УДК 004

INFORMATION SECURITY OF GLONASS-BASED AUTOMATED NAVIGATION SYSTEMS FOR GROUND TRANSPORTATION MONITORING AND SUPERVISORY CONTROL

Статья поступила в редакцию 13.08.2014, в окончательном варианте 03.09.2014.

Pavel Viktorovich Botvinkin, postgraduate student, Volgograd State Technical University, 28 Lenin av., Volgograd, 400005, Russian Federation, e-mail: pavel.botvinkin@gmail.com

In developed countries the creation and usage of satellite navigation systems for ground transportation monitoring has been helping to solve various problems for a long time, whereas in Russia similar systems based on GLONASS have been introduced relatively recently. Satellite monitoring is widely used to supervise ground transportation for solving logistical tasks, control of passenger and cargo traffic, optimization of courier services, providing the safety of passenger and freight transportation. Attackers in the case of gaining access to a system with read-permissions can illegally obtain information about the location of monitored objects. If attackers can access with write-permissions, they can affect the data in the system, intercepting or sending false data. Both of these options may entail serious negative consequences, and even cause casualties. Currently, the Russian authorities provide legislative stimulation for introduction of such systems at the municipal and commercial land transport, first of all at ambulance cars and city buses. The article describes the typical structure of such systems, the main protocols used to exchange data between their nodes; provides an overview of the most commonly used software and hardware solutions in such systems. In this article are also presented the possible issues of information security for such systems; recommendations for prevention and elimination of information security treats are made; directions of protection from adverse factors are listed.

Keywords: information security, satellite navigation systems, monitoring and supervisory control of ground transportation, automated information-measuring systems, SCADA, GPS, GLONASS

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ НАВИГАЦИОННЫХ СИСТЕМ МОНИТОРИНГА И ДИСПЕТЧЕРСКОГО УПРАВЛЕНИЯ НАЗЕМНЫМ ТРАНСПОРТОМ, ОСНОВАННЫХ НА ГЛОНАСС

Ботвинкин Павел Викторович, аспирант, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. Ленина, 28, e-mail: pavel.botvinkin@gmail.com

В развитых странах создание и использование спутниковых навигационных систем для контроля перемещений наземного транспорта помогает решать различные задачи уже в течение долгого времени. Однако аналогичные системы в России, основанные на ГЛОНАСС, стали повсеместно внедряться лишь относительно недавно. Спутниковый мониторинг получил широкое применение для наблюдения за наземным транспортом с целью решения логистических задач, для контроля над грузовыми и пассажирскими транспортными потоками, оптимизации работы курьерских служб, обеспечения безопасности пассажирских и грузовых перевозок. Атакующие, в случае получения доступа к системе контроля перемещений с «правом чтения», могут незаконно получить информацию о местоположении мониторируемых объектов. Если атакующие получают доступ с «правом записи», то они могут воздействовать на данные в системе контроля, перехватывая или посылая ложные данные. Реализация любого из этих вариантов может повлечь за собой серьезные негативные последствия и даже привести к человеческим жертвам. В настоящее время российские власти обеспечивают законодательное стимулирование для введения таких контролирующих систем в эксплуатацию на муници-

пальном и коммерческом наземном транспорте – в первую очередь в автомобилях скорой помощи и городских автобусах. В данной статье описывается типичная структура таких контролирующих систем, основные протоколы, применяемые для обмена данными между их узлами; представлен обзор обычно используемых в таких системах программных и аппаратных решений. В работе также описаны возможные проблемы информационной безопасности для рассматриваемых систем; даны рекомендации по предотвращению и устранению угроз информационной безопасности; перечислены направления защиты систем от воздействия неблагоприятных факторов.

Ключевые слова: информационная безопасность, спутниковые навигационные системы, мониторинг и диспетчерский контроль наземного транспорта, автоматизированные информационно-измерительные системы, SCADA, GPS, ГЛОНАСС

Introduction. Global navigation and positioning systems are parts of automated navigation systems for ground transportation monitoring and supervisory control, which have complex structure and include a variety of different software and hardware solutions. Data communication between their nodes is performed by a variety of protocols. Breach of information security of such systems can lead to serious negative consequences, but this problem is not analyzed in sufficient details.

