European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.04.02.175

GCPMED 2020
Global Challenges and Prospects of the Modern Economic Development

PROTECTION OF MOBILE EQUIPMENT IN JSC «RZD» UNDER THE CONDITIONS OF DIGITALIZATIONS

T. B. Efimova (a)*, L. I. Papirovskaya (b), D. A. Korunov (c)
*Corresponding author

(a) Samara State University of Economics, Soviet Army Str., 141, Samara, Russia, TB_Efimova@mail.ru
(b) Samara State Transport University, Svoboda Str., 2V, Samara, Russia, Papirovskaya@gmail.com
(c) Samara State University of Economics, Soviet Army Str., 141, Samara, Russia, korunov.2012@mail.ru

Abstract

Under the conditions of digitization the majority of companies of the Russian federation use different mobile devices in their work. It is obvious that alongside with convenience of use they may be considered to be a serious threat regarding ensuring information security. The company "RZD" also uses mobile devices in its work. There are no special means of mobile equipment protection in the company, which produces a negative impact on ensuring the company information security. The main protection methods used by the company employees are the graphic or digital password at the device entrance and sometimes folders coding on a mobile device, as well as installation of anti-virus programs and spyware tracing the user activity which prevent forbidden actions and disconnection of the device from the network during operation. The aim of this research is creation of the application for ensuring centralized protection of mobile devices of employees from theft, loss or illegal data transmission. The application allows tracing all mobile devices of employees with the help of geolocation, its introduction provides an opportunity of timely respond to emergency situations and, in case of defining the fact of theft of the device or illegal data transmission, it allows immediate blocking of the device. The advantage of this development is its uniqueness on the domestic market, as well as the fact that further it will be possible to combine the developed application with the already operating systems of the company "RZD", which will positively influence the quality of work.

2357-1330 © 2021 Published by European Publisher.

Keywords: Centralized operation, digitization, information, mobile device

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Noncommercial 4.0 Unported License, permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.15405/epsbs.2021.04.02.175
Corresponding Author: T. B. Efimova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Security of information systems is the feature characterizing ability of the system to ensure confidentiality and integrity of information, i.e. information protection from unauthorized access for the purpose of its disclosure, changing and destruction. The law considers the order of work with data, which allows ensuring protection of rights and freedoms of a human or a citizen. The railway uses the internal network Intranet in its operation. A user is connected to information resources only after an application of AAPS is agreed upon. This connection is provided for two years from the moment of the application creation. Within the framework of ensuring information security of the holding JSC «RZD» a number of requirements are imposed to users. While working in JSC "RZD" information systems an internal user is obliged to:

⁻ keep his passwords (key bearers) of access to PC and AWS in secret;

⁻ during intervals in work with information systems of JSC «RZD» containing information of commercial confidentiality of JSC «RZD», provide blocking of PC with a password screen saver;

⁻ provide verification of used removable media for the presence of malicious software with the help of the installed anti-virus software;

⁻ when having suspicion of appearance of malicious software on the PC, which are not automatically discovered or deactivated by the system of anti-virus protection, immediately switch the PC off the network of data transfer and report about it to the user support service;

⁻ in case of complete or partial termination of operation of anti-virus software immediately report about it to the joint user support service;

⁻ when discovering incorrect operation of software of the PC apply to the joint user support service.

When working with information systems of JSC "RZD" an internal user is forbidden to:

⁻ allow access to PC for other persons, except for employees of The Main computer center of JSC «RZD» (the information computer center – a structural division of The Main computer center of JSC «RZD») servicing this PC, as well as employees of Security Department of JSC «RZD» (the regional security center – a structural division of JSC «RZD») maintaining control functions;

⁻ perform unauthorized connection to the PC and network equipment of external devices, including telecommunication and information processing devices;

⁻ use the PC for non-production purposes;

⁻ transmit confidential information via unprotected channels of data transmission network of JSC "RZD";

⁻ disconnect “the security agent” or change its settings (except for specialists of The Main computer center of JSC "RZD" or the information computer center – a structural division of The Main computer center of JSC «RZD» servicing this PC), install independently any software onto the PC or allow somebody to do it, except for specialists of The main computer center of JSC RZD or the information computer center – a structural division of The Main computer center of JSC «RZD» as well;

⁻ use the PC with partially or completely non-operating anti-virus software, as well as incorrect operation of software;

⁻ use removable data storage medium on the PC, including external data storage media without preliminary verification for the presence of malicious software;

⁻ provide network access to his automated working station for other users.

