A Model of the Application of IoT Devices Based on RFID to Ensure the Safety of the Military and Civilian Population under War Conditions

Myroslava Gladka [1], Alexander Kuchansky [1], Mykola Kostikov [1,2] and Rostyslav Lisnevskyi [1]

[1] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska Str., Kyiv, 01033, Ukraine*
[2] *National University of Food Technologies, 68 Volodymyrska Str., Kyiv, 01601, Ukraine*

Abstract

IoT devices using radio-frequency identification (RFID) systems are becoming more popular in many fields where clear identification and affiliation of a specific person to a specific activity is important. These are various branches of industry, banking, the economic sector, medicine, etc.

However, creating and using an IoT model for the protection and security of the military and civilian population in wartime has not yet gained widespread use. It is in the conditions of combat actions, where there is a need to identify each person, and their movement within the scope of military operations, conducting or participating in evacuation procedures, involvement in various types of military or humanitarian missions, prompt provision of medical assistance, etc. In all these situations, issues of identification are of vital importance, because not only security but also the lives of the military and civilian population may depend on it.

The purpose of this study is to investigate the features and prove the advantages of applying an IoT model based on RFID in the conditions of martial law to ensure the safety of the health and life of the military and the civilian population. The paper considers the use of RFID tags to ensure the safety of movement, and personal identification for those who need medical assistance or are in danger on the territory of combat operations or occupied territories.

Keywords [1]

IoT, model, RFID, identification, war, military, civilian population, protection, safety, security

1. Introduction

In the conditions of conducting military operations, there arises an urgent need for personal identification of military personnel, medics, volunteers, civilians, etc. Personal identification is the mechanism that enables the implementation of movement control mechanisms to ensure the security of the military and civilian population; prompt provision of medical care in accordance with the personal data of the injured; movement adjustments in evacuation missions; assisting victims in accordance with the territorial availability of medical workers.

Modern trends in managing the movement of military personnel, medics, volunteers, and the civilian population under martial law have a common problem – increasing the risks for movement due to the lack of up-to-date coordination depending on the current state of threats [1, 2]. Another important component of personal identification is the ability to obtain up-to-date information when there is a need to provide decent medical assistance to people in the combat zone [3].

IoT devices are widespread in all areas of human life. Therefore, using such technology for protecting the military and the civilian population under war conditions is of vital importance. One of

Information Technology and Implementation (IT&I-2022), November 30 – December 02, 2022, Kyiv, Ukraine
EMAIL: gladkam@fit.knu.ua (A. 1); kuchansky@knu.ua (A. 2); kostikov@knu.ua (A. 3); lisnevskyir@fit.knu.ua (A. 4)
ORCID: 0000-0001-5233-2021 (A. 1); 0000-0003-1277-8031 (A. 2); 0000-0002-1569-8179 (A. 3); 0000-0002-9006-6366 (A. 4)

the approaches to using IoT for protection may be creating a model using radio frequency identification (RFID) – a wireless technology that implements a mechanism capable of automatic and unambiguous identification of objects that can be out of sight. It is achieved by extracting a unique identifier from microelectronic tags attached to objects [4].

RFID is a technology for object identification and tracking that uses radio waves to transmit data. A special reader gets the data from an electronic label (RFID tag) attached to the object [5]. With the help of an IoT model based on RFID, we can track and monitor the movements of people. Data can be collected in real-time and be immediately available for military, humanitarian or volunteer missions, providing medical care, which increases security and minimizes travel time thanks to RFID.

Data can be collected in real-time and have live access thanks to RFID. Response teams in command posts, medics, humanitarian missions managers, and other people involved in solving problems under martial law can access the data of subjects who own an RFID tag via a computer database [6]. The lack of up-to-date information about a person in need of medical assistance can significantly reduce the level of such assistance or even cause harm. The inability to promptly manage the movement of people in areas of increased danger can have disastrous consequences for the life and health of such people. The use of modern information technologies, software, and hardware in the territories of active combats, where there is a constant threat to the life and health of military personnel or other people, stimulates the use of all available algorithms and mechanisms in IT, as well as the development new ones [7]. It is the technologies that will reduce the possible risks of people who are in the combat areas, through the optimization of communications, prompt access to information, assistance in decision-making, etc., that should have a prominent place in the current conditions of our and other countries suffering from war.

2. Methods for Solving the Problem

A model of an IoT system using RFID is a complex of hardware and software. Its basic elements are tags attached to objects that need to be identified. There may be name tags for military personnel, medics, and volunteers, or individual tags for the civilian population that can be fixed on a person's identity card or other belongings. Each such tag has an internal memory sufficient to record a limited amount of data. This memory may be read-only for use in name tags, or rewritable if the tags are used for variable subjects, such as civilians undergoing evacuation. Accordingly, recording in such memory is carried out once or repeatedly with the help of special software [8].