Over the past few years in Russia such systems have been being systematically implemented at the federal and municipal levels. The first city in Russia, where public transport was equipped with navigational monitoring equipment based on GLONASS (GLObal NAvigation Satellite System), became Sochi. In order to control transportation flows, GLONASS equipment was installed on 250 buses in Sochi by company "M2M telematics" [11].

The purpose of this article is to analyze possible threats to information security of GLONASS-based automated navigation systems for ground transportation monitoring and supervisory control.

Brief information about global navigation and positioning systems. The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites [20].

The system provides critical capabilities to military, civil and commercial users around the world. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver [10].

The GPS project was developed in 1973 to overcome the limitations of previous navigation systems, integrating ideas from several predecessors, including a number of classified engineering design studies from the 1960s [12]. GPS was created and realized by the United States (US) Department of Defense (DoD) and was originally run with 24 satellites. Currently there are 31 in-orbit and healthy satellites [10].

GLONASS – GLObal NAvigation Satellite System – is the Russian satellite navigation system designed for operative support of quick navigation. The system is intended for an unlimited number of users. GLONASS satellite monitoring can be carried out on a land, sea, river and air transport. Access to civil GLONASS signals at any point on the globe is provided on the basis of Presidential Decree granted to Russian and foreign consumers at no cost and without restrictions.

GLONASS can provide not only navigation, but also satellite monitoring of transport [7], which allows monitoring ground transportation on purpose to solve logistical problems, to control cargo traffic, to optimize courier services, to ensure safety of passenger and freight transportation, to perform survey and cadastral works.

Russian authorities doesn't have jurisdiction on GPS, and, unlike GLONASS, stable access to it on country's territory cannot be guaranteed.

Russian GLONASS, as well as USA's GPS, is used both in civil and military (army vehicles movement, fire coordination etc.) purposes. It means that at any moment civil access to these systems may become limited or even completely restricted by military orders.

Parts of these systems may become objects of political showdowns, as it happened at summer 2014 – Russian government decided to shut down all 11 American-run GPS stations within its territory [16].

That's why European Union (EU) decided to become independent of those two systems and make its own navigation and positioning system called «Galileo», as well as Earth monitoring program called «Copernicus» [6].

The first three Copernicus services under the land, ocean and emergency response themes and two additional services addressing the atmosphere and security themes were unveiled at the Copernicus Forum held in Lille in September 2008. Currently in their pre-operational phase, it is foreseen that these services enter into an EU-wide operational phase by 2011, with the objective to be fully operational by 2014. Its cost during 1998 to 2020 is estimated to be 8.4 billion euro [4].

Legislative control. At the moment, the Russian government has adopted a series of regulations and laws that establish the basic concepts, procedures and standards of installation and operation of GLONASS-based automated navigation systems for ground transportation monitoring and supervisory control, and has aimed at stimulating their implementation and use [13, 15, 17]

According to Resolution of the Russian Government on August 25, 2008 № 641 «About equipment transportation, technical facilities and systems by satellite navigation systems based on GLONASS or GLONASS/GPS», the following vehicles, devices and systems should be equipped by facilities, based on GLONASS or GLONASS/GPS [15]:

- space devices;
- state aircraft, civil and experimental aviation planes;
- sea, river and mixed («river-sea») vessels;
- road and rail vehicles, used for the transportation of passengers, special and dangerous freight;
- apparatus and equipment, used to carry out geodetic and cadastral works;
- time synchronization systems.

Although the law does not directly limit the application of the navigation equipment, based on GPS on these types of devices, it does so indirectly, by only allowing the use of devices based on GLONASS or GLONASS/GPS combination.

A typical structure of automated navigation systems, their vulnerabilities and information security. Thus, due to the growing number of GLONASS-based automated navigation systems for ground transportation monitoring and supervisory control (it varies up to few hundreds of such systems in each administrative region of Russia in civil sector), issues of information security has become extremely important.

