Journal of Theoretical and Applied Information Technology
15th August 2021. Vol.99. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY THREATS TO PERSONAL DATA IN THE IMPLEMENTATION OF DISTANCE EDUCATIONAL SERVICES USING MOBILE TECHNOLOGIES

[1]VASILY NIKOLAEVICH POPOV, [1]VITALY NIKOLAEVICH VASILENKO, [2]VICTOR ANATOLYEVICH KHVOSTOV, [2]VLADIMIR VLADIMIROVICH DENISENKO, [3]ALEKSEY VASILYEVICH SKRYPNIKOV, [4]ANDREY VALENTINOVICH IVANOV, [5]ALEXANDER NIKOLAEVICH BELYAEV, [6]OKSANA GEORGIEVNA STUKALO

[1]Voronezh State University of Engineering Technologies, Revolyutsii ave., 19, Voronezh, 394036, Russia
[2]Department of Information Security, Voronezh State University of Engineering Technologies, Revolyutsii ave., 19, Voronezh, 394036, Russia
[3]Faculty of Management and Informatics in Technological Systems, Voronezh State University of Engineering Technologies, Revolyutsii ave., 19, Voronezh, 394036, Russia
[4]Department of Information and Control Systems, Voronezh State University of Engineering Technologies, Revolyutsii ave., 19, Voronezh, 394036 Russia
[5]Faculty of Agricultural Engineering, Department of Applied Mechanics, Voronezh State Agrarian University named after Emperor Peter the Great, Michurina ave., 1, Voronezh, 394087, Russia
[6]Department of Management, Organization of Production and Industrial Economics, Voronezh State University of Engineering Technologies, Revolyutsii ave., 19, Voronezh, 394036, Russia
E-mail: vasily.nik.popov@gmail.com

ABSTRACT

The purpose of the article is to develop a model of threats to the security of personal data in the implementation of distance educational services using mobile technologies. The model of threats to the security of personal data in the implementation of remote educational services using mobile technologies will allow forming requirements and recommendations for their protection and providing the initial data for the synthesis of the information security system, as a set of heterogeneous tools. Therewith, internal and external communications on data and management, the presence of a management system lead to the appearance of integrative effects and ensure the completeness and consistency of protection. The construction of a model of threats to the security of personal data in the implementation of distance educational services using mobile technologies is carried out by the method of information-logical analysis of existing approaches to the classification of threats to information security contained in the regulatory documents of regulators in the field of information security. The second method is the collection of data contained in domestic and international knowledge bases containing information about the vulnerabilities of mobile technologies used in the implementation of educational services and vectors of information security threats using these vulnerabilities. As a result of the work, a new classification scheme of information security threats has been formed, taking into account the peculiarities of personal data protection in the implementation of distance educational services using mobile technologies. The objectives of information security in the implementation of distance education services using mobile technologies have been analyzed and the analysis of possible technical measures for information protection has been carried out.

Keywords: *Distance Educational Service, Mobile Station, Security Gateway, Mobile Device Manager.*

1. INTRODUCTION

An individual approach to learning, free access to the electronic educational environment, the requirements of individual tracking and control over the processes of independent development of educational material by students have led to the widespread use of mobile technologies in secondary and higher schools.

In modern electronic educational systems (EES), mobile stations perform the following functions [1-4]:

1. implement the management of educational and methodological complexes located

in the EES, the coordination of pedagogical processes in the educational institution;

2. provide remote interaction within the teaching community and communication with students;

3. mobile devices for monitoring and direct educational impact on students are used to register the accumulation, processing, and transmission of necessary information;

4. provide direct access to the EES, including direct testing and knowledge control capabilities;

As the analysis of modern mobile applications shows, most of them have a client-server architecture [5]. Therewith, the client part runs under the mobile operating system (Android or iOS). Installation of the client-side is provided by an application store – a specialized platform where developers place their programs.

The user installs the program on the mobile station and interacts directly with the EES: studies the theoretical material of lectures receive advice from teachers, passes intermediate and final testing. Therein, the main component of the EES is the server of the educational institution.

The server is a platform hosted by an educational organization, which in most cases contains a Web application. The software installed on the server interacts with students' mobile clients through the Internet via an interface (API). The server of the educational organization is the basis of the EES. This is where information is processed and stored, mobile stations are managed, and user data is synchronized.

The functioning of the EES with the use of mobile technologies is associated with the processing of information in the technical media about the identification information of students, personal data of teachers, and confidential information of educational institutions [4].

Thus, the use of mobile technologies in addition to EES is associated with the organization of processing of confidential information of various contents, and following [6-8], requires the implementation of organizational and technical protection measures.

The analysis of standards and guidelines of regulators in the field of personal data protection, carried out in [9, 10], shows that in Russia, at present, the issues of information protection in information systems using mobile technologies are not regulated. Requirements for the protection of personal data information, technical and organizational protection measures contained in [7, 8] are focused on traditional computers. Similarly, the methodological approach to the development of an up-to-date model of threats to the IS of Personal data does not consider mobile systems [11].

Thus, the means of ensuring the security of information of mobile components of the system used in the personal data information system are not subject to regulatory regulation and, in this regard, are applied without legislative and methodological justification.

