, რის შემდეგაც დაიწყო მასობრივი დაკავებები.

მას მერე, რაც „DarkComet“ დაუკავშირდა სირიის რეჟიმს, ჟან-პიერ ლესუურმა შეწყვიტა ინსტრუმენტის შემუშავება და განაცხადა: ”- მე არასოდეს წარმომედგინა, რომ მთავრობა მას ჯაშუშობაში გამოიყენებდა, ეს რომ მცოდნოდა, არასოდეს შევქმნიდი ასეთ ხელსაწყოს.”

დღევანდელი მონაცემებით “DarkComet”-ის პროგრამაზე მუშაობა შეწყვეტილია, ხოლო მისი გადმოტვირთვა ოფიციალური ვებ-გვერდიდან აღარაა შესაძლებელი.

ამ შემთხვევამ ნათლად დაგვანახა, რომ სწრაფი ტექნოლოგიური პროგრესის საუკუნე, არის დრო, როცა ჩვენი ყოველდღიური ცხოვრება უშუალოდაა დაკავშირებული ციფრულ ტექნოლოგიასთან და სოციალურ ქსელებთან, რაც მნიშვნელოვნად ზრდის კიბერდანაშაულის რისკებს. განვიხილეთ ერთ-ერთი ყველაზე ცნობილი „ტროიანი“ - Dark Comet”, რომლის შემქმნელს ისევე ვერ წარმოედგინა ამ ხელსაწყოს ბოროტად გამოყენება, როგორც აინშტაინს, ის, რომ მისი ფორმულა საფუძველი გახდებოდა ბირთვული იარაღის შექმნისა, რომლის ბოროტი მიზნებით გამოყენებამაც XX საუკუნეში უდიდესი ტრაგედიები გამოიწვია.

ბიბლიოგრაფია

1. McMillan, Robert. “How The Boy Next Door Accidentally Built a Syrian Spy Tool”(07/11/2012) https://www.wired.com/2012/07/dark-comet-syrian-spy-tool/?fbclid=IwAR1_9WwMBqk2iTsGLwXfmCn03Gt-1b0BK3MmERTEZOL2iAL2Ve69gfV_qHU
2. “DarkComet”(2012) https://www.enigmasoftware.com/darkcomet-removal/?fbclid=IwAR1iDHGo3W5J3PCL2sxpP5cyEmGWBzdJzzN1XI1jCuQvel5v1dowPc8006Q
3. “DarkComet Surfaced in The Targeted Attacks in Syrian Conflict”(23/02/2012) https://blog.trendmicro.com/trendlabs-security-intelligence/darkcomet-surfaced-in-the-targeted-attacks-in-syrian-conflict/?fbclid=IwAR0rc-2t2SlPbV-63JKASqZ6aX7fI5NJgQ29qVf6xXZGU8XXFCr1gJbT8AI
4. “DarkComet Analysis – Understanding the Trojan used in Syrian Uprising”(16/03/2012) https://resources.infosecinstitute.com/darkcomet-analysis-syria/?fbclid=IwAR39kzxgBnRkuD2X0F37f8F9XtNXyLvMOoFPT6dwO0eQiLP3tXQogmRHqCI#gref
5. "Spy code creator kills project after Syrian abuse". BBC. 10 July 2012. https://www.bbc.com/news/technology-18783064?fbclid=IwAR0DG-AyU1c3KDSDqqKoC9qyTuOkEQqYq6p7oXL5OgDrUFKVYMn4JIa5Yi8
6. “The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict”. Zürich, October 2017. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-05.pdf?fbclid=IwAR1vUGDqF2xq-SyHH4MoECftOB-CIBMtGX_3ZWX4eDN5pyxk1Zks_Aq6QIo

Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 75 - 74 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

რუსეთის „ჰიბრიდული ომი“ საქართველოსა და უკრაინაში

RUSSIA'S HYBRID WARFARE IN GEORGIA AND UKRAINE

Ilia Khutsishvili
New Vision University

ანოტაცია. ჰიბრიდული ომის წარმოებისას სახელმწიფოთათვის დროული, სრულყოფილი და ობიექტური სადაზვერვო ინფორმაციის მოპოვება და კონტრსადაზვერვო რეაგირება სასიცოცხლოდ მნიშვნელოვანია სწორი, საშინაო და საგარეო პოლიტიკური კურსის გასატარებლად. ჰიბრიდული ომის ერთ-ერთ მიმართულებას სწორედ ინფორმაციული ომის წარმოება წარმოადგენს, ვინაიდან ინფორმაციული ომის მიზანი სწორედ ქვეყნის მოსახლეობის საზოგადოებრივი აზრის ფორმირება და ფსიქოლოგიური ზემოქმედების მოხდენაა.

ნაშრომის მიზანია რუსეთის ფედერაციის მიერ საქართველოსა და უკრაინაში წარმოებული ჰიბრიდული ომის პირობებში, რუსეთის სპეცსამსახურების დაინტერესების სფეროების, მიზნების, მისწრაფებებისა და ამოცანების გათვალისწინებით გამოიკვეთოს ძირითადი მიმართულებები, საფრთხეები და რისკ-ფაქტორები.

საკვანძო სიტყვები: ეროვნული უსაფრთხოება, ინფორმაციული ომი, დეზინფორმაცია, ჰიბრიდული ომი;

ABSTRACT. During the hybrid warfare obtaining timely, comprehensive and objective intelligence information and counter-intelligence responses for states is vital to pursuing the right, domestic and foreign policy course. One of the directions of hybrid warfare is to conduct information warfare, as the purpose of information warfare is to shape public opinion and to exert psychological influence on the population.

The purpose of this paper is to identify the main directions, threats and risk factors of the Russia’s special services in the context of the hybrid warfare to outline Russia’s special servises’ interests, goals, aspirations and objectives in Georgia and Ukraine.

Keywords: National Security, Information Warfare, Disinformation, Hybrid Warfare;

შესავალი*

ნებისმიერი სახელმწიფოს მიზანი საკუთარი ეროვნული უსაფრთხოების უზრუნველყოფაა, რომელიც გულისხმობს ქვეყნის შიგნით და მისი ფარგლების გარეთ არსებული საფრთხეების, რისკებისა და გამოწვევების გამოვლენას, იდენტიფიცირებას,

* ნაშრომში გამოთქმული მოსაზრებები და დასკვნები ეკუთვნის ავტორს და არ გამოხატავს რომელიმე ორგანიზაციის ან უწყების ოფიციალურ პოზიციას;

შეფასებასა და თავიდან აცილებას. ამისათვის სპეცსამსახურების მეშვეობით მიმართავენ სხვადასხვა ხერხს, როგორც ე.წ „მშვიდობიან“ ასევე აქტიურ საომარ მოქმედებებს.[1]