Attackers in the case of gaining access to a system with read-permissions can illegally obtain information about the location of monitored objects. If attackers can access with write-permissions, they can affect the data in the system, intercepting or sending false data. Both of these options may entail serious negative consequences, and even cause casualties.

To contemplate the possible security issues of such systems, it's necessary to analyze the elements of their typical structure (fig.).

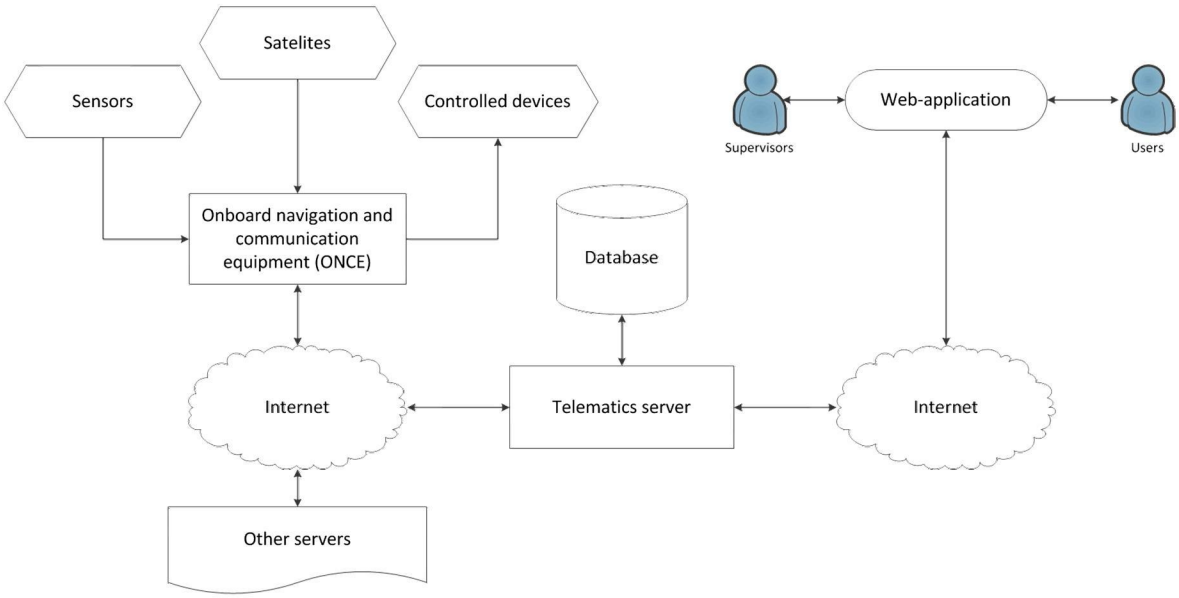

Fig. A typical structure of automated navigation system
for ground transportation monitoring and supervisory control

As seen, automated navigation systems for ground transportation monitoring and supervisory control by their functions and structure can be considered as systems for control and data acquisition (SCADA).

Stability of system's measurements mainly depends on the space satellites: their amount, on-line status, coverage zones, stability of firmware, etc. To properly calculate the position of object it's necessary to have communication with at least four available satellites at once (three satellites are enough for two-dimensional measure without of altitude parameter), but more satellites will improve accuracy of calculations [14].

Another way to improve accuracy of object's coordinates calculations is to use ground-based reference stations, which broadcast the difference between the positions indicated by the satellite systems and the known fixed positions. These stations broadcast the difference between the measured satellite pseudoranges and actual (internally computed) pseudoranges, and receiver stations may correct their pseudoranges by the same amount [5].

Vulnerabilities of navigation satellites and ground stations lay beyond the scope of this article.

Onboard navigation and communication equipment (ONCE, or for brevity is often used the word «terminal») is intended for installation on the vehicle as an additional device, recording at specified intervals (from one second to several minutes) using an internal GLONASS (or GLONASS/GPS) module the current location (coordinates) of the vehicle, its speed, movement direction. Additionally a number of other parameters can be recorded, such as status of the analog and digital inputs, sensors data (ignition status, fuel level, etc.). This information can be transmitted to a specified server and stored there for further analysis.