In this regard, the article solves a new practical and theoretical problem of forming a model of personal data security threats when implementing distance educational services using mobile technologies, which is a methodological basis for further developing a system of requirements and recommendations for ensuring information security in educational institutions when implementing distance educational services.

2. MODEL OF THREATS TO THE SECURITY OF PERSONAL DATA IN THE IMPLEMENTATION OF DISTANCE EDUCATIONAL SERVICES

Analysis of the current state of mobile systems has shown that the movement known today as BYOD (Bring Your Own Device) is gaining more and more popularity, meaning the use of personal stations in professional activities by specialists in various fields of activity. According to the results of the study, about 60% of office workers use mobile devices not only for personal purposes but also to perform certain work tasks [12].

Therewith, all the variety of mobile technologies can be divided into the following areas. The first group of technologies is used to coordinate work processes, manage data, and access corporate resources. The technologies of the first group increase the efficiency of the user's work, save his/her time, provide operational reference information, and improve remote interaction within organizations and professional groups. The second group of applications is used for direct interaction with objects of the physical world (CPCS). In the English-language literature, CPCS is called Industrial Control Systems (ICS) or Industrial Automation and Control Systems (IACS). In this case, the interaction between the elements of the system is organized at different levels of representation. The third group of technologies is information and reference services (including emergency services). The fourth group represents technologies for implementation in the terminal mode as a thin client with information systems (remote diagnostics, remote maintenance, etc.).

When organizing the functioning of mobile technologies, the main information circulating in technical means is the confidential information of various levels, technological information, and key information of cryptographic protocols of various types.

Thus, the use of mobile technologies is associated with the organization of processing confidential information of various contents and, following the requirements of the organization of information protection [6-8].

Analysis of state standards, regulatory documents of regulators in the field of confidential information protection, and information protection issues showed that currently there are no methodological recommendations for information protection in information systems using mobile technologies. Information security tools used in information systems that ensure the safety of mobile components are not subject to regulatory regulation and, accordingly, are applied without legislative and methodological justification.

Following the existing methodological approach to solving information security issues [8, 9], the beginning of solving the problem of information security is to develop a model of threats to information security, containing both the classification of threats and a brief description of the implementation of the most urgent threats.

A threat to information security is understood as a set of conditions and factors that create a risk of unauthorized, including accidental, access to personal data, which may result in the destruction, modification, blocking, copying, distribution of personal data, as well as other unauthorized actions during their processing in the personal data information system [11].

Traditionally, a threat to information security can be represented as a formal record of the following form:

threat of unauthorized access to ISPD: = <source of threat>, <vulnerability of ISPD>, <method of threat implementation>, <object of influence (program, protocol, data, etc.)>, <destructive action>.

The source of threats can be:

1. user;
2. malicious program;
3. instrument bug.

Concerning mobile technologies, users can be divided into several categories.

Employees of the institution. This category of users gets access to the organization's data and services from a mobile device. The level of access for users in this category is based on the requirements of their job responsibilities, the level of confidentiality of the information that the employee shall access, and the need to access this data using a mobile device. A set of mobile credentials is required for an employee of an institution, which is used to access the internal resources of the information system.

Partners are employees of third-party organizations who cooperate with the organization in performing certain tasks, including technical personnel who maintain the functionality of technical means. Partner users may need access to the system, applications, and infrastructure to perform assigned maintenance and maintenance work, but they are not granted access and rights as employees are. Partner users are typically provided with a limited set of mobile credentials that are used to access the organization's internal systems.

External users are individuals who are not associated with the organization, but who need access to the organization's public data through the interfaces provided and maintained by the organization. These interfaces are usually WEB applications, mobile applications, or other implementation mechanisms. External users usually do not need to have credentials to identify themselves. In some cases, an organization's data interfaces may have a set of locally used credentials that are only valid for the resource that is being accessed.

Suppliers of components, assemblies, and accessories for mobile devices. This category of security information threat sources can physically interfere with the operation of a mobile device before delivering and install malicious software.

Service providers of wireless technology services. This category of threat sources is dangerous due to the possibility of installing malicious software aimed at both affecting user data and the management processes of the mobile device. This category of threat sources, having full access to the cellular control network, can reconfigure the mobile device, gain access to the information resource of the mobile station, and cache user data on the carrier. In this case, not only information transmission channels using IP transport (MMS/SMS) can be used, but also control channels of the mobile network.

The most dangerous source of information security threats for mobile technologies is malware or malicious code. This is software designed to perform an unauthorized action that could compromise the confidentiality, integrity, or availability of a mobile device. Malware can be attached to instant messages, added to email, or uploaded to the Internet as an infected file. Malware

can also be embedded in downloaded apps. This category of information security threat sources can affect the operating system of a mobile device, compromise data or applications on a mobile device, or both.

The vulnerabilities of mobile technologies are:

1. vulnerabilities of wireless technologies that provide Internet access to mobile devices;
2. mobile device vulnerabilities;
3. vulnerabilities of mobile access services of information systems.