ბოლო პერიოდში წარმოებული ექსპანსიური პოლიტიკის (მათ შორის, სამხედრო ძალის გამოყენება) გამო რუსეთის ფედერაციას საგრძნობლად დაეძაბა ურთიერთობა ევროპის სახელმწიფოებთან და ამერიკის შეერთებულ შტატებთან, რამაც ფაქტიურად გამოიწვია მისი საერთაშორისო იზოლაცია, ამასთან დაწესებულმა ეკონომიკურმა სანქციებმა[2] (როგორც ევროკავშირის[3] ისე აშშ-ის მიერ დაწესებული) საგრძნობლად გააუარესა რუსეთის შიდა პოლიტიკური და სოციალური ვითარება. არსებული რეალობა აიძულებს რუსეთს, ე.წ ჰიბრიდული ომის ხერხებისა და მეთოდების გამოყენებით დააჩქაროს თავისი გეოპოლიტიკური გეგმის რეალიზება, რომლის მიზანია კონტროლის აღდგენა მთელს პოსტ-საბჭოთა სივრცეზე, რომელიც მიმართულია ყოფილ საბჭოთა ქვეყნებზე საკუთარის გავლენისა და პოზიციების აღდგენისაკენ, სამხედრო, პოლიტიკური და ეკონომიკური კონტროლის გაძლერებსაკენ.[4]

რუსეთის ფედერაციის აგრესიულმა მოქმედებება ჯერ საქართველოში, შემკდეგ უკრაინასა და სირიაში ნათლად წარმოაჩინა, რომ რუსეთის სპეცსამსახურები საკმაოდ ეფექტიანად იყენებენ მათ ხელთ არსებულ სამხედრო, ეკონომიკურ და პოლიტიკურ შესაძლებლობებს. განსაკუთრებით აქტიურია რუსული პროპაგანდა და ინფორმაციული ომი, რომელშიც სპეცსამსახურებთან ერთად ჩართულია რუსეთის ყველა მნიშვნელოვანი სახელმწიფო ინსტიტუტი.

1. რუსეთის მერ გამოყენებული ძალები და საშუალებები

სადაზვერვო საქმიანობა სახემწიფოთა საერთაშორისო ურთიერთობების მნიშვნელოვანი შემადგენელი ნაწილია. სადაზვერვო საქმიანობის ძირითად პრინციპს მძლავრი საინფორმაციო აპარატის შექმნა და მოწინააღმდეგე სახელმწიფოს ირგვლივ მასშტაბური ინფორმაციის შეკრება წარმოადგენს. რუსეთის ფედერაციისთვის საქართველო და უკრაინა სადაზვერვო ზეგავლენისა და შეღწევადობის მნიშვნელოვან ობიექტებს წარმოადგენენ და დღესდღეობით, როგორც მართვის მყარ ბერკეტად რუსეთის სპეცსამსახურების მიერ გამოყენებულია ეთნიკური და რელიგიური ხასიათის კონფლიქტების ინსპირირება და საქართველოსა და უკრაინის ოკუპირებულ ტერიტორიებზე ბუფერულ ზონებად ჩამოყალიბებული სეპარატისტული რეჟიმები.

[1]Lind W.S., Nightengale K., Schmitt John F., Sutton J., Wilso G.I., The Changing Face of War: Into the Fourth Generation, Marine Corps Gazette, Oct 1989, 22;

[2] Congressional Research Service, U.S. Sanctions on Russia, January 11, 2019, https://fas.org/sgp/crs/row/R45415.pdf [წვდომის თარიღი: 27.07.2019];

[3] Council of the European Union General Secretariat, EU restrictive measures in response to the crisis in Ukraine, 5 September 2018, https://eeas.europa.eu/sites/eeas/files/eu_restrictive_measures_in_response_to_crisis_in_ukraine_en.pdf [წვდომის თარიღი: 27.07.2019];

[4] Jonavicius L., Delcour L., Dragneva R., and Wolczuk K., Russian Interests, Strategies, and Instruments in the Common Neighbourhood, No. 16, March 2019, <http://eu-strat.eu/wp-content/uploads/2019/03/EU-STRAT-Working-Paper-No.-16.pdf>, [წვდომის თარიღი: 27.07.2019];

2016 წლის 30 ნოემბერს რუსეთის ფედერაციამ დაამტკიცა საგარეო პოლიტიკის ახალი კონცეფცია,[5] რომლის თანახმად, რუსეთის ერთ–ერთ პრიორიტეტად დასახელებულია გლობალურ საინფორმაციო სივრცეში რუსული მედია საშუალებების პოზიციების გაძლიერება და საერთაშორისო საზოგადოებისათვის საერთაშორისო პროცესებზე რუსული ხედვის მიწოდება. კონცეფციის მეოთხე თავი რუსეთის საგარეო პოლიტიკის რეგიონულ პრიორიტეტებს, მათ შორის პოსტსაბჭოთა ქვეყნებს ეხება.

რუსეთის დაინტერესება საქართველოთი განპირობებულია, როგორც ევროპისა და აზიის გასაყარზე მდებარე ქვეყანა და კავკასიის რეგიონში მისი სტრატეგიული მნიშვნელობით, ხოლო უკრაინით დაინტერესება განპირობებულია, იმით რომ იგი წარმოადგენს ევროკავშირისა[6] და NATO-ს[7] დიდ სტრატეგიულ დასაყრდენს შავი ზღვის აუზში, როგორც პოლიტიკური, ასევე სამხედრო თვალსაზრისით.* აგრეთვე რუსეთისთვის საყურადღებოა საქართველოსთან და უკრაინასთან[8] მიმართებით შემდეგი ასპექტები: დასავლეთზე ორიენტირებული პოლიტიკა, NATO-სთან თანამშრომლობის გაღრმავების დადებითი დინამიკა, საქართველოს მიერ აღმოსავლეთ პარტნიორობის პროექტში[9] მონაწილეობა,* ენერგომატარებლებისა და ტვირთების საერთაშორისო სატრანზიტო

[5] Концепция внешней политики Российской Федерации, 30 ноября 2016 г. <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU> [წვდომის თარიღი: 27.07.2019];

[6] European Parliament Resolution „EU Strategy for the Black Sea“, 20 January 2011, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0025+0+DOC+XML+V0//EN [წვდომის თარიღი: 27.07.2019];

[7] NATO Parliamentary Assembly Resolution #437 on STability And Security In The Black Sea Region, 09 October 2017, <https://www.nato-pa.int/download-file?filename=sites/default/files/2017-10/2017%20-%20RESOLUTION%20437%20-%20BLACK%20SEA%20-%20SCHMIDT%20%20-%20%20219%20CDS%2017%20E.pdf> [წვდომის თარიღი: 27.07.2019];