ONCE enables control of external equipment via digital outputs using commands sent via GPRS or SMS. Mounted ONCE must be certified, and the requirements for them are determined by several state standards of the Russian Federation, in particular, the standard «GOST R 54024-2010 Global navigation satellite system. Urban land passenger transport supervisory control. The purpose, composition and characteristics of onboard navigation and communication equipment» [17].

Some models of terminals have independent internal power supply in case of disconnection from external power supply (car battery), and it's possible for them to keep collect and send all necessary data.

To ensure data integrity on external power failure or GSM network disappearance, the state of all events is recorded by the terminal and stored in non-volatile memory. The accumulated data is transmitted as soon as the network of mobile operator is available, usually through GPRS as data packets to the telematics server (some models of devices support more than one server) with a static IP-address or domain name (some devices support only IP-addresses).

Consider the most probable ways of intervening into the regular job of automated navigation systems for ground transportation monitoring and supervisory control by intruders (hackers), their targets and ways to detect attacks and prevent their possible negative consequences.

Physical impact on the ONCE as of the system part or on its contents can be performed by temporarily disabling or damaging the terminal nodes by mechanical (breaking inside the device, powering it off, or pulling out the SIM-card) or electromagnetic (shielding, powerful electromagnetic impulse) effects. Disabling SIM-card module can cause temporary loss of communication with the telematics server, however, if the navigation module is still functional and the sensors are still connected, data, anyway, will be put into non-volatile memory. The software will alert the supervisor about the communication failure, and after recovery the data will arrive into the system. If the malefactor would break the navigation module or disconnect any of the sensors, the loss of information is inevitable.

Physical influence can be prevented mostly by sealing equipment's casing and sensors' inputs. The best way to reduce the probability of physical infiltration is to place [3] the equipment into the most inaccessible place of the vehicle.

The other «weak point» of terminals is their electronic components, which normally are not of «space» or «military», but of «civil» class. It means that their reliability depends on significant environment factors (temperature, humidity, vibrations, electromagnetic fields). Though it's possible to improve nodes' reliability by backing them up with duplicates, normally owners don't do this, because it also leads to doubling the cost (and weight) of hardware, and it's cheaper to replace a node each time it breaks.

Natural influences are determined by a combination of factors (physical, chemical, thermobarical, etc.) capable of exerting direct or indirect, immediate or mediate impact on performance and work regimes of terminals [3].

In Russia the current related standard is GOST 14254-96 (Russian National Standard, harmonized with IEC 529-89) «Degrees of protection provided by enclosures», which defines the requirements in terms of resistance of enclosures and electrical equipment in general to external impact factors, as well as the methods and modes of controlling and testing to check for compliance with enclosures' electrical protection level sets.

This standard indicates the degree of protection provided by enclosures. Electrical protection index (IP) consists of two digits. The first shows the protection against ingress of solid particles inside the structure: from zero to six. The second shows protection against moisture: from zero to eight.

Along with the indicators of protection against external influences there are concepts of climatic performance and allocation category. Climatic performance shows in which temperature range the device is operated. Allocation category defines a number of external factors (such as humidity) in place of the product's exploitation [3].

In accordance with the definition of security, all attacks on navigation systems for ground transportation monitoring and supervisory control can be divided into the following categories [2].

1. Access attacks, which include attempts to gain unauthorized access to system resources.

2. Attacks on privacy, which represent attempts to intercept the data transfer in the transport environment.

3. Attacks on integrity, which include the generation and transfer of frames to capture and control of the whole system, to call faults and failures in its work or to prepare other attacks.

Supervisory software has features for interrupted connections detection and will alarm if it receives data gaps or zero values from remote devices.