3. VULNERABILITIES OF WIRELESS TECHNOLOGIES THAT PROVIDE INTERNET ACCESS TO MOBILE DEVICES

Vulnerabilities of wireless technologies that provide Internet access to mobile devices are vulnerabilities that can be exploited by a threat source through the network at the application level or in applications, document files, or data (both data transfer protocols and management protocols), as well as using mobile device management protocols. Network security threats are related to vulnerabilities within the network and network protocols, as well as devices, applications, and data that reside on the network. The use of mobile devices actualizes the problem of analyzing network-based security threats, since cellular communication, WiFi, Bluetooth, Infrared Communication (IR), and Near Field Communication (NFC) technologies are used to transmit the digital stream, which has several specific vulnerabilities and have a fairly low level of security.

Mobile devices transmit a digital stream over cellular networks. Accordingly, they are characterized by vulnerabilities of the global GSM mobile communication system [11, 13, 14], supported by the provider, digital wireless data transmission technology for mobile communications, functioning as an add-on over 2G and 2.5 G EDGE, UMTS, HSDPA, and its high-speed version HSUPA. The vulnerabilities of cellular technologies with multiple access with code division CDMA, which use the Evolution-Data Optimized (EV-DO) and Long-Term Evolution (LTE) protocols for receiving and sending data over cellular networks, can also be considered.

Data and voice transmission over the managed network of mobile operators can be intercepted, and the configuration, as well as the main components, can be compromised through the control channels.

Mobile devices use Wi-Fi wireless networking, based on the IEEE 802.11a/b/g/n set of standards. These devices can connect to any mobile access point, personal or corporate access points, or similar devices for peer-to-peer communication. Devices that use Wi-Fi communication are vulnerable to interception by other Wi-Fi devices and wireless software, as well as signal analyzers [15-17]. Illegitimate access points (unauthorized scammers in an administratively managed domain) also pose a potential threat by exposing mobile devices to man-in-the-middle threats.

Bluetooth. Bluetooth short-range wireless technology provides a standard wire replacement protocol for connection. The technology is used both for data transfer between devices in a personal network and for commands, as well as for voice communication between the device and the headset. Bluetooth provides its encryption and authentication mechanisms but also has known vulnerabilities and information security threats, such as a key hijacking attack during session initiation [16].

Infrared port (InfraRed Data Association — IrDA). A type of short-range fiber-optic communication line. Even though IrDA technologies were most popular in the late 1990s and early 2000s and are now almost replaced by more modern analogs, such as WiFi and Bluetooth, several mobile devices can use them and, accordingly, the vulnerabilities of the IrLAP, IrLMP, IrCOMM, Tiny TP, IrOBEX, IrLAN, IrSimple, and IrFM specifications should be taken into account.

Infrared radiation is used both for data transmission between devices within a local area network (PAN) and for commands (one-way transmission). The infrared port does not provide encryption and authentication mechanisms and therefore has known vulnerabilities. Most of the information security threats associated with IrDA vulnerabilities depend on the provider, for example, due to a buffer overflow in the receiving infrared communication code.

Near field communication, NFC is a technology for wireless data transmission of a short-range, which makes it possible to exchange data between devices located at a distance of about 10 centimeters. This technology is a set of standards for low-power, miniature wiring replacement for point-to-point communication, mobile devices.

NFC vulnerabilities are related to the fact that the technology's protocol stack does not provide for cryptography during transmission. Standards for storing data in labels and maps, as well as their emulation, do not provide cryptographic protection during storage.

NFC services traditionally place excessive trust in the information stored in the mobile device, as a result, data filtering is not performed. NFC connectivity is primarily susceptible to physical layer attacks, such as signal interception and introduction, but specific implementations may contain additional vulnerabilities.

Vulnerabilities of mobile systems. Vulnerabilities of mobile systems can be classified by belonging to an element of the mobile system. Therewith, it is possible to identify the vulnerabilities of the hardware component of the mobile station, the vulnerability of the mobile operating system, and the vulnerability of the mobile application.

Vulnerabilities in the hardware component of the mobile station are mainly associated with errors or with intentionally installed hardware hatches contained in the firmware of the mobile station [18]. Also, additional hardware modules can be installed in mobile stations that implement various functions of tracking and intercepting information.

The vulnerabilities of the mobile operating system and mobile applications are similar to those that exist for traditional computers and are constantly detected [16, 19]. Operating system vulnerabilities can be exploited in a similar way to vulnerable applications. Operating system vulnerabilities pose a greater threat because the operating system operates with a higher level of privilege than applications. Mobile apps, like apps on other devices, can also be poorly written and vulnerable to attacks and exploitation. Many applications are vulnerable due to programming errors, design errors, or configuration choices in security capabilities.

Additionally, users disable the built-in security features of the OS, commonly known as "jailbreak" or "rooting". Disabling the OS's built-in security features allows users to install applications and system enhancements that would otherwise be restricted. There is a high level of risk associated with using modified devices with disabled mobile OS security features.

The main channels for the impact of information security threats are:

1. physical access to the mobile station;
2. access to the digital stream radio channel from the mobile station to the base station;
3. access to high-speed trunk digital stream transmission channels used by cellular operators;
4. access to the internal infrastructure of the organization's information system.

The main vulnerability of physical access to the mobile station is the possibilities associated with the access of an attacker when losing a smartphone. The loss of a mobile device jeopardizes the privacy, integrity, and availability of information. Also, the device may contain credentials for accessing the organization's information system, which creates an additional risk for it. Also, data on the mobile device may be lost if the device is not backed up.