When working with information systems of JSC "RZD" an internal user is forbidden to:

⁻ publish his addresses (e-mail, IP-addresses, etc.), as well as addresses of other employees of JSC "RZD" on Internet resources of wide access (forums, conferences, etc.);

⁻ use accessible electronic mail systems and other services of message exchange for personal purposes, as well as for distribution of any information;

⁻ connect automated working stations, on which processing of confidential information is carried out, to information systems of common use;

⁻ transmit information causing threat to the state security and defense, health and safety of people;

⁻ launch executive files obtained from information systems of common use (files with program database exe, com, bat, scr, reg, etc.) on the PC;

⁻ apply to potentially dangerous resources of information systems of common use.

At present mobile communication facilities are connected to the company information system in JSC "RZD" by various means: at the same time using the technology ViPNet, means of VPN IPSEC, professional information leak and access to Internet resources from a mobile device is not controlled. Frequently confidential information is transmitted to mobile communication means using public mail and file services, and it is not surprising that documents transmitted to a concrete addressee may be found in open access. Use of mobile technical devices in JSC "RZD" is regulated by the order, in which requirements and terms of possible application of this equipment, while organizing interaction with corporate resources, is formulated.

2. Problem Statement

At present in JSC "RZD" there is only one MDM system built into the Kaspersky packet named “Kaspersky MDM”. Kaspersky Security for mobile devices helps employees to carry out their work tasks on smartphones and pads in any part of the world, not putting important business data or critical business processes at risk. This application ensures multi-level protection of mobile devices which includes protection from malicious software, anti-spam, web-control, software and equipment control, and provides the function Anti-Thief as well. In order to simplify tasks of administration all functions are operated from a single console. Tracing, management and protection of mobile devices used by employees for work may require substantial resources. Nowadays reliable protection of mobile devices is simply necessary: the number of threats for them is actively growing, and mobile devices for the working process are not less important sometimes than desk computers. Kaspersky Security for mobile devices ensures their protection and allows to control security politics on each smartphone or pad having access to the network corporate data. One of the leaders in this sphere on the Russian market is LLC «NII SOKB», its system SafePhone was certified by FSTEC RF. The idea of development of the own application is important, because it will allow to make the work of employees on mobile devices secure and will provide access to certain company information resources, depending on position and requirements.

https://doi.org/10.15405/epsbs.2021.04.02.175
Corresponding Author: T. B. Efimova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

3. Research Questions

Analysis of the subject field was conducted for the purpose of development of the mobile application, ways of interaction realization were considered, modelling by means of CASE-technologies was carried out, it allowed to determine users, the character of their actions and business-processes. Issues of choice of the mobile operating system for development of the mobile application and information security were considered. After conducting detailed analysis, the development medium was chosen to be Android Studio. At present Android Studio is the official medium of development for Android. Android Studio is characterized by the flexible system of Gradle assembly and extended support of Google services and various types of devices. It has a rich functional of the editor of application screens with editing support of interface themes and possibility of signing applications. Android Studio has built-in support of the cloud platform Google and possibility of simple integration with Google Cloud Messaging and App Engine.

4. Purpose of the Study

A great number of works of domestic and foreign scientists, such as Xu and Warkentin (2020), Rantao and Njenga (2020), Solomon and Brown (2020), Darms et al. (2020), Polykhan (2019), Chebotareva (2016), is devoted to the issues of information protection on the enterprise. When developing the application, the legal base in the field of information security of the Russian Federation, orders of JSC "RZD" were studied in detail. Foreign analogues and domestic developments were considered. Types of attacks on mobile applications, types of security vulnerability were studied in detail. The corresponding company business processes were analyzed, and proposals on their improvement were made. Development of the application was carried out using C#. Further it will be possible to combine the developed application with the already operating systems of the company "RZD", which will positively influence the quality of work.