Programmatic impact can be performed by direct connection to the device by an attacker using a data cable, or by remote connection to the node at interval between the server and the node. Such attack requires special equipment and skills and allows an attacker to modify the internal settings of the device and even its firmware. Telematics server software usually allows performing mass remote firmware updates. If an attacker will be able to break into the channel of communication between the server and the ONCE and prove it that he is legitimate, the consequences could be extremely negative, up to the failure at the hardware level. This kind of attacks is almost impossible to detect, but they can be prevented by filtering by IP and MAC address of the remote devices by the firewall and applying crypto-stable passwords, as well as strong authentication methods.

Many of ONCE's types have another vulnerability – the ability to change internal settings via SMS. Knowing the phone numbers, assigned to device's SIM-card, an attacker can send a stack of SMS with malicious settings. Even despite the fact that such devices require a password to accept permission to perform any critical action via SMS, the people, who install them, usually does not change the password, and it remains the default (such as "1234" or "0000"). This greatly reduces the information security not only of one device, but the whole navigation system for ground transportation monitoring.

If the operator does not own the ONCE, it makes an agreement which prescribes the operator's liability to the owner of this device. In most cases there is an agreement with a contractor to install a number of devices for the operator. Thus, for any direct interference or violation of information security and integrity of the unit, the operator and (partially) the contractor shall be liable to the owner of the equipment.

Telematics server has specialized software installed to receive data from external sources (ONCE, web application, other servers), put the incoming data into the database, manage date inside the database, send data from the database to other servers or into web application, perform management of settings of the remote equipment.

There are many software solutions, but the most common software that can be considered are:

- "BN Complex" by "M2M telematics" [1];
- "ACS Navigation" by "Transnavigation (NPP Transnavigatsiya)" [18];
- "Wialon Pro" by "Gurtam" (it's also possible to rent a telematics server from this company) [21].

However, at the moment, the developers of these systems keep their product's support and development going.

The data on the server software may come through a large number of protocols, based on HTTP, SMTP, FTP, etc. [13] Protocol, used to transfer data between the server and ONCE, may be open (for example, «Garmin FMI» [7]) or closed (for example, "Granite-2.07").

The most serious vulnerability of any open protocol can be considered as device's identity forgery. That is, an attacker knowing telematics server's address, a unique identifier number of the device (UIN) and used data transfer protocol, may send false messages on behalf of this device. Currently there is no certain way to defend against such an attack. Even the use of proprietary protocols does not guarantee protection. Proprietary protocols are such only formally and informally it's possible obtain the information about the messages' format using reverse engineering on the server side.

Good, but not an absolute way to protect at the moment seems filtering data packets from devices by their IP and MAC addresses. But in the case of a large number of devices (often several

thousand or more – normally an average main regional transport supervisory system includes tens of thousands onboard terminals) this way is extremely difficult, inefficient and does not protect against IP and MAC addresses forgery.

To transfer data between servers is most commonly used the «Unified protocol for communication of telematic platform of moving objects monitoring and control systems» based on SOAP [19], often called for brevity "NIS/Olimpstroy/SOAP". In this case, the method, described above forgery of device's UIN, is still possible. However, this protocol involves allocation of special URL-gates on the server side with the ability to use Basic or NTLM authentication combined with SSL for each incoming data connection. Thus, the use of SSL is recommended. When the connection is being configured, it's necessary to create a separate account protected by a strong password.

Telematics server may also become a source of danger, because normally it is operated by Microsoft Windows Server system, which itself has a lot of vulnerabilities, is able to run viruses, rootkits and other malware. Administrators of the telematics server should be aware of possible security threats and be able to prevent them in time. It's crucial to use anti-virus, anti-malware programs and to monitor the system's security logs. It's also important to setup the backup mechanisms for the database and the whole system.

Another weakness of the system is the area between the telematics server and the web-application. An attacker can intercept the data or send a control signal to the server. In this case it's reasonable to use SSL and setup crypto-steady users' accounts for accessing the web interface of the application.

Despite the fairly large number of possible vulnerabilities of SCADA-systems, the most dangerous are the internal anthropogenic threats to information security, which include [7]:

- unintentional personnel actions that create the auspicious conditions for external attacks by hackers;
- intentional ignoring the requirements of information security by staff that serving SCADA-system;
- the lack of qualification of personnel in the field of information technologies and implementation of methods of information security;
- the lack of proper security-aimed training courses for personnel.