Additionally, if an attacker can access the mobile station, it is possible to install malicious hardware or software that can collect or damage data, both on the device and in the organization's information system. An attacker can use external interfaces to connect a mobile device to a USB/Bluetooth modem. Also, an attacker can connect a computer or an external hard drive to clone, copy, destroy, delete, or modify the contents of a mobile device.

Existing vulnerabilities in the mobile device's built-in features, such as the camera and microphone, pose an increased security risk by creating a means to collect sensitive images or conversations.

Vulnerabilities leading to an increase in the possibility of implementing threats to information security can also be in mobile peripheral devices physically interacting with a mobile station (docking station, headsets, additional equipment).

The channel for realizing information security threats when accessing the radio channel for transmitting a digital stream from a mobile station to a base station is electronic wiretapping through a wireless network (Wi-Fi or GSM), the digital stream or voice signals can change, they can be manipulated or selectively blocked during transmission.

Channel of secondary electromagnetic radiation. Mobile stations are based on the operation of various discrete electrical components inside the device itself. They also emit out-of-band and multiple signals corresponding to their main radio interfaces, such as cellular, Bluetooth, NFC, or Wi-Fi. This radiation is within the radio frequency spectrum and can be captured and decoded since the information emitted by the CPU and its subsystems is mostly unencrypted. Therefore, vulnerable to observation by a third party both in the immediate vicinity and at a distance (for example, approximately 100 meters) using special receiving equipment.

In addition to intercepting signals from mobile stations, an additional threat to information security is jamming mobile station receivers (any wireless protocol used on a mobile device is susceptible to interference, including GPS, cellular,

Wi-Fi, and Bluetooth). Also, a specific threat affecting the radio channel is a flood threat that sends more information to the system than it can process.

Most mobile devices provide some level of capability to determine the actual geographical location of an electronic device (geolocation) in their applications. These apps can use this feature to display the current position on the map, search for nearby resources, or track the user's path. The ability of apps to show driving directions is even more popular among users. These location services may disclose the location of the device (or provide inaccurate information about the location of the user of the device due to external interference or manipulation).

The channel for the implementation of the information security threats from the network of a cellular provider leads to the possibility of violating the confidentiality and integrity of information since high-speed backbone networks are used for operation, which are an integral part of the country's public communication networks [20-25].

The objects of influence of information security threats are information resources containing personal data, confidential service information of the organization, as well as technological information, software, and hardware for information processing, personal data protection, information exchange, and telecommunication channels. Depending on the location of the objects of threat impact, they can be classified into the following types:

1. information resource contained in the mobile station;
2. digital stream transmitted over the radio channel "mobile station — base station of the cellular provider";
3. digital stream transmitted over the radio channel "mobile station — Wi-Fi access point";
4. digital stream transmitted over the network of a cellular service provider;
5. digital stream transmitted over high-speed backbone networks that are part of the country's public communication networks;
6. a digital stream processed on the organization's network.

Depending on the type of threat impact objects can be divided into:

1. open data;
2. data encrypted with a symmetric cipher (DES, AES);
3. data encrypted with an asymmetric cipher (A5) [25].

The destructive action of a threat to information security.

According to the type of destructive actions affecting confidential information in mobile technologies, the following classes of threats to information security are traditionally distinguished: [10]:

1. leading to a breach of confidentiality;
2. leading to a violation of integrity;
3. leading to a violation of accessibility.

Therewith, it is necessary to consider several specific information security threats caused by the use of mobile stations and do not directly violate the state of security of personal data.

During operation, the mobile station transmits the service information of the pair to the base station (LAC, CellID), IMSI, Network Identity and Time Zone, etc. The service data transmitted by the mobile station can be used to analyze the behavior of the user and/or organization (for example, local and remote logs). There is also widespread use of dedicated software and services from mobile service providers to combine geolocation data with SSID information to collect location information about specific wireless networks that are shared by their customers. There are examples of software installed by a mobile service provider that is used to track user behavior, as well as performance indicators of a mobile station or mobile service. This data can also be sent directly to the supplier or a third party.

During the use of the mobile station, the user can install an application containing malicious code that allows reconfiguring the mobile device (directly or indirectly) or offering the service directly or through a third-party device.

Ransomware has become an extremely common class of malicious software for mobile systems. As a rule, the operation of the mobile station is blocked, requiring a ransom from the victim, after payment of which the user is returned control of the smartphone or tablet. Also, criminals choose call history, contacts, photos, or messages as targets, which almost always forces the user to pay the requested amount [25].

Botnets consisting of compromised mobile stations are another pressing threat to information security. Infected devices that are part of botnets are under the control of attackers, who at any time can order them to initiate a DDoS attack on a resource or start mass mailing of spam emails [19].

The composition of the elements for describing threats to the information security of mobile technologies is shown in Figure 1.