5. Research Methods

When developing a mobile application, it should be taken into consideration, that data which this application uses may be of certain interest for third persons. The main types of attacks on a mobile application are:

1. Decompiling of an application file and analysis of data saved locally. Protection of this level is a mobile developer's sole responsibility.

2. Capture of data transmitted via the network (MITM-attacks). Most mobile applications are client-server ones, therefore they constantly transmit and accept vast volumes of information. Although modern mobile and web developments actively complete transfer to the HTTPS-communication protocol.

3. Settings of the device developer and an attack on an application, as well as algorithms used in it through external debugging tools.

Let us consider vulnerability of general character, without connection with a concrete platform. Critically important data of users are any data which must not be accessible for a third party; this concerns both personal user data (date of birth, residential address, private correspondence), and private data (passwords, credit cards data, numbers of bank accounts, numbers of orders, etc.)

List of main vulnerabilities:

1. Use of unprotected local data stores.

The danger is very high, it is met everywhere and is expressed in storage of critically important data in unprotected or weakly protected local stores specific for a concrete platform. For a third person it is easy to discover, and, as a rule, no special skills are necessary for an intruder. Critically important data may be stored only in protected platform stores.

2. Storage of critically important data with a code.

The danger is high, vulnerability concerns storage of Critically important data inside the code (in statistical constant lines, application resources, etc.).

3. Application of algorithms with the private key storage.

The danger is high, vulnerability is critical, if private information of an algorithm (private key) is forcedly saved in the code or the mobile application resources (which happens more often). It is easily disclosed by the method of decompiling. For the purpose of protection of the mobile application, it is advisable to use only modern symmetric algorithms with the generated arbitrary one-time key, which have high level of strength to breaking by the method of brutal force, or take the asymmetric private key outside the limits of the application, or personalizethis key (for example, a private key may be the user entrance key saved in a coded view in the protected storage of the operation system).

There a number of points common for all mobile platforms which should be compiled with in developing:

1. Protection with the user code. If an application is protected with the user password (PIN-code, the finger print scan, graphic password, etc.), it must immediately display the entrance window of this protection code overlapping the entire application screen, when the application disappears onto the background (“folding”).

2. Functioning of the client-server application. For client-server applications it is very useful to apply the session mechanism with the limited time of session life. It allows avoiding the application “downtime” in an unprotected mode, if a user simply forgot about it and left the device for free access.

3. Work with data. Absolute meanings should be transmitted using universal methods of exchange of such information, without connection to the time zone of a concrete user device. More frequently, the optimum variant is the application behavior, when data are displayed for the user in his local time zone, but their storage and transmission are carried out in a format not connected with the time zone.

6. Findings

Owing to the developed application it is possible to estimate information obtained from a mobile device. Apart from this, it will allow to control the user files, SMS messages, to manage calls, contacts, review of the device location, manage the device accounts (Kurganskaya & Kubaev, 2017). It is also possible to get access to the device camera, review information about the system condition and the mobile device version, review and manage applications on the device, receive access to the device microphone. If an employee is dismissed, the application, through which control is carried out, is deleted, and a port, through which operation of the device is carried out, is deleted from the list of ports on the computer. The application is implemented on the client-server architecture. The use of this type of architecture ensures reliability of the entire system against failures, as well as simplicity and convenience in realization and support. Using this architecture further it is possible to introduce such components into the system as data cloud storage. The decision was taken to choose the development medium Visual Studio and the programming language C# for writing the client-server application with the operating system Windows.

The application for installation is filled out in the automated application processing system by the person responsible for processing applications or by the user himself, you must specify the purpose of the connection and the reasons for granting access must be attached (Korablev et al., 2020; Pogorelova et al., 2020). The basis for installing the application on the mobile device of an internal user is their job responsibilities, as well as a written instruction from the management of JSC "RZD" or the head of a branch (structural division) JSC "RZD", a copy of which is attached to the application. If it is not possible to use the automated system, the application must be submitted in writing together with a cover letter stating the purpose of the connection and the reason for granting access to the information system. A written request is sent by mail in compliance with all the requirements of the established procedure.