Unlike external intruder, staff of the enterprise has the great opportunities for attacks to infect and spread malicious code on the sensor network. Information security problems often caused not so much by external attacks, but more as non-compliance with staff regulations and rules of the enterprise information security policy. Managers and other staff of the enterprise may ignore their duties and in the "free" time do the Internet "surfing", social networking, and playing computer games. The result may be an unauthorized PC infection by computer viruses, Trojan horses and worms, which then may penetrate into the sensor networks. This explains why viruses and worms like Stuxnet often present in SCADA-systems, and this fact is normally hidden by staff and managers, as the disclosure of this information will lead all the staff and management to the detailed inspection and then to subsequent negative consequences for them. In addition, the finding of the infection in SCADA system may cause a need of hard reset to clean the virus and will stop the most of enterprise processes, but it is not always feasible from an economic standpoint [2].

Also, the lack of qualifications of personnel, which works with terminals, requires the involvement of outside experts to identify and correct software or even firmware changes in terminals, because after cleaning the system it's necessary to be ensured that the programs and settings in the system nodes correspond to the values required for the proper functioning of system [8].

It is well known that the human factor is the main reason of deviations from normal operation status in various technical systems. This requires special attention to the establishment and maintenance of appropriate technical regulations.

The price of such systems' security improvement varies. It depends of the complexity of system, its purpose, types of used terminals and telematics server

Conclusion. Automated navigation systems for ground transportation monitoring and supervisory control currently receive active development on the territory of Russia. Such systems may be considered as complicated information-measuring systems [3] and, because of their complex structure, they have many potential vulnerabilities.

Without the analysis and taking measures to prevent these vulnerabilities, malicious attackers can cause serious damage to the system and to dependent from it organizations and individuals. Most of the attacks can be prevented, but in such systems there are still some vulnerabilities. Therefore prevention methods should be found, and it is an urgent task.

After analyzing possible adverse factors, the following directions of protection of GLONASS-based automated navigation systems for ground transportation monitoring and supervisory control can be denoted:

- protection from natural factors: climate, sunlight, extreme temperatures, rain, high relative humidity, high atmosphere pressure, dust, sand, etc.;
- protection from biological agents (insects, rodents, etc.);
- protection from technogenic effects;
- protection from malicious human intervention: mechanical intrusions, software and hardware hacking.

In general, the task of such systems' protection involves the use of special technical, technological, software and hardware solutions, and should be developed and implement as a set of measures to comply with the constitutive and legislative standards, rules and regulations. The most important parts with the weakest security grades are information transmission channels and software solutions.

The most of owners of such systems do not aware of existing and possible risks, they don't care about importance of providing proper security measures, and thus they don't spend money on it. These expenses may vary of system's structure and complexity, but anyway they're lower than possible damages from possible system failure.

Bibliography

1. BN-Complex®. Управление и контроль автопарком, мониторинг и диспетчеризация транспорта. – Режим доступа: http://m2m-t.ru/software/server_software/?ELEMENT_ID=483 (дата обращения 01.08.2014), свободный. – Заглавие с экрана. – Яз. рус.

2. Botvinkin P. V. Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems / P. V. Botvinkin, V. A. Kamaev, I. S. Nefedova, A. G. Finogeev, E. A. Finogeev // Life Science Journal. – 2014. – № 11 (11s). – P. 384–388.

3. Ботвинкин П. А. О методах защиты от неблагоприятных факторов, воздействующих на автоматизированные информационно-измерительные системы контроля и учёта энергоресурсов / П. А. Ботвинкин // Известия Волгоградского государственного технического университета. – 2013. – № 22 (125). – P. 50–53.

4. Copernicus Programme. – Available at: http://en.wikipedia.org/w/index.php?title=Copernicus_Programme&oldid=621621667 (accessed 01.08.2014).

5. Differential GPS. – Available at: http://en.wikipedia.org/w/index.php?title=Differential_GPS&oldid=623142292 (accessed 01.08.2014).