* NATO-სთვის შავ ზღვას სტრატეგიული მნიშვნელობა აქვს, რადგან მას სამხედრო თვალსაზრისით, დიდი ადგილი უჭირავს ევროპული კოლექტიური თავდაცვის სისტემაში. ამავდროულად რუსეთთან გამკლავების ერთ-ერთ ფრონტს წარმოადგენს და სხვადასხვა კონფლიქტებისა და დაპირისპირების ფონზე ევრო-ატლანტიკური სივრცის სტაბილურობისთვის მნიშვნელოვან გამოწვევას წარმოადგენს. ტერორიზმის საფრთხემ და ახლო აღმოსავლეთში (კერძოდ, სირიაში) მდგომარეობის ესკალაციამ კიდევ უფრო დიდი სტრატეგიული დატვირთვა შესძინა ამ რეგიონს. აგრეთვე სირიაში მიმდინარე სამხედრო მოქმედებებისთვის შავი ზღვის აუზი NATO-ს, რუსეთისა და თურქეთის სამხედრო გემებისა და სხვა შეირაღების განთავსებისთვის სტრატეგიულ სივრცედ იქცა;

[8] Robert C., “Top Russian General Lays Bare Putin's Plan for Ukraine”, Huffington Post, 09 February 2014, <https://www.huffpost.com/entry/valery-gerasimov-putin-ukraine_b_5748480> [წვდომის თარიღი: 27.07.2019];

[9] The Eastern Partnership (EaP), https://www.euneighbours.eu/en/policy#the-eastern-partnership, [წვდომის თარიღი: 27.07.2019];

* ,,აღმოსავლეთ პარტნიორობა“, როგორც ევროკავშირის აღმოსავლეთ ევროპულ მეზობელ ქვეყნებთან (აზერბაიჯანი, ბელარუსი, მოლდოვა, საქართველო, სომხეთი, უკრაინა) თანამშრომლობის ფორმატი, წარმოადგენს შვედეთისა და პოლონეთის ინიციატივას. მისი მთავარი მიზანია, ევროპელ პარტნიორებთან მიმართებაში, ევროპული სამეზობლო პოლიტიკის (ENP) განხორციელების ხელშეწყობა და მისი აღმოსავლეთ განზომილების გაძლიერება. აღსანიშნავია, რომ მოცემული ინიციატივა ამ ქვეყნებს, ევროკავშირთან მნიშვნელოვნად დაახლოების მიზნით, კონკრეტულ მექანიზმებს სთავაზობს და ახალ შესაძლებლობებს უხსნის. 2008 წლის 3 დეკემბერს, ევროკომისიამ გამოაქვეყნა კომუნიკაცია “აღმოსავლეთ პარტნიორობის“ შესახებ, რომელიც დამტკიცდა 2009 წლის 19 მარტს ევროპული საბჭოს სხდომაზე;

ფუნქციის შეძენა,* დემოკარატიული პროცესების გაღრმავება, ქვეყანაში არსებული ოკუპირებული ტერიტორიების საკითხი.

აღნიშნულიდან გამომდინარე, რუსეთის სპეცსამსახურები სადაზვერვო საქმიანობას ახორციელებენ მათი სახელმწიფოების პოლიტიკის შესაბამისად, რომელსაც იგი ატარებს საქართველოსთან და უკრაინასთან მიმართებით.[10] შესაბამისად რუსეთი სადაზვერვო საქმიანობას წარმართავს, რათა გავლენა იქონიონ საქართველოსა და უკრაინაში მიმდინარე პოლიტიკურ, სოციალურ-ეკონომიკურ და ეთნიკურ-რელიგიურ პროცესებზე.

საქართველოსთან მიმართებაში რუსეთი მოქმედებს თავისი საგარეო პოლიტიკური კონცეფციის - ე.წ „რბილი ძალის“ ფარგლებში,[11] რომელის შემადგენელი ნაწილია სახალხო დიპლომატია.

სახალხო დიპლომატია გულისხმობს პოლიტიკური (საერთაშორისო და რეგიონალური) პრობლემების განხილვას აკადემიურ და ექსპერტულ გარემოში, სადაც მოხდება აღნიშნულ პრობლემასთან დაკავშირებით რუსეთის პოზიციის „შემოჩეჩება“. ამ მიზნის მისაღწევად „რბილი ძალის“ პოლიტიკა მიმართულია საქართველოში მრავალრიცხოვანი „ელიტური ფენის“ შექმნისაკენ (მეცნიერები, ჟურნალისტები, მასმედია, ექსპერტები, პოლიტიკოსები, მაღალი თანამდებობის პირები და პოლიტიკური ფიგურები), რომელიც ორიენტირებული იქნება რუსეთთან თანამშრომლობაზე. რუსეთი ცდილობს აღნიშნული ფენაში გააძლიეროს და გააფართოვოს პოლიტიკური ზეგავლენის წრე.

რუსეთის საგარეო უწყებისა და სპეცსამსახურების ხელშეწყობით მოქმედი ორგანიზაციების წარმოამადგენლები სისტემატიურად ჩადიან საქართველოში კონფერენციების, სემინარების, მედიაფორუმების, ტელევიზიებსა და საქსპერტო დისკუსიების გასამართად. აქტიურად ახორციელებენ საქართველოში პრორუსული ორიენტაციის ორგანიზაციების, კონკრეტული ჯგუფების ან პირების (სხვადასხვა პროექტის ფარგლებში) დაფინანსებას და აყალიბებენ ახალ არასამთავრობო ორგანიზაციებს. [12]

„ჰიბრიდული ომის“ ელემენტს საქართველოსთან მიმართებაში წარმოადგენს ზეწოლის ბერკეტად ოკუპირებული ტერიტორიების ფაქტორის გამოყენება, ე.წ „მცოცავი ოკუპაცია“ და „ე.წ „ ბორდერიზაციის პროცესი“.[13]

---

* აზერბაიჯანს, საქართველოსა და თურქეთს შორის ჩამოყალიბდა სტრატეგიული თანამშრომლობა კასპიის ენერგო რეუსრსების სატრანზიტო პროექტების, კერძოდ, ბაქო-სუფსის (WREP), ბაქო-თბილისი-ჯეიჰანის (BTC) და ბაქო-თბილისი-ერზრუმის (SCP) მილსადენების და აგრეთვე, საქართველოს საზღვაო ტერმინალების და რკინიგზის, ეფექტური უტილიზაციისთვის;

[10] HRW – Human Rights Watch, World Report 2019 – Ukraine, <https://www.hrw.org/world-report/2019/country-chapters/ukraine> [წვდომის თარიღი: 27.07.2019];

[11] რუსეთის ხისტი და რბილი ძალის საფრთხეები საქართველოში, რედაქტორი: კაკოიაშვილი ი., ჩაგანავა ა., ვოთი ა., სნიპი ი., ევროპული ინიციატივა – ლიბერალური აკადემია, თბილისი, 2016 წელი, გვ. 8-14;