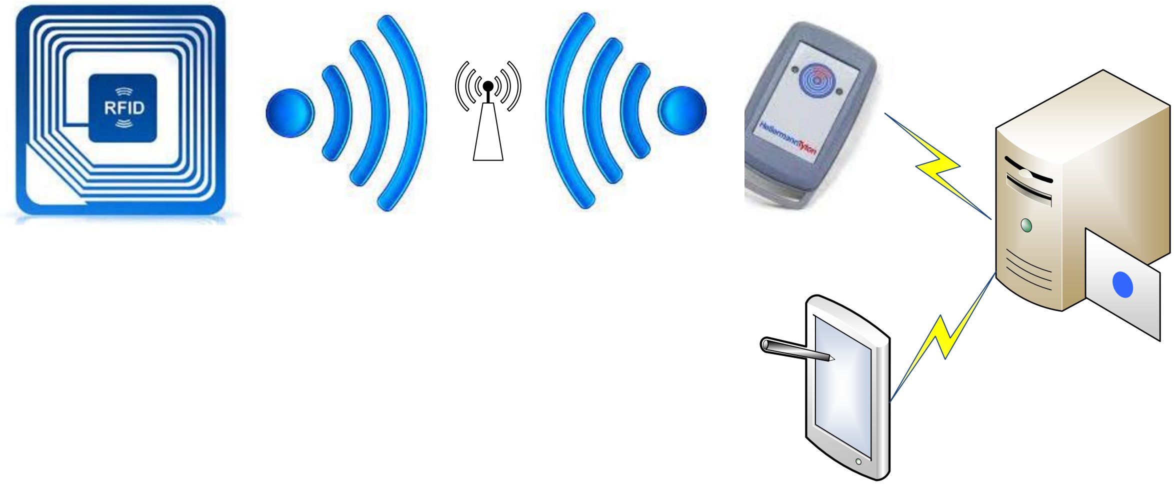

Figure 1: Work scheme of an IoT model based on RFID

The memory of each RFID tag stores information about the subject as a unique identifier, such as date of birth, personal number, etc. To receive stored data, the RFID reader generates magnetic fields that search for all RFID tags placed within its range. High-frequency electromagnetic energy generated in the process of creating a request activates tags to receive a response from the RFID memory [9]. Depending on the speed of changes in the information flow, such requests can be updated up to 50 times per second [10]. When the reader receives an RFID response from the RFID tag, a connection is created to receive data. Further, the data is sent to data processing servers and the results can be returned to any convenient mobile device for making necessary decisions [11] (Fig. 1).

2.1. RFID System Structure

An RFID system includes a set of elements united by a single radio frequency communication algorithm for the exchange of information flows. The system constantly monitors the presence of RFID tags in the range of the RFID scanner for further processing depending on the given work scenarios [12]. The RFID system may include the following elements (Fig. 1):

- The tag which is placed on the subject and has a unique identification;
- Antenna – activates the magnetic field intended for data transmission between the tag and the reader; depending on the antenna power, the area of operation of the RFID tag detector can be expanded;
- Reader – for reading information from RFID tags;
- Communication infrastructure – for data exchange between readers, the database, and other smart devices that receive a response from the database;
- Database – contains all the necessary information about subjects related to a specific identifier recorded in the RFID tag;
- Software – an information system with a convenient user interface for receiving and processing information obtained from the database via RFID tags. Such programs can be implemented to work with both the web interface and mobile applications.

2.2. RFID tags

RFID tags are small objects consisting of a microcircuit – a chip and an antenna [13] (Fig. 2). The microcircuit includes a receiver, a transmitter, and a memory block for data storage. The composition of active RFID tags can also include a power element. Passive tags receive power from the radio signal of the reader's antenna. The main difference between active and passive tags is their range of action, in active tags this range can be several times greater.After receiving a signal from the RFID reader, the tag activates a response in the form of a signal containing identification information [14].