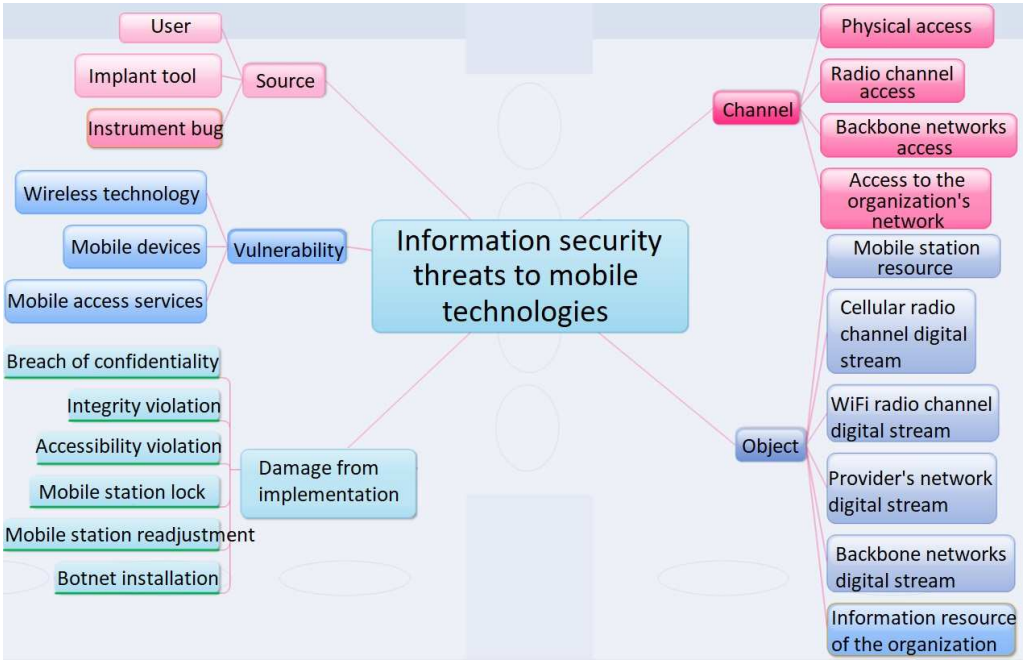

Figure 1: Composition Of Elements For Describing Threats To Information Security Of Mobile Technologies

Despite the completeness of consideration of the totality of threats to information security in the provision of distance educational services, the issues of information protection of the server part of the system for the provision of distance educational services remained outside the scope of the problem being solved. Currently, the software of educational organizations installed on the EOS servers is outside the legal field of regulators in the area of information protection, the threat model for this category of programs is not formed and requires a solution. The problem is compounded by the fact that this category of programs is developed by foreign companies and requires legislative measures for certification (verification of compliance with the requirements of regulators on protection against unauthorized access, control of undeclared functions) and certification during commissioning following the norms and rules of Russia as ISPD.

4. METHODS AND WAYS TO PROTECT PERSONAL DATA WHEN PROVIDING DISTANCE EDUCATION SERVICES USING MOBILE TECHNOLOGIES

When constructing a system of PD protection in the provision of distance educational services using mobile technologies, it is advisable to consider the entire set of information protection tools presented in detail in [26, 27]. In particular, it is advisable to consider the following components of the system: Mobile Device Manager (MDM), Mobile Application Manager (MAM), Mobile App Store (MAS), identification and access management (IAM), gateway and security stack (GSS), virtual private network (VPN) technologies.

Mobile Device Manager (MDM). The MDM implements the personal data security policies adopted in the organization, which are applied when configuring the settings and operating modes of users' mobile devices. In this case, the following parameters are configured:

1. Hardware parameters, such as permission to use Bluetooth, NFC
2. Password parameters, including password length and quality
3. Encryption options
4. Browser settings, such as disabling cookies, blocking jscript
5. Allowed and prohibited apps
6. Compliance policies, such as OS version

When implementing the threat of violating the physical integrity of the user's mobile station, MDM implements the removal of confidential data and applications from the device, as well as performing a complete cleanup. Also, if necessary, clearing of secret codes or remote locking is implemented.

The MDM application may include licenses for antivirus support.

Examples of the most effective MDMs are Microsoft Intune, AirWatch by VMware, Citrix XenMobile. The entire process of managing mobile

devices can be divided into five main steps shown in Figure 2.

Figure 2: Mobile Device Management Process Using Standard Mdm Solutions

When registering, the User shall install a special application on their smartphone. After the user has installed the app and connected to the mobile service, the device will be registered. Once the device is registered, it can be managed.

Mobile Application Manager (MAM). This class of ISS provides a subset of the functions provided by mobile device management. The program provides comprehensive distribution, configuration, data management, and lifecycle management for specific applications installed on a mobile device. As with MDM, key features of MAM include the set of supported devices, platforms, and applications, as well as the security of the mechanisms used to authenticate the device as well as manage and control. MAM can also include diagnostic features such as remote login, reporting, and troubleshooting. Some MAM implementations are designed to support a small, specialized set of software, such as virtual application containers ("Sandboxes"), rather than being applied to all applications on the device. Customized MAM implementations may not integrate with more general MDM implementations and are therefore considered a separate component of a mobile solution. An example of the most effective MAM is Kaspersky Security for Mobile, SOTI Mobicontrol.

The approaches to protect personal data from information security threats aimed at vulnerabilities in mobile applications are based on the use of specially developed software packages placed in the information resource of an educational organization – a mobile application store (MAS). Public app stores (that is, external app stores) offer mobile apps for sale (or free) to all users. Organizations can obtain licenses for software to manage their app store, which is only available to the organization's staff. These "vaults" provide a selection of approved applications that can be downloaded and installed on approved employee and patient devices. Some mobile app store implementations may support multiple mobile platforms, but many of them are limited to a single platform, requiring remote access to work with multiple app stores.