[12] საერთაშორისო სამხრეთ კავკასიური მედია ფორუმი თბილისში, <https://euronews.ge/%E1%83%A1%E1%83%90%E1%83%9B%E1%83%AE%E1%83%A0%E1%83%94%E1%83%97%E1%83%99%E1%83%90%E1%83%95%E1%83%99%E1%83%90%E1%83%A1%E1%83%98%E1%83%A3%E1%83%A0%E1%83%98-%E1%83%A1%E1%83%90%E1%83%94%E1%83%A0%E1%83%97/>, 27 ივნისი, 2017, [წვდომის თარიღი: 27.07.2019];

[13] საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, ოკუპირებული ტერიტორიები, 01.01.2016-31.12.2016, გვ. 4-7;

საქართველოს მსგავსად, უკრაინასთან მიმართებითაც რუსეთის გავლენის ბერკეტს წარმოადგენს ოკუპირებული ტერიტორიების ფაქტორით მანიპულირება (ყირიმის, დონეცკისა და ლუგანსკის ოლქები) და აღნიშნულ ტერიტორიებზე რუსეთთან მიერთების თაობაზე რეფრენდუმის ჩატარება.[14]

1.1 ეთნიკური უმცირესობებით მანიპულირება და კუთხური სეპარატიზმის ინსპირირება

საქართველო, რომელიც გეოპოლიტიკურად და სტრატეგიულად იმყოფება საკმაოდ რთულ რეგიონში, მის განსაკუთრებულ ნიშან-თვისებას სწორედ ეთნიკური და რელიგიური მრავალფეროვნება წარმოადგენს.[15]

საქართველოში ეთნიკურ-რელიგიურ ფონზე დაპირისპირებისათვის ხელსაყრელი ნიადაგის შესაქმნელად, რუსეთის სპეცსამსახურების განსაკუთრებული დაინტერესების ობიექტს სწორედ ქვეყნის ეთნიკური და რელიგიური უმცირესობებით მჭიდროდ დასახლებული რეგიონები (ქვემო ქართლი, კახეთი, სამცხე-ჯავახეთი, აჭარა)[16] წარმოადგენენ, სადაც მიზანმიმართულად ახორციელებენ ეთნიკურ და რელიგიურ ნიადაგზე მოსახლეობაში დასპირისპირებისა და შუღლის ინსპირირებას.

კუთხური სეპარატიზმის გაღვივების მხრივ, რუსეთის სპეცსამსახურების ინტერესის სფეროში ექცევა აჭარა, სვანეთი და სამეგრელო, სადაც ცდილობენ კუთხური სეპარატიზმის გაღვივებას (მათ შორის რელიგიური კუთხით), რაც ქვეყნის მოსახლეობაში მუდმივი დაძაბულობისა და არეულობის განცდის გაჩენას ემსახურება, რათა გაჩნდეს სეპარატისტული კერები ქვეყანაში, ისე როგორც ეს განხორციელდა აფხაზეთსა და სამაჩაბლოში.[17] აღნიშნული რეგიონები (აფხაზეთი და სამაჩაბლო) საქართველოს ფაქტობრივი კონტროლის ზონიდან გავიდა, რამაც მნიშვნელოვანი დარტყმა მიაყენა სახელმწიფოს ეროვნულ უსაფრთხოებას, რითაც ფაქტობრივად შეიქმნა ე.წ ბუფერული ზონები. პრაქტიკულად სახეზეა ვითარება, როდესაც საქართველო სამართლებრივი კონტროლის ფონზე ფაქტობრივ კონტროლს ვერ ახორციელებს ზემოაღნიშნულ რეგიონებზე.

ანალოგიურად, ადგილობრივ მოსახლეობაში სეპარატისტული განწყობების ინსპირირებითა და მათზე სადაზვერვო შეღწევადობით მოახდინა რუსეთმა ყირიმის ანექსია[18] და დონეცკისა და ლუგანსკის ოლქების ოკუპაცია,[19] იმ საბაბით, თითქოსდა

---

[14] Office of the United Nations High Commissioner for Human Rights, Situation of human rights in the temporarily occupied Autonomous Republic of Crimea and the city of Sevastopol (Ukraine), P.1-3, <https://www.ohchr.org/Documents/Countries/UA/Crimea2014_2017_EN.pdf>, [წვდომის თარიღი: 27.07.2019];

[15] საქართველოს მთავრობის განკარგულება №1740, სამოქალაქო თანასწორობისა და ინტეგრაციის სახელმწიფოს ტრატეგიისა და 2015-2020 წწ. სამოქმედო გეგმის დამტკიცების შესახებ, 2015 წლის 17 აგვისტო ქ. თბილისი;

[16] ეთნოსთა შორის ოთანამშრომლობისა და კონსულტაციების ანალიტიკური ცენტრი, საქართველოში ეთნიკური უმცირესობათა სათემო ორგანიზაციების საჭიროებების შეფასება, რედ. ალეკსანდრა დელემენჩუკი, თბილისი, 2012, გვ. 9-17;

[17] კუხალაშვილი დ., „სადაზვერვო და კონტრსადაზვერვო საქმიანობის ორგანიზაცია რელიგიის საფარქვეშ," შსს აკადემიის გამომცემლობა, თბილისი, 2016 წელი, გვ. 87-90;

[18] MH17: How did the conflict in Ukraine start?, By international correspondent Mark Corcoran, 29 Jul 2014, <https://www.abc.net.au/news/2014-07-29/mh17-how-did-the-conflict-in-ukraine-start/5629990> [წვდომის თარიღი: 18.09.2019];

აღნიშნულ რეგიონში მცხოვრები მოსახლეობის სურვილი იყო გასულიყვნენ უკრაინის შემადგენლობიდან.* რეალურად რუსეთის მიერ ყირიმის ანექსიის მიზაზი გახდა მისი სტრატეგიული მნიშვნელობა, რომელიც სამხედრო-სტრატეგიული მიზეზებით შეიძლება აიხსნას. კერძოდ, კონტინენტურ ევროპაში NATO-ს სამხედრო მონოპოლიის დასრულება, NATO-სა და ევროკავშირის საზღვრების გაფართოების აღკვეთა და შავ ზღვაზე ერთპიროვნული სამხედრო კონტროლის მოპოვება.[20]

1.2 ენერგო რესურსებზე კონტროლი და ეკონომიკური ექსპანსია

უკანასკნელ ათწლეულში, მსოფლიო გლობალიზაციის პროცესების ფონზე, ენერგო რესურსებით მანიპულირება საერთაშორისო ურთიერთობებში რუსეთის ძირითად პოლიტიკურ ბერკეტად იქცა. ყოველივე ამას სპეცსამსახურები საკუთარი ინტერესების გატარებისათვის და სასურველი საზოგადოებრივი აზრის ფორმირებისათვის აქტიურად იყენებენ სხვა სახელმწიფოს წინააღმდეგ.