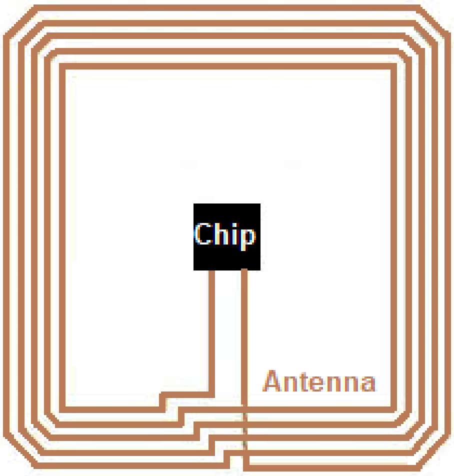

Figure 2: RFID tag

The following types of RFID tags can be used to implement military missions [15]:

- R/O (Read Only) – the data is recorded at the tag manufacturing stage, and is immutable. Such tag should be used on military weapons and equipment;
- WORM (Write Once Read Many) – tags for one-time recording and multiple reading. No data is entered on such tag during the production process. The information is recorded by the user

once, and then it can be read multiple times. Such tags should be used to identify military personnel or other people involved in military operations;

- R/W (Read/Write) – rewritable tags that can be written and read multiple times. Such tags may be used for subjects undergoing evacuation.

The key factor in the RFID tag radius range is the design of the antenna, which must take into account the following parameters: resistance to radiation, bandwidth, and efficiency. Meanwhile, RFID antennas are tuned to resonate only in a narrow range of radio frequencies that work according to the rules defined by RFID [16]. The RFID antenna spreads the wave in horizontal and vertical dimensions. For the identification of subjects in war conditions, it becomes necessary to spread the wave at an angle, which causes a loss of signal strength, so the question of increasing the power of the antenna arises. An increase in antenna power is achieved by increasing its area, and using special materials for its manufacture [17, 18]. Increasing the range of the RFID tag antenna can be achieved by increasing the turns [19] (Fig. 3).

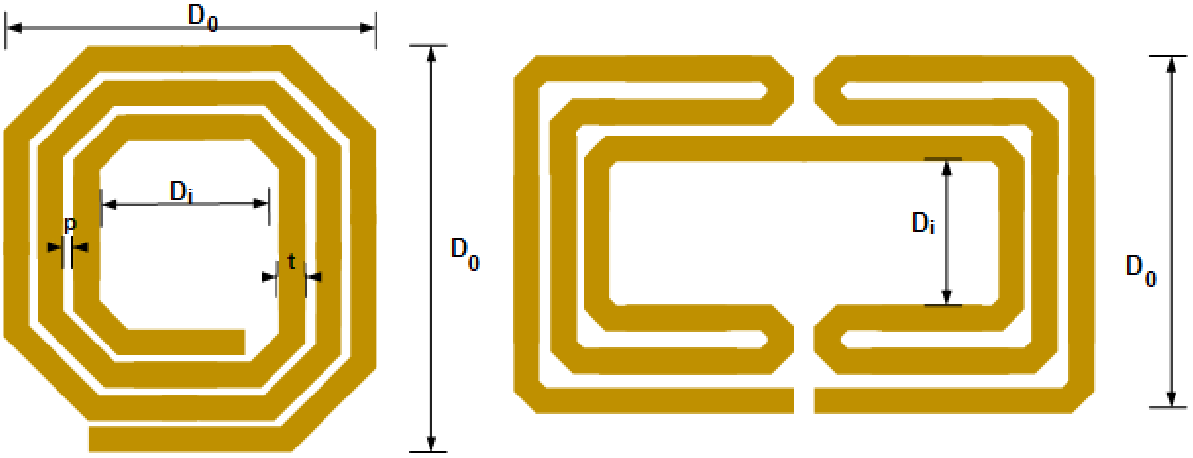

Figure 3: Representation of the RFID tag multi-turn antenna

To calculate the antenna power, it is necessary to take into account the width of the lines of turns *t* and the material from which they are made, the number of turns *i* increasing their size from the inner to the outer turn. Then the power of each *i*-th turn of the antenna can be written as

$$P_i = I^2 R_i \tag{1}$$

where *I* is the current, and R_i is the resistance on the i-th turn.

To determine the magneto-inductive losses on each turn *i*, it is necessary to take into account the size of each turn *D* (length and width), the total number of turns *n*, the resistance of the base where the antenna is located μ, the conductivity of the material ρ and the thickness of the antenna tape *t*. [5, 20]:

$$Q = \mu\rho t \frac{D_i^2}{P_i}(i-n)I \tag{2}$$

By making calculations, you can get an antenna of such power that will be necessary for use in the conditions of warfare. Of course, the complexity of the design and the use of materials with higher conductivity increases the cost of the antenna, but life and health safety are important factors in increasing the cost of development [6].