When organizing the protection of information resources of a university from information security threats aimed at vulnerabilities in mobile access services for information systems, identification tools and access control (IAM) are used. This class of ISS is used to integrate services such as authentication and authorization into a mobile solution to form a single security profile for each user. The IAM system ensures consistent application of security policies for all mobile services and allows integrating the corporate authentication and authorization systems with the mobile solution. For example, using an IAM system in combination with an MDM system allows each user of a mobile solution to have multiple devices (such as a tablet and a smartphone) configured with the same access level and the same security profile. IAM systems can also be used to provide data synchronization between multiple devices and users.

Separately, it is necessary to consider the many threats to information security caused by wireless technologies that provide Internet access to mobile devices.

Vulnerabilities of wireless technologies that provide Internet access to mobile devices are vulnerabilities that are implemented over the network at the application level or in applications, document files, or data (both data transfer protocols and management protocols). The considered class of threats is related to vulnerabilities of the network and network protocols, as well as devices, applications, and data that provide work with the network. The use of mobile devices actualizes the problem of analyzing network-based security threats, since cellular communication, WiFi, Bluetooth, Infrared Communication (IR), and Near Field Communication (NFC) technologies are used to transmit the digital stream, which has several specific vulnerabilities and have a fairly low level of security.

Mobile devices transmit a digital stream over cellular networks. Accordingly, they are characterized by vulnerabilities of the global GSM mobile communication system [27], supported by the provider, digital wireless data transmission technology for mobile communications, functioning

as an add-on over 2G and 2.5 G EDGE, UMTS, HSDPA, and its high-speed version HSUPA.

Mobile devices use Wi-Fi wireless networking, based on the IEEE 802.11a/b/g/n set of standards. These devices can connect to any mobile access point, personal or corporate access points, or similar devices for peer-to-peer communication. Devices that use Wi-Fi communication are vulnerable to interception by other Wi-Fi devices and wireless software, as well as signal analyzers. Illegitimate access points (unauthorized scammers in an administratively managed domain) also pose a potential threat by exposing mobile devices to man-in-the-middle threats.

Security requires a gateway and a security stack (GSS). Mobile devices, like almost all computing devices, can be used to attack other network devices. The unique dual connectivity (cellular and wireless Ethernet) of mobile devices makes them ideal platforms for bypassing traditional network boundary protection. To prevent damage from a compromised mobile device, access to an organization's information resources should be restricted through one or more known network routes (i.e. Gateways) and verified by standard network defenses such as stateful packet inspection, intrusion detection, and digital stream filtering. These standard defenses are collectively known as a "filter stack" because they serve to filter unwanted network traffic and are usually configured in a "stack" with traffic passing through each filter in sequence. The gateway and security stack typically operates at the session and lower layers of the OSI network model.

Also, when transmitting a digital stream of a mobile station through high-speed trunk channels for transmitting a digital stream used by cellular operators, it is possible to ensure information protection only using cryptographic information protection methods. Therewith, security tools that implement a virtual private network (VPN) are used. This class of security features provides a reliable method for creating secure connections between mobile devices and information resources when using public unmanaged networks. VPN technologies are usually used only by authorized and partner users, but some technologies allow establishing VPN connections for external users [21].

When using a VPN, mobile systems use a radio access network (RAN) and a packet core (PS Core) as shown in Figure 3.

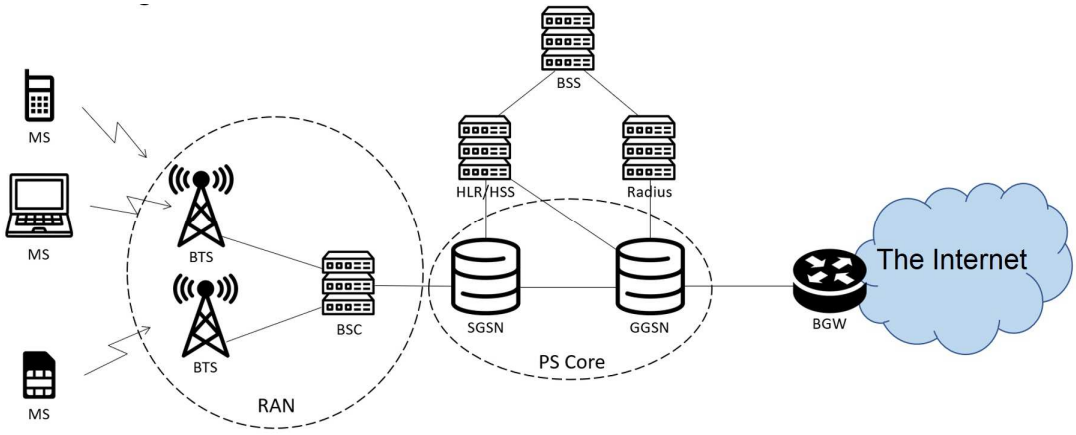

Figure 3: Application of VPN Technology in Mobile Systems

Each mobile station registered in the packet network, before starting to transmit data, shall request the creation of a data transfer session (PDP context) in the GGSN packet network core router [27]. When initiating a session, the following parameters are used in the request to GGSN: APN, username, and password. APN (access point) is a parameter that provides the mode of operation of the GGSN: depending on which APN the session is initiated from, the GGSN operates in different ways. As a result of the successful processing of the user's request, the GGSN shall activate the data transfer session and inform the device of its parameters, in particular, the IP address and DNS addresses issued to the device. Examples of the most effective VPNs are Twingate, Cloudflare for Teams, and Zscaler Private Access [22-28].