რუსეთი განსაკუთრებულ ყურადღებას იჩენს საქართველოში ეკონომიკური ბერკეტების შესაქმნელად. მათი სპეცსამსახურების მხრიდან გაძლიერდა ქვეყნს ეკონომიკური პოლიტიკის, პოტენციალისა და ბაზრის შესწავლა, რის შედეგადაც ხორციელდება კომპანიების შერჩევა საქართველოში შემოსასვლელად. რუსული ინვესტიცია განსაკუთრებით მსხვილი მასშტაბებითაა წარმოდგენილი ენერგეტიკის, ფინანსური, სატელეკომუნიკაციო და სასარგებლო წიაღისეულის მოპოვების სფეროებში.

ეკონომიკური დაზვერვის კუთხით რუსეთის მიზანს მის ბაზარზე საქართველოს დამოკიდებულების ეტაპობრივი ზრდა და გაძლიერება წარმოადგენს. ამ კუთხით ღია წყაროებში არსებული მონაცემების ანალიზი იძლევა საშუალებას დავასკვნათ, რომ 2008 წლამდე და მის შემდგომ პერიოდში საქართველოს მიერ სტრატეგიული (მათ შორის ეკონომიკური და ენერგეტიკული) ობიექტები გადაცმულ იქნა რუსეთის ფედერაციისათვის ან მასთან დაკავშირებული კომპანიებისათვის. დიდი ალბათობით აღნიშნული ფაქტი სადაზვერვო ზეგავლენითა და შეღწევადობით არის განპირობებული.

რუსეთი აგრეთვე იყენებს ისეთ ფორმებს, როგორიცაა ეკონომიკური ბერკეტებით მანიპულირება (რუსული ბაზრის დახურვა, ქართულ პროდუქტზე შეზღუდვების დაწესება, რუსეთის ენერგო რესურსებზე საქართველოს დამოკიდებულება, პირდაპირი

---

[19] The army of the Lugansk and Donetsk People's Republics has 20,000 fighters – Gubarev, Information Telegraph Agency of Russia. 9 July 2014, <https://tass.com/world/739790>[წვდომის თარიღი: 18.09.2019];

* 2008 წლის აგვისტოს ომის წინ აფხაზეთში და განსაკუთრებით ცხინვალის რეგიონში დაიწყო რუსეთის ფედერაციის პასპორტების დარიგება, რაც ხელ-ფეხს უხსნიდა კრემლს, თავისი მოქალაქეების დაცვის საბაბით სუვერენული საქართველოს ტერიტორიაზე შეიარაღებული ძალები შემოეყვანა. იგივე სცენარით განვითარდა მოვლენები უკრაინაში, როდესაც რუსეთის ფედერაციის სახელმწიფო დუმამ მიიღო კანონი, რომელიც უკრაინის მოქალაქეებს, სურვილის შემთხვევაში, დაჩქარებული წესით მიანიჭებდა რუსეთის მოქალაქეობას და კიდევ ერთ კანონი, რომელიც ითვალისწინებდა რუსეთის ფედერაციისთვის უცხო ქვეყნის ტერიტორიების სწრაფი ტემპით მიერთებას ადგილობრივი მოსახლეობის რეფერენდუმის საფუძველზე;

[20] Radin A., Rach C., Russian Views of the International Order, Published by the RAND Corporation, Santa Monica, Calif, 2017, P. 79, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1800/RR1826/RAND_RR1826.pdf [წვდომის თარიღი: 27.07.2019];

ავიარეისების აკრძალვა), ფინანსური და ეკონომიკური შესაძლებლობების გარდაქმნა კულტურულ-საგანმანათლებლო და ინფორმაციულ იარაღად, ასევე საქართველოში შესაბამისი „რესურსების“ ინვესტირება“ რუსეთის პოზიტიური იმიჯის შესაქმნელად და საქართველოს „მეგობრად“ წარმოსაჩენად.

უკრაინაში რუსეთის მიერ ენერგო რესურსებით მანიპულირების მაგალითია რუსეთის მიერ უკრაინისთვის ბუნებრივი აირის მიწოდების შეწყვეტა და ამით ევროპისთვის სერიოზული პრობლემების შექმნა. უკრაინის სტრანზიტო როლის შემცირებამ შეუქმნა პრობლემები როგორც ქვეყნის ენერგეტიკულ უსაფრთხოებას, ასევე, ევროკავშირისთვისაც საფრთხის შემცველია, რომელსაც არ გააჩნია ენერგობაზარი და ძირითადად, რუსეთის ენერგორესურსებზეა დამოკიდებული.[21]

2. დეზინფორმაცია და კიბერელემენტები ინფორმაციული ომის წარმოებაში

სახელმწიფოში ინფორმაციული უსაფრთხოების უზრუნველყოფის ხარისხი განაპირობებს სახელმწიფოს პოლიტიკური დესტაბილიზაციისა და დივერსიებისგან დაცვის ხარისხს.

ინფორმაციული უსაფრთხოიების ერთ-ერთ შემადგენელ კომპონენტს წარმოადგენს კიბერ უსაფრთხოება, რომელიც ტექნოლოგიების განვითარებასთან ერთად სულ უფრო და უფრო აქტუალური ხდება სახლემწიფოთათვის. ბოლო ათწლეულში მსოფლიოში მომხდარი კონფლიქტების დროს, სახელმწიფოთა სპეცსამსახურების მიერ აქტიურად გამოიყენება კიბერშეტევები. 2008 წლის აგვისტოს ომის დროს კიბერშეტევები ხორციელდებოდა მასობრივად სახელმწიფოს საინფორმაციო-ტექნოლოგიურ სისტემაზე, რომელიც მიზნად ისახავდა სახელმწიფოს კრიტიკული ინფრასტრუქტურის პარალიზებას.[22]

საომარი მიმდინარეობის დროს სამხედრო კიბერშეტევების განხორციელება მოწინააღმდეგე სახელმწიფოზე ზუსტად ერგება ე.წ. ჰიბრიდული ომის კონცეფციას.[23] კიბერშეტევებით ხდება სახელმწიფოს იზოლაცია ცივილიზებული სამყაროსაგან და მისი მოქცევა ინფორმაციულ ვაკუუმში, რაც დამაზიანებლად მოქმედებს როგორც შეიარაღებული ძალების კოორდინირებულად მოქმედებაზე, ისე ქვეყნის მოსახლეობაზე, ვინაიდან ასეთ შემთხვევაში მოწინააღმდეგე სახელმწიფოს სპეცსამსახურების მიერ ადგილი აქვს დეზინფორმაციის გავრცელებას, რაც იწვევს შიშს, პანიკასა და არეულობას მოსახლეობაში რომელიც უარყოფითად აისახება სახელმწიფოს თავდაცვისუნარიანობაზე.