2.3. Advantages of Creating and Using an IoT Model Based on RFID

In information technologies, there are quite a lot of identification mechanisms: optical identifiers (barcodes, QR codes), biometrics (fingerprints, face recognition, voice identification), etc. [21]. However, in the time of combat actions, it may be necessary to recognize a person who needs medical intervention, has a psychological shock, and does not respond to external factors. In such cases, biometric identifiers may not work. Therefore the use of identifiers that do not depend on the state of the person is quite critical. The proposed IoT model uses RFID tags that have a fairly small size but can store a large amount of information. Thanks to this, such tags can be placed in the individual tokens of military personnel or other people involved in military operations. This will allow additionally protect the identifier from the influence of external factors. It will also ensure the durability of the tag, which is impossible to implement for graphic identifiers.

It is reasonable to use rewritable RFID tags in personal protection systems (helmets, armored vests) for people undergoing evacuation from the zone of combat actions. After the successful completion of the operation, the data is erased, and the tags are prepared for recording the data of people from the next mission [8]. The reuse of RFID tags with other information is easily implemented by the rewriting mechanism. Readers can simultaneously receive information from a large number of tags, thanks to the implemented anti-collision mechanism.

Hidden tags can only be recognized if information about their placement is available. Additionally, the data recorded on the tag can be protected by a password or identified only by a trust system, to which only specific people involved in military operations have access [9].

2.4. Standards in Radio-Frequency Identification

Among the current ISO standards, there are separate sections regulating tracking system standards (ISO 11784, ISO 11785), standards for identifying RFID tags (ISO 10536, ISO 14443, ISO 15693), standards for RFID AIDC and control technologies (ISO 15961, ISO 15962, ISO 15963, ISO 18001). The ISO 18000 standard is used to control the elements of RFID systems. It regulates the use of common communication protocols in accordance with the norms of international use of RFID. This standard covers the entire spectrum of the RFID frequency range (LF, HF, UHF, and microwaves). The specifications of this standard are presented in seven parts (Table 1) [22].

Table 1
Parts of the ISO/IEC 18000 standard "Information technology — Radio frequency identification for item management"

Part	Name
Part 1	Reference architecture and definition of parameters to be standardized
Part 2	Parameters for air interface communications below 135 kHz
Part 3	Parameters for air interface communications at 13,56 MHz
Part 4	Parameters for air interface communications at 2,45 GHz
Part 5	Parameters for Air Interface Communications at 5.8 GHz
Part 6	Parameters for air interface communications at 860 MHz to 960 MHz
Part 7	Parameters for active air interface communications at 433 MHz

The current EPC Gen 2 standard has more advanced functionality for UHF-RFID operation, which allows for even distribution between different RFIDs. This standard provides an option of "tag destruction" for additional protection against unauthorized reading when there is a need to protect the subject that owns the RFID tag and ensure its privacy [23].

3. Practical Implementation

Modern wars are wars of technology and equipment. The paths of troop movement, the equipment locations, and the conduct of military operations are constantly tracked. In such conditions, there is a need to accurately and promptly determine the position of subjects with RFID tags, therefore it is appropriate to use a real-time locating system [24].

3.1. A Model of an IoT Real-Time Locating System (RTLS) for RFID Tag Detection

A real-time locating System (RTLS) is an IoT system that implements identification with the determination of location and exact coordinates according to the territory plan within the monitoring zone [25]. An IoT model using RTLS makes it possible to get and process information about the subject location: monitor the movement of people in evacuation missions, monitor military operations, search for the wounded and dead, and organize rescue missions by teams that have the closest location to the affected subjects. Thanks to the introduction of RTLS into the IoT model, the received information about military operations can be coordinated in real time according to the current state of threats and dangers [25]. Another key advantage of RTLS with the characteristic accuracy of ultrasonic positioning is the possibility of mining territories with the accuracy of laying routes up to ten centimeters [25].

Locating accuracy depends both on the quality of the radio frequency signal from the tag and on the influence of interference, as well as the number of responses to the signal (print fading), so these characteristics must be taken into account when designing RFID tags (antenna power, antenna material, type of microprocessor, type of tag). The polling frequency to obtain real-time locating should be based on the speed of movement of the subjects. Accordingly, the higher the speed of movement, the more frequent the survey should be so that the accuracy of the indicators is sufficiently high [25]. To determine coordinates more accurately, each active tag can interact with several readers in fixed locations at the same time. From this data, the locating of the RFID tag is calculated. Such coordinate calculations can be based on key locating algorithms: trilateration or multilateration (based on measuring the distances from the readers to the tag), and triangulation (based on measuring the direction angles from the readers to the tag). When making such calculations, it is necessary to take into account the map of the area: the location of buildings, the presence of plantations, additional permanent and variable obstacles, and interferences [25].