The requirements for deploying special services that ensure the safe use of mobile systems have led to the integration of heterogeneous tools into a single security architecture. In general, the security architecture of remote educational services in the organization can be represented in the form shown in Figure 4, which reflects the relationship of

the organization"s infrastructure interacting through a gateway that protects the internal information structure from attacks arising from the use of mobile systems with the corporate mobile service and possible external mobile services.

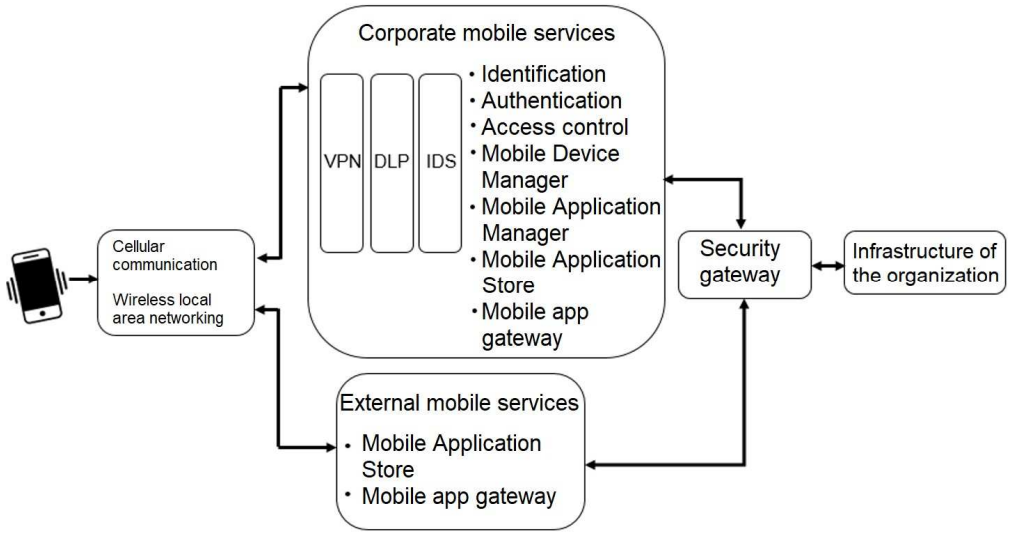

Figure 4: Generalized Security Architecture of Distance Education Services in the Organization

5. CONCLUSION

An analysis of the features of using mobile technologies in education to improve the efficiency of providing educational services showed the urgency of the problem of protecting personal data from new information security threats caused by the use of mobile technologies. The implementation of special mobile security services is required to protect personal data when providing distance education services. Therewith, along with the VPN, IAM technologies were widely used to protect the information, the use of specific information protection technologies such as MDM and MAM is required.

The analysis of threats to the information security of hardware and software of mobile technologies, carried out in the article, showed a significant complication of the problem of ensuring information security with a significant increase in the efficiency of functioning when using this technology. The use of mobile stations as the main tool for accessing the educational environment, the participation of a third party in the processing of confidential information (cellular service provider, wireless access service provider, organizations operating high-speed backbone digital stream transmission channels) led to a significant complication of the information security threat model. New threats to information security caused by the use of mobile technologies and new vectors of the implementation of threats discussed in the article made it possible to refine the model of threats to information security and develop a classification scheme for threats to information security.

A significant limitation of the proposed model of PD threats in the provision of distance education services is the lack of an analysis of the problem of information protection behind the GSS security gateway. The limitations of the proposed model are associated primarily with the absence in the existing regulatory framework for the analysis of threats to the security of information on the server-side of the system for providing distance education. Accordingly, a further direction of research in the field of information security in distance education is only a logical justification of security goals, security tasks, security requirements for a mobile component, but the formation of a threat model for the server part of the distance education system.

REFRENCES:

[1] A.T. Abdykarimova, L.S. Krivankova, and R.Zh. Zheksembaeva, “Mobilnye ustroistva i prilozheniya v obrazovanii: neobkhodimost ili dan vremeni [Mobile devices and apps in education: a necessity or a tribute to the times]”, *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk*, No. 2, 2018, pp. 36-38.

[2] V.B. Luzgina, and Zh.A. Stakhovskaya, "Opyt ispolzovaniya mobilnykh tekhnologii v obrazovatelnoi srede vuza [Experience of using mobile technologies in the educational environment of the university]", *Obrazovatelnye tekhnologii i obshchestvo*, No. 3, 2016, pp. 463-472.

[3] S.S. Koloskov, V.N. Babeshko, A.V. Samochadin, and Yu.A. Koshlich, "Metodika aprobatsii vnedreniya mobilnykh servisov na platforme upravleniya mobilnymi ustroistvami v vuzakh [Methodology for testing the implementation of mobile services on a mobile device management platform in universities]", *Ekonomika. Informatika*, Vol. 19, No. 216, 2015, pp. 152-159.