---

[21] BBC News, Ukraine crisis: Russia halts gas supplies to Kiev, < https://www.bbc.com/news/world-europe-27862849>, [წვდომის თარიღი: 27.07.2019];

[22] საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, კიბერუსაფრთხოება, 01.08.2015-31.12.2015, გვ. 15;

[23] საქართველოში მომხდარ კონფლიქტთან დაკავშირებული ფაქტების დამდგენი დამოუკიდებელი საერთაშორისო მისია, ტომი II, სექტემბერი, 2009, გვ. 256-258;

2014 წელს, რუსეთ-უკრაინის კონფლიქტის დროს[24] განხორციელდა ისეთი კიბერ აქტივობები, როგორიცაა კიბერ შპიონაჟი, ანტისახელმწიფოებრივი და პროპაგანდისტული კამპანიები, კიბერ შეტევები უკრაინული მედიისა და სამთავრობო საიტებზე, NATO-სა და არასამთავრობო ორგანიზაციების საიტებზე.[25]

გარდა ამისა, რუსეთის დაზვერვის მიერ, ინტერნეტში არსებულ მონაცემები გამოიყენებოდა აღმოსავლეთ უკრაინაში განთავსებული უკრაინული სამხედრო შენაერთების ადგილმდებარეობის დასადგენად. აგრეთვე ხდებოდა დეზინფორმაციის გავრცელება ფორუმებზე, სოციალურ ქსელებში და საინფორმაციო სისტემაში. ყოველივე ზემოაღნიშნული ადასტურებს, რომ სახელმწიფოთა შორის საომარი მოქმედებების მიმდინარეობამდე უკრაინის საკომუნიკაციო არხების შესაძლებლობების შესახებ სადაზვერვო ხასიათის ინფორმაციის შეგროვება ხორციელდებოდა.[26]

3. მართლმადიდებლური ეკლესიისადმი დაინტერესება

უკრაინასა და საქართველოში მართლმადიდებლური ეკლესიის დიდი ავტორიტეტიდან და გავლენიდან გამომდინარე, იკვეთება რუსეთის სპეცსამსახურების მზარდი დაინტერესება აღნიშნულ ქვეყნებში მოქმედი მართლმადიდებლური ორგანიზაციებისა და სასულიერო იერარქების მიმართ, რომლებიც რელიგიური ღირსებისა და ეროვნული ტრადიციების დაცვის საბაბით შესაძლოა აქტიურად იქნან გამოყენებული მათი ინტერესებისათვის.[27]

უკრაინის მართლმადიდებელი ეკლესიის კიევის საპატრიარქოს 2019 წლის 6 იანვარს, კონსტანტინოპოლის მსოფლიო პატრიარქ ბართლომეს მიერ გადაეცა ტომოსი -ავტოკეფალიის შესახებ დოკუმენტი, რომელიც კონსტანტინოპოლის მხრიდან უკრაინის ეკლესიის დამოუკიდებლობის ცნობას გულისხმობს. [28]

ამჟამად უკრაინაში სამი მართლმადიდებელი ეკლესიაა: უკრაინის მოსკოვის საპატრიარქოს მართლმადიდებელი ეკლესია, რომელიც რუსეთს ექვემდებარება საბჭოთა კავშირის დაშლის შემდეგაც, უკრაინის კიევის საპატრიარქოს მართლმადიდებელი ეკლესია და უკრაინის ავტოკეფალიური მართლმადიდებელი ეკლესია. [29]

---

[24] Ukraine in Crisis, <https://www.cfr.org/backgrounder/ukraine-crisis>, [წვდომის თარიღი: 29.07.2019];

[25] Col. Kowalik T.K., and Jankowski D.P., Hybrid warfare – a known unknown?, Monday, 04 July 2016. http://neweasterneurope.eu/2016/07/04/hybrid-warfare-a-known-unknown/ [წვდომის თარიღი: 19.07.2019];

[26] U.S. Department of State, Congressional Notification, ICS-CERT, U.S. Department of Homeland Security, "Cyber-Attack Against Ukrainian Critical Infrastructure," < https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01> , February 25, 2016;

[27] კუხალაშვილი დ., „სადაზვერვო და კონტრსადაზვერვო საქმიანობის ორგანიზაცია რელიგიის საფარქვეშ," შსს აკადემიის გამომცემლობა, თბილისი, 2016 წელი, გვ. 87-98;

[28] Bartholomew calls on leaders of autocephalous churches to recognize Orthodox Church of Ukraine Read, https://www.unian.info/politics/10399443-bartholomew-calls-on-leaders-of-autocephalous-churches-to-recognize-orthodox-church-of-ukraine.html, [წვდომის თარიღი: 29.07.2019];

[29]Bentzen N., EU, Ukraine: Religion and (geo-) politics Orthodox split weakens Russia's influence, Religious demography of Ukraine, February 2019, P.3,

უკრაინის მართლმადიდებელი ეკლესიის ავტოკეფალიის საკითხის განხილვის პერიოდში დადგინდა, თუ როგორ ცდილობდნენ რუსი ჰაკერები შეეღწიათ და მოეპოვებინათ საჭირო ინფორმაცია ამერიკელი დემოკრატების, სამხედრო კონტრაქტორებისა და სამხედრო მოსამსახურეების ცოლების, ამერიკული დაზვერვის თანამშრომლებისა და ჟურნალისტების ელექტრონული ფოსტებიდან.[30]

რუსი ჰაკერების მიზანს ასევე წარმოადგენდა მართლმადიდებელი სამყაროს უმაღლეს მღვდელმთავართა პირადი მიმოწერების ფარულად მოპოვება, ამა თუ იმ სასულიერო პირზე სხვადასხვა სახის მაკომპრომეტირებელი მასალების შეგროვება, რათა გავლენა მოეხდინათ მათ პოზიციაზე უკრაინის ავტოკეფალიის საკითხში.[31]

რუსეთის მართლმადიდებელი ეკლესია კატეგორიულად ეწინააღმდეგება უკრაინის მართლმადიდებელი ეკლესიის ავტოკეფალიას და მიიჩნევს, რომ უკრაინა მისი კანონიკური ტერიტორიაა. უკრაინის ეკლესიის დამოუკიდებლობის ცნობა გამოიწვევს რუსეთის სპეცსამსახურების პოზიციების შესუსტებას აღნიშული მიმართულებით, რომელიც სწორედაც რომ ჰიბრიდული ომის წარმოების ინსტრუმენტია, რომლის ჩავარდნაც უკრაინაში რუსეთის სტრატეგიულ ინტერესებს საგრძნობლად ასუსტებს.