If an employee is dismissed or transferred to another division of JSC "Russian Railways", the head of the division of JSC "RZD", in which he worked, is obliged to inform the Main computing center (the corresponding information and computing center) in writing no later than the next day after the day of dismissal or transfer. Based on this message, the Main computing center or information and computing center that the employee was assigned to will disconnect the specified user from the system and delete all applications from the device.

If necessary, the specialist can request any information from the employee's device in real time. First of all, you need to pay attention to the integrity of the device system and whether there were absolutely any interactions with the device management application itself. The second stage of verification will be viewing installed apps on the device and evaluating them according to the criteria:

- source of the installed application – whether the source is trusted or a third-party application that is not confirmed by a certificate;
- app impact on the system – how the app interacts with the device's main system;
- device resources required to maintain the application's performance – the amount of RAM, power consumption, and memory used in the device;
- the purpose of installing the app is to work, study, or play games.

The next step will be to check such sections as the documentation stored on the device and whether there have been any attempts to transfer these files to others. The specialist will also be able to view where the device is located at the current time – this is done so that in case of theft or loss of the device by an employee, it can be found or, in extreme cases, completely blocked to protect the company's data. The specialist will be able to listen to the situation occurring near the device through a microphone and view the situation through the camera. You can also use this function to contact a specialist to resolve urgent user questions. The installation of more precise criteria of assessment is possible only when the required testing of the software product in a real test. The data provided above only describes how to use the software functionality. It is necessary to take into account such a factor as the user's personal information, so it is best to install this application not on the employee's personal device, but on a device issued by the organization itself in order to avoid conflict situations on the part of the user.

7. Conclusion

Using the developed application, it is possible to ensure reliable protection of mobile devices of the company employees, risks of information leak which could cause great damage to the company are also decreased. The first indicator of protectiveness of the developed application is the fact that it is practically impossible to get access to it from outside, the installation file is to be located strictly on the administrator's computer of the given system and must not leave its boundaries. The second indicator is the fact, that the program installed on the mobile device operates off-screen and controls all processes of the device. It should also be noted that the mobile application operates according to its own security policy, so that the possibility of debugging and damage is very small. The third indicator is the fact that interaction of the mobile device and the work station of the system administrator is carried out via the client VipNET, which allows coding the entire flow of data passing between the administrator and the user. It should also be mentioned, that the program may be combined with the already functioning security application WorksPad, which will increase protection of both a great deal and will also decrease a chance of any information leakage. Further it will be possible to improve the program and install anti-virus systems, as well as additional modules which will ensure reliable protection not only of the application, but of the user of the mobile device as well.

References

Chebotareva, A. (2016). Ensuring information security of the personality: The role of international information security and strategic partnership. *Bulletin of the Academy of Law and Management, 1*(42), 48-51.

Darms, M., Hassfeld, S., & Fedtke, S. (2020). Information security and data protection in medicine. *MKG-Chirurg, 13*(4), 240-247.

Korablev, A. V., Petrushova, M. V., & Andreev, A. V. (2020). Development of information risk management theory. *European Proceedings of Social and Behavioural Sciences, 82,* 589-594.

Kurganskaya, L. M., & Kubaev, A. A. (2017). Library space: Concept, types and modernization. *Science Art Culture, 3*(15), 168-173.

Pogorelova, E., Yudina, O., & Kolotilina, M. A. (2020). Mobile app design for business and supervisory activities. *European Proceedings of Social and Behavioural Sciences, 82,* 581-588.

Polykhan, K. O. (2019). Problems and features of the condition of information security in accordance with the doctrine of information security of the Russian Federation. *Sustainable Development of Science and Education, 5,* 154-160

Rantao, T., & Njenga, K. (2020). Predicting communication constructs towards determining information security policies compliance. *South African Journal of Information Management, 22*(1), 1-10.

Solomon, G., & Brown, I. (2020). The influence of organisational culture and information security culture on employee compliance behavior. *Journal of Enterprise Information Management.* https://doi.org/10.1108/JEIM-08-2019-0217

Xu, F., & Warkentin, V. (2020). Integrating elaboration likelihood model and herd theory in information security message persuasiveness. *Computers & Security, 98,* 102009.