When organizing the control of identifiable entities on the territory controlled by the RTLS infrastructure, packets are exchanged between RFID tags and software. Thanks to this tracking, it is possible to create maps of military movements, and execution of military or other operations. If it is necessary to receive help for the wounded or search for the dead, we can identify the precise location of the subject. To perform missions, medical workers must synchronize the location of individual teams that are closest to the victims. When carrying out humanitarian and evacuation missions, we should monitor deviations from routes, the trajectory of movement, violation of traffic columns in convoys, speed of movement, etc.

3.2. Radio Frequency Identification Range

The main feature of military operations is a large territory, therefore, when choosing an environment for data exchange, you need to take this factor into account. The use of RFID systems in ultra-high-frequency mode – Microwave (from 2.45 GHz) may be recommended in this case. The range of such tags can be from 300 meters to several kilometers while maintaining a fairly high reading speed. Of course, when accounting for military weapons and equipment, you can use low-frequency tags, which will be much cheaper to develop and use. But the emphasis of our work is precisely on the development of mechanisms for the identification of military personnel and other people in the combat zone [7].

To ensure the operation of high-frequency identification for the safety of military personnel and other people in the conditions of martial law, it is advisable to use communication devices with a long-field strategy implemented in a UHF-RFID reader. A feature of UHF-RFID is work with standard tags with a large reading range and the possibility of limiting the electric field. This allows you to distinguish between the reading range and the types of tags that are scanned. Thanks to this, it is possible to perform various tasks of locating and identifying certain subjects.

To increase the operating range, it is necessary to use antennas with a wave loop, a traveling wave, which is faster in space [26]. To analyze lossless range scanning in a one-dimensional metamaterial structure *M*, we determine the parameter λ, which corresponds to the phase constant value of the signal passing through this structure, the radio frequency signal propagating in space – l_0, l_x, *and* l_y – its projection in the *x* and *y* planes (Fig. 3). Depending on the method of developing the structure of the metamaterial *M*, it is possible to adjust the wave λ by adjusting the effective dielectric permittivity ρ and magnetic permeability φ of the metamaterial *M* [27]. The range of the identifier l_0 directly depends on the environment surrounding the metamaterial structure. Therefore, the more obstructions and obstacles in the way of the identifier's actions, the more the reading range is reduced [28]. The ideal environment is air when there are no more restraining factors in the obstacle. Then to ensure the continuous interconnection of RFID elements at the boundary of the distribution of the metamaterial structure and the environment, the vectors λ and l_0 must coincide. Then the ratio between the values of the vectors λ and l can be determined from the standard distribution

$$l_0^2 = l_x^2 + l_y^2 = \lambda^2 + \lambda_0^2 \tag{3}$$

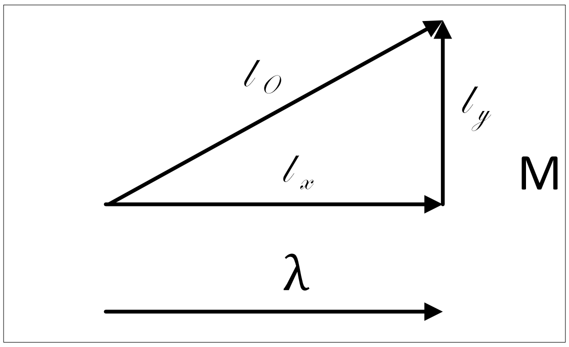

Figure 4: Representation of the wave signal *λ* passing through the metamaterial *M* and propagating in the space *l₀, lₓ, l_y*.

Therefore:

$$l_y = \sqrt{l_0^2 + \lambda^2} \tag{4}$$

If conditions are created in the active antenna when it is possible to control the direction of the wave signal λ, then we level the value of l_y , and l_x will correspond to the wavelength. Such conditions can be created for multi-turn antennas, which were discussed above.

We describe the designed communication network for locating subjects as a graph *G*(*V*, *H*) where *V* is a set of vertices – RFID tags and readers, and *H* is a set of arcs operating within the antenna bandwidth. Accordingly, with proper communication between the system devices within the working range, each arc $h \in H$ of graph *G* is characterized by c_h. We denote all the possible paths for connecting tags with readers as *LT* [29].

The logical structure *LS* of the network communication can be presented as:

$$LS = LS(LT, x_t, t \in LT) \tag{5}$$

which is represented by a set of paths for communication of network elements as vertices in graph *G* indicating communication lines x_t in each path.