დასკვნა

ნაშრომში მოყვანილი ფაქტების განხილვისა და გაანალიზების საფუძველზე შეიძლება ითქვას, რომ იკვეთება ის ძირითადი მიმართულებები, საფრთხეები და რისკ-ფაქტორები, რომლებიც მიესადაგება რუსეთის მიერ წარმოებულ „ჰიბრიდული ომს“ უკრაინასა და საქართველოში, კერძოდ:

- უკრაინისა და საქართველოს წინააღმდეგ ინფორმაციული ომის საწარმოებლად კიბერ ომი, კიბერ ტერორიზმი, ჰაკერული შეტევები და სხვ. მიმართულია კრიტიკული ინფრასტრუქტურის პარალიზებისაკენ, რომელიც ემსახურება სამოქალაქო ან სამხედრო (ან კომბინირებულად ორივე ერთად) სექტორის დაზიანებას, დამთრგუნველი საზოგადოებრივი აზრის ჩამოყალიბებასა და დეზინფორმაციის გავრცელებას, რასაც თან სდევს სადაზვერვო შეღწევადობისათვის ხელსაყრელი პირობებისა და საზოგადოების მიერ ხელისუფლებისადმი უარყოფითი განწყობების, მასობრივი არეულობის, კანონიერი ხელისუფლების დამხობის წინაპირობების შექმნა;

- რუსეთის სპეცსამსახურების მიერ, თავიანთი ე.წ „წარმომადგენლების“ დახმარებით, „ჰიბრიდული ომის“ მიზნებისა და ამოცანების განსახორციელებლად საქართველოსა და უკრაინაში მიმდინარე პოლიტიკურ-ეკონომიკურ პროცესებში ჩართვა, ქვეყნის

<http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635525/EPRS_BRI(2019)635525_EN.pdf> [წვდომის თარიღი: 29.07.2019];

[30] Raphael Satter, Jeff Donn, Desmond Butler, FBI leaves US targets of Russian hackers in the dark, <https://www.apnews.com/eb4df4898e334654a28de14dbfa7ab94> [წვდომის თარიღი: 30.07.2019];

[31] Raphael Satter, Ungodly espionage: Russian hackers targeted Orthodox clergy, <https://www.apnews.com/26815e0d06d348f4b85350e96b78f6a8> [წვდომის თარიღი: 30.07.2019];

სოციალურ-დემოგრაფიული და ეკონომიკური განვითარების დონის შესწავლა და რუსეთისათვის სასარგებლო პროპაგანდის წარმოება მიმდინარეობს;

- რუსეთის მიერ მათ პოლიტიკაზე ორიენტირებული მასმედიის საშუალებების ფორმირება, ფინანსური მხარდაჭერა და მათი მეშვეობით მათთვის სასარგებლო პროპაგანდის წარმოება (ქვეყნის საგარეო და საშინაო პოლიტიკური კურსის დისკრედიტაცია და საკუთარი საგარეო კურსის პოლულარიზაცია, მოსახლეობის იდეოლოგიური დამუშავება, სეპარატისტული იდეების გაჟღერება, ეთნიკურ-რელიგიური შუღლის გაღვივება და სხვ.) მიმდინარეობს, რომელიც მოწინააღმდეგე სახელმწიფოთა მოსახლეობაში რუსეთისთვის ხელსაყრელი განწყობების ჩამოყალიბებას ემსახურება;

- რუსეთის სპეცსამსახურები, თავიანთი ე.წ. „წარმომადგენლების“ დახმარებით, „ჰიბრიდული ომის“ მიზნებისა და ამოცანების განსახორციელებლად უკრაინისა და საქართველოში ეწევიან საკუთარი სახელმწიფოსათვის სასარგებლო პროპაგანდას.

- სადაზვერვო საქმიანობის ფარგლებში, ოპერაციული ქმედებების ნაწილს წარმოადგენს რუსეთის მიერ საქართველოსა და უკრაინის ხელისუფლებაზე ზეგავლენის მოსაპოვებლად ისეთი სადაზვერვო ოპერაციების დაგეგმვა-განხორციელება, როგორებიცაა ემბარგო, ეკონომიკური ბლოკადა, ენერგო რესურსებით მანიპულირება, აღნიშნული ქვეყნების მიერ საკუთარი სახელმწიფოს ინტერესების საზიანო გადაწყვეტილებების მიღების უზრუნველსაყოფად;

- რუსეთის სპეცსამსახურების მიერ საზოგადოებაში მიმდინარეობს პროცესების იმგვარად წარმართვა, რომ შეიქმნას შთაბეჭდილება, თითქოს საქართველო და უკრაინა არ არიან მზად ევრო ინტეგრაციისათვის და აღნიშნული ქვეყნები წარმოაჩინოს არაევროპულ სახელმწიფოდ, სადაც ადამიანის უფლებების ტოტალურად ირღვევა.

ბიბლიოგრაფია

1. Lind W.S., Nightengale K., Schmitt John F., Sutton J., Wilso G.I., The Changing Face of War: Into the Fourth Generation, Marine Corps Gazette, Oct 1989, 22;

2. National Security Decision Directive 108 on “Soviet Camouflage, Concealment and Deception”, The White House, 12 October 1983, https://fas.org/irp/offdocs/nsdd/nsdd-108.pdf [წვდომის თარიღი: 27.07.2019];

3. Max B., “The Evolution of Irregular War: Insurgents and Guerillas from Akkadia to Afghanistan”, Foreign Affairs, 92 (2), 2013, 100-114;

4. საქართველოს თავდაცვის სამინისტრო, კონფერენცია, ჰიბრიდული ომი და მისი გავლენა ნატოს წევრ და პარტნიორ ქვეყნებზე, 27 ოქტომბერი, 2015.

<https://mod.gov.ge/ge/news/read/4266/hibriduli-omi-da-misi-gavlena-natos-cevr-da-partnior-qveknebze>, [წვდომის თარიღი: 27.07.2019].

5. Hoffman, F.G., Hybrid Warfare and Challenges, JFQ / issue 52, 1st quarter 2009, 34;

6. Congressional Research Service, U.S. Sanctions on Russia, January 11, 2019, https://fas.org/sgp/crs/row/R45415.pdf [წვდომის თარიღი: 27.07.2019];

7. Council of the European Union General Secretariat, EU restrictive measures in response to the crisis in Ukraine, 5 September 2018, https://eeas.europa.eu/sites/eeas/files/eu_restrictive_measures_in_response_to_crisis_in_ukraine_en.pdf [წვდომის თარიღი: 27.07.2019];

8. Laurynas Jonavicius, Laure Delcour, Rilka Dragneva, and Kataryna Wolczuk, Russian Interests, Strategies, and Instruments in the Common Neighbourhood, No. 16, March 2019, <http://eu-strat.eu/wp-content/uploads/2019/03/EU-STRAT-Working-Paper-No.-16.pdf>, [წვდომის თარიღი: 27.07.2019];

9. Концепция внешней политики Российской Федерации, 30 ноября 2016 г. <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU> [წვდომის თარიღი: 27.07.2019];

10. European Parliament Resolution „EU Strategy for the Black Sea“, 20 January 2011, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0025+0+DOC+XML+V0//EN [წვდომის თარიღი: 27.07.2019];

11. NATO Parliamentary Assembly Resolution #437 on STability And Security In The Black Sea Region, 09 October 2017, <https://www.nato-pa.int/download-file?filename=sites/default/files/2017-10/2017%20-%20RESOLUTION%20437%20-%20BLACK%20SEA%20-%20SCHMIDT%20%20-%20%20219%20CDS%2017%20E.pdf> [წვდომის თარიღი: 27.07.2019];