6. EUROPA – Press release – European Satellite Navigation Galileo services will start at the end of 2014. – Available at: http://europa.eu/rapid/press-release_IP-14-80_en.htm (accessed 01.08.2014).

7. Финогеев А. Г. Анализ и классификация атак через беспроводные сенсорные сети в SCADA системах / А. Г. Финогеев, И. С. Нефедова, Е. А. Финогеев, Куанг Винь Тхай, Б. В. Ботвинкин // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 1. – С. 12–23.

8. Финогеев А. Г. Система удаленного мониторинга и управления сетями теплоснабжения на основе беспроводных сенсорных сетей / А. Г. Финогеев, В. Б. Дильман, В. А. Маслов, А. А. Финогеев // Прикладная информатика. – 2011. – № 3 (33). – С. 83–93.

9. Garmin Fleet Management Interface Control Specification. – Available at: http://www.getacoder.com/data/projects/138695/001-00096-00_0F_web.pdf (accessed 01.08.2014).

10. Global Positioning System. – Available at: http://en.wikipedia.org/w/index.php?title=Global_Positioning_System&oldid=623182733 (accessed 01.08.2014).

11. GLONASS – navigation systems. – Available at: http://www.nis-glonass.ru/about-glonass (accessed 01.08.2014).

12. National Research Council (U.S.). Committee on the Future of the Global Positioning System; National Academy of Public Administration (1995). The global positioning system: a shared national asset: recommendations for technical improvements and enhancements. National Academies Press, 2013. – P. 16.

13. Приказ Министерства транспорта Российской Федерации от 31 июля 2012 г. № 285 «Об утверждении требований к средствам навигации, функционирующим с использованием навигационных сигналов системы ГЛОНАСС или ГЛОНАСС/GPS и предназначенным для обязательного оснащения транспортных средств категории M, используемых для коммерческих перевозок пассажиров, и категории N, используемых для перевозки опасных грузов.

14. Patent US5373298. Method of estimating the error in the calculation of the position of a mobile by a GPS receiver, and GPS receiver for implementing this method. – Published on Dec 13, 1994 by Alcatel Espace.

15. Постановление правительства Российской Федерации от 25 августа 2008 г. № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS».

16. Russia Will Shut Down All U.S. GPS Stations Within Its Borders. – Available at: http://gizmodo.com/report-russia-will-shut-down-all-u-s-gps-stations-wit-1575641874 (accessed 01.08.2014).

17. ГОСТ Р 54024-2010. Глобальная навигационная спутниковая система. Системы диспетчерского управления городским наземным пассажирским транспортом. Назначение, состав и характеристики бортового навигационно-связного оборудования. – Москва : Стандартинформ, 2011.

18. Научно-производственное предприятие «Транснавигация». – Режим доступа: http://www.transnavi.ru/projects/asdu/about/about.php (дата обращения 01.08.2014), свободный. – Заглавие с экрана. – Яз. рус.

19. Унифицированный протокол взаимодействия телематических платформ систем мониторинга и правления подвижными объектами. – Режим доступа: http://tdog2014.com/assets/ unificirovanuy-protokol2.pdf (дата обращения 01.08.2014), свободный. – Заглавие с экрана. – Яз. рус.

20. What is GPS?. – Available at: http://www.loc.gov/rr/scitech/mysteries/global.html (accessed 01.08.2014).

21. Wialon Pro Server Solution for GPS Tracking System. – Available at: http://gurtam.com/en/gps_tracking/wialon_pro.html (accessed 01.08.2014).

References

1. BN-Complex®. Carport management and control, transport monitoring and supervising. Available at: http://m2m-t.ru/software/server_software/?ELEMENT_ID=483 (accessed 01.08.2014).

2. Botvinkin P. V., Kamaev V. A, Nefedova I. S, Finogeev A. G., Finogeev Ye. A. Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems. *Life Science Journal*, 2014, no. 11 (11s), pp. 384–388.