We present a logical function for any path $t \in LT$ and any arc $h \in H$ as

$$\chi\{t,h\} = \begin{cases} 1, & h \in t \\ 0, & h \notin t \end{cases} \tag{6}$$

The set of requests from readers to RFID tags will be represented by *R*, then the logical structure *LS* that satisfies this set can be presented as

$$\sum_{t \in LT(s_k, r_k)} x_t \geq d_k, \quad k = 1, \ldots, |D| \tag{7}$$

where d_k, $k = 1, \ldots, |D|$ are values of requests between tags and readers s_k, r_k from the set *V*, i.e. $d_k = d_k(s_k, r_k)$.

As mentioned above, when determining the location of RFID tags, there is communication with several readers. Therefore, it is important to analyze the communication between IoT elements in a case when one of the readers fails or there are problems with the signal transmission. In such an unstable situation *NS*, each element $n \in NS$, $r = 1, \ldots, |NS|$, may be an element of the list of components $q(r)$ – arcs $h_{i1} \ldots h_{iq(r)}$ that failed in an unstable situation *r*.

In such situations, a set of communications between readers and tags $h \in LT$ in a logical structure $LS(q_r)$ will be

$$LT(q_r) = \bigcup_{i,j \in V, i \neq j} LT(i,j,q_r) \tag{8}$$

$$\chi\{h,q_r\} = \min\left(\sum_{j=1}^{q_r} \chi\{h,x_{i_j}\},1\right) \tag{9}$$

Accordingly, the failure of any IoT element for identification increases the risks in data transfer and proper communication between devices which reduces the accuracy of locating the tags.

4. Result

In the conditions of warfare, IoT systems using RFID technology can be used for the following purposes: tracking the progress of military missions, managing the movement of soldiers and medics, coordinating the movement of evacuation convoys, and monitoring and checking the identification data of subjects. Each of these characteristics provides the main values of humanity: the life and health of individuals due to prompt adjustments of movement, or the ability to receive/provide medical assistance to the injured [30].

RFID in IoT is used to track movement and relocations on the territory of combat actions. Due to such tracking, it is possible to monitor and control the location of subjects on the terrain in real-time in the area of operation of the readers, to coordinate their movement based on operational intelligence data on the state and actions of the enemy, which increases security.

It is possible to identify subjects in danger outside the range of readers with the help of drones equipped with special readers. Based on the received data, we can create rescue battalions, and organize medical assistance. When using RFID tags in IoT, it is possible to identify the subject and obtain its individual data (blood group and Rh factor, indications and contraindications, chronic diseases, etc.), which significantly increases the quality and efficiency of providing medical care.

Of course, the use of RFID in IoT systems can be used in various areas, e.g. for checking the availability of equipment and weapons, which must be inventoried, accounted for, and controlled [31]. The use of RFID tags for the identification of mines allows the development of maps of minefields to create mined areas safe for military personnel equipped with appropriate readers.

There is an obstacle to the high-quality work of IoT systems based on RFID technology which is the enemy's use of electronic warfare (EW), radio-electronic suppression, and radio-electronic reconnaissance. Those methods are used in military operations by our enemies, in particular, such EW systems as Borisoglebsk-2, the UAV Shipovnik-Aero, the satellite EW complex "Tirada", and others [32]. However, RFID tags, depending on their purpose, work at frequencies that are not prioritized for suppression by EW systems, but work in case of muted signals of command communication points, signals of cellular networks, Wi-Fi, WiMAX, and DECT networks. Individual stations, such as "Station R-934B", carry out automatic search and analysis of emitted signals, and detect coordinates of aviation UHF radio communication and tactical aviation guidance systems in the range of 100–150 MHz and 220–400 MHz. Accordingly, the use of RFID tags and readers in the range over 2.45 GHz defines them as an additional advantage in a military campaign.

All factors of the use of RFID in IoT systems contribute to increasing the safety of military personnel and the civilian population, the quality, and efficiency of receiving assistance (medical, coordination), and improving the operations of military, medical and humanitarian missions.

5. Conclusions

According to the results of the conducted research, it can be concluded that tags operating in the ultra-high frequency range are the most promising today for improving the security and protection of the military and other people in the area of combat actions. For the development of RFID tag antennas, it is necessary to use highly conductive materials with low resistance for an increased range antenna, which will provide coverage of large areas of identification and real-time locating.

The introduction of the model of IoT systems based on RFID for military campaigns increases the accuracy of task performance due to the monitoring and coordination of movements according to the change in the state of the troops [33, 34]. Synchronization of RFID with modern military navigation systems will improve the conduct of military campaigns [35].

Search and identification of the dead and wounded based on RFID ensures the precise locating of the subject. If the provision of medical assistance is necessary, it eliminates the issue of medical contraindications to treatment based on the received identification data, which will significantly reduce the risks associated with the administration of medications.