12. Robert C., “Top Russian General Lays Bare Putin's Plan for Ukraine”, Huffington Post, 09 February 2014, <https://www.huffpost.com/entry/valery-gerasimov-putin-ukraine_b_5748480> [წვდომის თარიღი: 27.07.2019];

13. The Eastern Partnership (EaP), https://www.euneighbours.eu/en/policy#the-eastern-partnership, [წვდომის თარიღი: 27.07.2019];

14. HRW – Human Rights Watch, World Report 2019 – Ukraine, <https://www.hrw.org/world-report/2019/country-chapters/ukraine> [წვდომის თარიღი: 27.07.2019];

15. MH17: How did the conflict in Ukraine start?, By international correspondent Mark Corcoran, 29 Jul 2014, <https://www.abc.net.au/news/2014-07-29/mh17-how-did-the-conflict-in-ukraine-start/5629990> [წვდომის თარიღი: 18.09.2019];

16. The army of the Lugansk and Donetsk People's Republics has 20,000 fighters – Gubarev, Information Telegraph Agency of Russia. 9 July 2014, <https://tass.com/world/739790>[წვდომის თარიღი: 18.09.2019];

1. საერთაშორისო სამხრეთ კავკასიური მედია ფორუმი თბილისში, <https://euronews.ge/%E1%83%A1%E1%83%90%E1%83%9B%E1%83%AE%E1%83%A0%E1%83%94%E1%83%97%E1%83%99%E1%83%90%E1%83%95%E1%83%99%E1%83%90%E1%83%A1%E1%83%98%E1%83%A3%E1%83%A0%E1%83%98-%E1%83%A1%E1%83%90%E1%83%94%E1%83%A0%E1%83%97/>, 27 ივნისი, 2017, [წვდომის თარიღი: 27.07.2019];

2. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, ოკუპირებული ტერიტორიები, 01.01.2016-31.12.2016, გვ. 4-7;

3. რუსეთის ხისტი და რბილი ძალის საფრთხეები საქართველოში, ევროპული ინიციატივა – ლიბერალური აკადემია, თბილისი, 2016 წელი, გვ. 8-14;

4. Office of the United Nations High Commissioner for Human Rights, Situation of human rights in the temporarily occupied Autonomous Republic of Crimea and the city of Sevastopol (Ukraine), P.1-3, <https://www.ohchr.org/Documents/Countries/UA/Crimea2014_2017_EN.pdf>, [წვდომის თარიღი: 27.07.2019];

5. საქართველოს მთავრობის განკარგულება №1740, სამოქალაქო თანასწორობისა და ინტეგრაციის სახელმწიფოს ტრატეგიისა და 2015-2020 წწ. სამოქმედო გეგმის დამტკიცების შესახებ, 2015 წლის 17 აგვისტო ქ. თბილისი;

6. ეთნოსთა შორის ოთანამშრომლობისა და კონსულტაციების ანალიტიკური ცენტრი, საქართველოში ეთნიკური უმცირესობათა სათემო ორგანიზაციების საჭიროებების შეფასება, რედ. ალეკსანდრა დელემენჩუკი, თბილისი, 2012, გვ. 9-17;

7. კუხალაშვილი დ., „სადაზვერვო და კონტრსადაზვერვო საქმიანობის ორგანიზაცია რელიგიის საფარქვეშ,“ შსს აკადემიის გამომცემლობა, თბილისი, 2016 წელი, გვ. 87-90;

8. Radin A., Rach C., Russian Views of the International Order, Published by the RAND Corporation, Santa Monica, Calif, 2017, P. 79, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1800/RR1826/RAND_RR1826.pdf [წვდომის თარიღი: 27.07.2019];

9. BBC News, Ukraine crisis: Russia halts gas supplies to Kiev, < https://www.bbc.com/news/world-europe-27862849>, [წვდომის თარიღი: 27.07.2019];

10. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, კიბერუსაფრთხოება, 01.08.2015-31.12.2015, გვ. 15;

11. საქართველოში მომხდარ კონფლიქტთან დაკავშირებული ფაქტების დამდგენი დამოუკიდებელი საერთაშორისო მისია, ტომი II, სექტემბერი, 2009, გვ. 256-258;

12. Ukraine in Crisis, <https://www.cfr.org/backgrounder/ukraine-crisis>, [წვდომის თარიღი: 29.07.2019];

13. Col. Kowalik T.K., and Jankowski D.P., Hybrid warfare – a known unknown?, Monday, 04 July 2016. http://neweasterneurope.eu/2016/07/04/hybrid-warfare-a-known-unknown/ [წვდომის თარიღი: 19.07.2019];

14. U.S. Department of State, Congressional Notification, ICS-CERT, U.S. Department of Homeland Security, "Cyber-Attack Against Ukrainian Critical Infrastructure," < https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01> , February 25, 2016;

15. კუხალაშვილი დ., „სადაზვერვო და კონტრსადაზვერვო საქმიანობის ორგანიზაცია რელიგიის საფარქვეშ," შსს აკადემიის გამომცემლობა, თბილისი, 2016 წელი, გვ. 87-98;

16. Bartholomew calls on leaders of autocephalous churches to recognize Orthodox Church of Ukraine Read, https://www.unian.info/politics/10399443-bartholomew-calls-on-leaders-of-autocephalous-churches-to-recognize-orthodox-church-of-ukraine.html, [წვდომის თარიღი: 29.07.2019];

17. Bentzen N., EU, Ukraine: Religion and (geo-) politics Orthodox split weakens Russia's influence, Religious demography of Ukraine, February 2019, P.3, <http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635525/EPRS_BRI(2019)635525_EN.pdf> [წვდომის თარიღი: 29.07.2019];

18. Герасимов В., „Новые вызовы требуют переосмыслить формы и способы ведения боевых действий,Опубликовано в выпуске № 8 (476), за 27 февраля, 2013 года <http://www.vpk-news.ru/articles/14632>, [ბოლო განალების თარიღი: 29.07.2019];

19. Antonenko A., Bambals R., Bērziņš J., Bond I.,Cepurītis M., Dobrokhotov R., Kažociņš J., Kudors A., Liuhto K., Nitsovych R., Pabriks A., Pavlenko O., The War in Ukraine: Lessons for Europe, The Centre for East European Policy, Studies University of Latvia Press Rīga, 2015, P. 44;

20. Raphael Satter, Jeff Donn, Desmond Butler, FBI leaves US targets of Russian hackers in the dark, <https://www.apnews.com/eb4df4898e334654a28de14dbfa7ab94> [წვდომის თარიღი: 30.07.2019];

21. Raphael Satter, Ungodly espionage: Russian hackers targeted Orthodox clergy, <https://www.apnews.com/26815e0d06d348f4b85350e96b78f6a8> [წვდომის თარიღი: 30.07.2019];