3. Botvinkin P. V. O metodakh zashchity ot neblagopriyatnykh faktorov, vozdeystvuyushchikh na avtomatizirovannye informatsionno-izmeritelnye sistemy kontrolya i ucheta energoresursov [About methods of protection from adverse factors that affecting automated information and measurement systems for control and energy resources accounting]. *Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta* [Proceedings of the Volgograd State Technical University], (2013), no. 22 (125), pp. 50–53.

4. Copernicus Programme. Available at: http://en.wikipedia.org/w/index.php?title= Copernicus_Programme&oldid=621621667 (accessed 01.08.2014).

5. Differential GPS. Available at: http://en.wikipedia.org/w/index.php?title=Differential _GPS&oldid=623142292 (accessed 01.08.2014).

6. EUROPA – Press release – European Satellite Navigation Galileo services will start at the end of 2014. Available at: http://europa.eu/rapid/press-release_IP-14-80_en.htm (accessed 01.08.2014).

7. Finogeev A. G., Nefedova I. S., Finogeev Ye. A., Kuang Vin Tkhay, Botvinkin P. V. Analiz i klassifikatsiya atak cherez besprovodnye sensornye seti v SCADA sistemakh [Analysis and classification attacks via wireless sensor networks in SCADA systems]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2014, no. 1. pp. 12–23.

8. Finogeev A. G., Dilman V. B., Maslov V. A. and Finogeev A. A. Sistema udalennogo monitoringa i upravleniya setyami teplosnabzheniya na osnove besprovodnykh sensornykh setey [System for remote monitoring and control of district heating network based on wireless sensor networks]. *Prikladnaya informatika* [Applied informatics], 2011, no. 3 (33), pp. 83–93.

9. Garmin Fleet Management Interface Control Specification. Available at: http://www.getacoder.com/data/projects/138695/001-00096-00_0F_web.pdf (accessed 01.08.2014).

10. Global Positioning System. Available at: http://en.wikipedia.org/w/index.php? title=Global_Positioning_System&oldid=623182733 (accessed 01.08.2014).

11. GLONASS – navigation systems. Available at: http://www.nis-glonass.ru/about-glonass (accessed 01.08.2014).

12. National Research Council (U.S.). Committee on the Future of the Global Positioning System; National Academy of Public Administration (1995). The global positioning system: a shared national asset: recommendations for technical improvements and enhancements. National Academies Press, 2013, p. 16.

13. Order of the Ministry of Transport of the Russian Federation of July 31, 2012 no. 285 "On approval of requirements for aids to navigation, functioning using the navigation signals of GLONASS or GLONASS/GPS and mandatory equipment intended for vehicles of category M, used for the commercial carriage of passengers and category N, used for the transport of dangerous goods". (In Russ.)

14. Patent US5373298. Method of estimating the error in the calculation of the position of a mobile by a GPS receiver, and GPS receiver for implementing this method. Published on Dec 13, 1994 by Alcatel Espace.

15. Resolution of the Russian Government of August 25, 2008 no. 641 "About equipment transportation, technical facilities and systems by satellite navigation systems based on GLONASS or GLONASS/GPS". (In Russ.)

16. Russia Will Shut Down All U.S. GPS Stations Within Its Borders, http://gizmodo.com/report-russia-will-shut-down-all-u-s-gps-stations-wit-1575641874

17. Russian National Standard "GOST R 54024-2010 Global navigation satellite system. Urban land passenger transport supervisory control. The purpose, composition and characteristics of onboard navigation and communication equipment". (In Russ.)

18. Scientific-Production Enterprise "Transnavigation". Available at: http://www.transnavi.ru/projects/asdu/about/about.php (accessed 01.08.2014). (In Russ.)

19. Unified protocol for communication of telematic platform of moving objects monitoring and control systems. Available at: http://tdog2014.com/assets/unificirovanuy-protokol2.pdf (accessed 01.08.2014). (In Russ.)

20. What is GPS? Available at: http://www.loc.gov/rr/scitech/mysteries/global.html (accessed 01.08.2014).

21. Wialon Pro Server Solution for GPS Tracking System. Available at: http://gurtam.com/en/gps_tracking/wialon_pro.html (accessed 01.08.2014).