An obstacle to the implementation of RFID for the identification of the military and other people in the combat zone is the cost of implementation, since long-range RFID tags have a higher manufacturing cost compared to short-range ones; and the insufficient budget for the army, the complexity of systems and technologies may be an additional restraining factor.

6. References

[1] Military Doctrine of Ukraine, in: Presidential Bulletin, 2004, vol. 14.

[2] About the internal and external situation of Ukraine in 2015, National Institute for Strategic Studies, Kyiv, 2015, 684 p.

[3] V. Nikiforenko, A. Vikhtiuk, Main threats to the national security of Ukraine on the state border and trends in their development, in: Collection of scientific works of the National Academy of the State Border Guard Service of Ukraine, series: Military and Technical Sciences, 2021, vol. 85, no. 2–3, pp. 202–221.

[4] S. Ajami, A. Rajabzadeh, Radio Frequency Identification (RFID) technology and patient safety, in: J Res Med Sci., 2013 Sep, 18(9):809-13. PMID: 24381626. PMCID: PMC3872592.

[5] Y. Wu, D. C. Ranasinghe, Q. Z. Sheng, S. Zeadally, J. Yu, RFID enabled traceability networks: a survey, in: Distributed and Parallel Databases, 2011, 29:397–443.

[6] J. Landt, The history of RFID, in: IEEE Potentials, New York, NY, 2005, 24(4):8–11. DOI: 10.1109/MP.2005.1549751.

[7] M. Shport, Procedure of building a wave algorithm mask in order to find rational routes while solving the emergency service tasks of the State Border Guard Service of Ukraine, in: Scientific Works of Vinnytsia National Technical University, 2014, no. 2, 4 p.

[8] D. W. Bates, A. A. Gawande. Improving safety with information technology, in: N Engl J Med., 2003, 348:2526–34.

[9] K. Finkenzeller, RFID Handbook, Radio-Frequency Identification Fundamentals and Applications, Wiley, New York, NY, USA, 2nd edition, 2004.

[10] F. J. Herraiz-Martínez, F. Paredes, G. Zamora, F. Martín, J. Bonache, Printed magnetoinductive-wave (MIW) delay lines for chipless RFID applications, in: IEEE Transactions on antennas and propagation, 2012, vol. 60, no. 11, pp. 5075–5082.

[11] B. Glover, H. Bhatt, RFID Essentials, O'Reilly, Sebastopol, Calif, USA, 2006.

[12] H. Xu, A. Kuchansky, M. Gladka, Development of individually-oriented method of selection of scientific activity subjects for scientific projects implementation based on scientometric analysis, in: East.-Eur. J. Enterp. Technol., 2021, 6(3(114)), 93–100. DOI: https://doi.org/10.15587/1729-4061.2021.248040.

[13] A. N. Nambiar, RFID technology: A review of its applications, in: Proceeding of the World Congress on Engineering and Computer Science Oct. 20–22, San Francisco, USA, 2009.

[14] K. Ahsan, H. Shah, P. Kingston, RFID applications: An introductory and exploratory study, in: IJCSI Int J Comput Sci Issues, 2010, 7:1–7.

[15] N. C. Karmakar, Handbook of Smart Antennas for RFID Systems, John Wiley and Sons, NJ, 2010, 218 p.

[16] X. Qing, C. K. Goh, Z. N. Chen, Segmented loop antenna for UHF near-field RFID applications, in: Electronics Letters, 2009, vol. 45, no. 17, pp. 872–873.

[17] X. Z. Lai, Z. M. Xie, Q. Q. Xie, J. W. Chao, A Srr-based near field RFID antenna, in: Progress in Electromagnetics Research C, 2012, vol. 33, pp. 133–144.

[18] C. F. Huang, Y. F. Huang, Design of RFID reader antenna for exclusively reading single one in tag assembling production, in: Int J Antennas Propag, 2012, vol. 2012, Article ID 162684, 5 p.

[19] B. Shrestha, A. Elsherbeni, L. Ukkonen, UHF RFID reader antenna for near-field and far-field operations, in: IEEE Antennas and Wireless Propagation Letters, 2011, vol. 10, pp. 1274–1277.

[20] Z. Xing, L. Wang, C. Wu, J. Li, M. Zhang, Characteristics and application of a novel loop antenna to UHF RFID receivers, in: Int J Antennas Propag, 2011, vol. 2011, Article ID 480717, 7 p.

[21] R. Boyko, D. Shumyhai, M. Gladka. Concept, Definition and Use of an Agent in the Multi-agent Information Management Systems at the Objects of Various Nature. Recent Advances in Systems, Control and Information Technology, in: Proceedings of the International Conference SCIT 2016, May 20–21, 2016, Warsaw, Poland, pp. 59–63. Series ISSN: 2194-5357. DOI: https://doi.org/10.1007/978-3-319-48923-0.

[22] ISO/IEC 18000 Information technology — Radio frequency identification for item management, 2004. URL: https://iso.org.

[23] P. V. Nikitin, K. V. S. Rao, S. Lazar, An overview of near field UHF RFID, in: Proceedings of the IEEE International Conference on RFID, Grapevine, Tex, USA, March 2007, pp. 166–174.

[24] S. Ajami, R. Arab-Chadegani, What are the most important barriers to implement Radio Frequency Identification Device (RFID) in healthcare system?, in: J Inform Tech Soft Eng., 2013, S7:e004.

[25] J. Slovák, M. Melicher, M. Šimovec, J. Vachálek, Vision and RTLS Safety Implementation in an Experimental Human—Robot Collaboration Scenario. Sensors, 2021, 21(7):2419. DOI: https://doi.org/10.3390/s21072419.

[26] G. Z. González, Radio Frequency Identification (RFID) Tags and Reader Antennas Based on Conjugate Matching and Metamaterial Concepts, Bellaterra (Cerdanyola del Vallès), July 2013, 130 p.

[27] T. Kokkinos, C. D. Sarris, G. V. Eleftheriades, Periodic FDTD analysis of leaky-wave structures and applications to the analysis of negativerefractive-index leaky-wave antennas, in: IEEE Trans. Microw. Theory Tech., Jun. 2006, vol. 54, no. 4, pp. 1619–1630.

[28] G. Zamora, S. Zuffanelli, F. Paredes, F. J. Herraiz-Martinez, F. Martín, J. Bonache, Fundamental mode leaky-wave antenna (LWA) using slot line and split-ring-resonator (SRR) based metamaterial, in: IEEE Antennas and Wireless Propagation Letters, May 2013, vol. 12, pp. 1424–1427. DOI: 10.1109/LAWP.2013.2287525.

[29] N. Shor, I. Serhiienko [et al.], Problems of optimal design of reliable networks, Naukova Dumka, Kyiv, 2005, 230 p.

[30] S. Ajami, B. Akbari, M. H. Yarmohammadian, M. Hejazi, Evaluation Usage of “Radio Frequency Identification” in Earthquake's victims tracking Information Management System through viewpoint of Relief Experts, Isfahan, Iran: Isfahan University of Medical Sciences; 2012.

[31] M. Gladka, O. Kravchenko, Y. Hladkyi, S. Borashova, Qualification and appointment of staff for project work in implementing IT systems under conditions of uncertainty, in: 2021 IEEE International Conference on Smart Information Systems and Technologies. Astana IT University. Nur-Sultan, Kazakhstan, April 28–30, 2021. DOI: 10.1109/SIST50301.2021.9465897

[32] B. Prykhodko. How to determine the radio electronic warfare and intelligence systems of the Russian Federation – photos and characteristics of the occupiers' equipment, 2022. URL: https://ukraine.segodnya.ua/ua/ukraine/kak-opredelit-sistemy-radioelektronnoy-borby-i-razvedki-rf-foto-i-harakteristika-tehniki-okkupantov-1608046.html.

[33] E. Bergeret, J. Gaubert, P. Pannier, J. M. Gaultier, Modeling an design of CMOS UHF voltage multiplier for RFID in a EEPROM compatible process, in: IEEE Trans. Circuits and Systems, Oct. 2007, vol. 54, no. 10, pp. 833–837.

[34] M. Gladka, A. Kuchansky, R. Lisnevskyi, Teams formation for IT projects implementation on the basis of the model of limited rationality, in: Management of Development of Complex Systems, 2021, vol. 48, pp. 17–23. DOI: 10.32347/2412-9933.2021.48.17-23

[35] R. Lisnevskyi, M. Kostikov, M. Gladka, Analysis of integrations of software tools for project management and their use for the needs of the Armed Forces of Ukraine, in: Collection of the Scientific Papers of the Centre for Military and Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskyi, 2020, vol. 3(70), pp. 107–112. ISSN 2304–2699.

[36] Y. Hladkyi, M. Gladka, M. Kostikov, R. Lisnevskyi, An IoT Solution: A Fitness Trainer, in: CEUR Workshop Proceedings, 2021, 3179, pp. 215–226.

[37] M. Shport, Consideration of supply of radio communication while constructing rational routes in the process of solving of tasks of operation and service activity of the State Border Guard Service of Ukraine, in: Collection of scientific works of the National Academy of the State Border Guard Service of Ukraine, series: Military and Technical Sciences, 2013, vol. 59, no. 1, pp. 312–320.