[4] D.Yu. Raichuk, A.V. Samochadin, S.M. Nosnitsyn, and I.A. Khmelkov, "Kompleks mobilnykh sredstv podderzhki uchebnogo protsessa [Complex of mobile tools to support the educational process]", *Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika, telekommunikatsii i upravlenie*, Vol. 6, No. 210, 2014, pp. 7-15.

[5] S. Retabouil, *Android NDK. Razrabotka prilozhenii pod Android na S/S++ [Development of applications for Android in C / C ++ /]*. Moscow, Russia: "DMK press. Elektronnye knigi", 2014, 496 p.

[6] State Duma of the Federal Assembly of the Russian Federation, *Federal Law of the Russian Federation of July 27, 2006, No. 152-FZ "On Personal Data"*. Rossiiskaia Gazeta [Ros. Gaz.] 29.07.2006 No. 165 (Russ.).

[7] Government of the Russian Federation, *Decree of 01.11.2012 No. 1119 "On approval of requirements for the protection of personal data during their processing in information systems of personal data"*. Rossiiskaia Gazeta [Ros. Gaz.] 07.11.2012 No. 265 (Russ.).

[8] Federal Service for Technical and Export Control (FSTEC) of Russia, *Order of February 18, 2013, No. 21 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems"*. [Online]. Available: https://fstec.ru/normotvorcheskaya/akty/53-prikazy / 691 (access date: September 26, 2019).

[9] V.P. Gulov, V.A. Khvostov, A.V. Skrypnikov, V.P. Kosolapov, and G.V. Sych, "Analiz ugroz bezopasnosti informatsii pri obrabotke personalnykh dannykh v mobilnoi meditsine [Analysis of information security threats when processing personal data in mobile medicine]", *Sistemnyi analiz i upravlenie v biomeditsinskikh sistemakh*, Vol. 19, No. 2, 2020, pp. 129-138.

[10] V.P. Gulov, V.A. Khvostov, V.P. Kosolapov, and G.V. Sych, "Analiz osobennostei zashchity personalnykh dannykh v mobilnoi meditsine [Analysis of the peculiarities of personal data protection in mobile medicine]", *Sistemnyi analiz i upravlenie v biomeditsinskikh sistemakh*, Vol. 19, No. 3, 2020, pp. 171-176.

[11] Federal Service for Technical and Export Control (FSTEC) of Russia, *Methodological document of the FSTEC of Russia. Basic model of threats to the security of personal data when they are processed in personal data information systems (extract),* 2008. [Online]. Available: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (access date: January 10, 2019).

[12] *Mobile managers.* [Online]. Available: https://www.comss.ru/list.php?c=mobilemanager (access date: November 10, 2020).

[13] K. Shestakova, *What vulnerabilities smartphone manufacturers intentionally leave in your smartphone,* December 18, 2019. [Online]. Available: https://www.iphones.ru/iNotes/sekretnye-uyazvimosti-v-vashem-smartfone-12-11-2019 (access date: March 31, 2020).

[14] O. Shwartz, A. Cohen, A. Shabtai, and Y. Oren, "Shattered Trust: When Replacement Smartphone Components Attack" in *11th USENIX Workshop on Offensive Technologies (WOOT)*, 2017. [Online]. Available: https://www.usenix.org/conference/woot17/workshop-program/presentation/shwartz (access date: January 10, 2019).

[15] E. Mixon, and C. Steele, *MDM intends to centralize and optimize the functionality and security management of a mobile communications*. [Online]. Available: http://searchmobilecomputing.techtarget.com/definition/mobile-device-management (access date: January 10, 2017).

[16] *Apowersoft ApowerManager (Phone Manager) version: 3.2.6.1*. [Online]. Available: https://4pda.ru/forum/index.php?showtopic=831525 (access date: November 10, 2020).

[17] I.O. Kutsenko, and D.A. Zhaivoronok, "Analiz uyazvimostei besprovodnykh setei [Wireless vulnerability analysis]", *Vestnik VI MVD Rossii*, No. 4, 2007, pp. 140-143.

[18] A.V. Morozov, and V.G. Shakhov, "Analiz atak na besprovodnye kompyuternye interfeisy [Analysis of attacks on wireless computer interfaces]", *Omskii nauchnyi vestnik*, Vol. 3, No. 113, 2012, pp. 323-327.

[19] C. Montero-Luque, *The science of app-wrapping*, May 7, 2013. [Online]. Available: https://web.archive.org/web/20130701173859/http://www.NetworkWorld.com/news/tech/2013/050713-app-wrapping-269503.html (access date: November 10, 2020).

[20] *The Attack Vector "BlueBorne" Exposes Almost Every Connected Device*. [Online]. Available: https://www.armis.com/blueborne/ (access date: March 31, 2020).

[21] V.I. Komashinskii, and A.V. Maksimov, *Sistemy podvizhnoi radiosvyazi s paketnoi peredachei informatsii. Osnovy modelirovaniya [Mobile radio communication systems with packet data transmission. Basics of modeling]*. Moscow, Russia: Goryachaya liniya. Telekom, 2007, 176 p.

[22] *Secure access to private data for your distributed workforce*. [Online]. Available: https://www.twingate.com (access date: March 31, 2020).

[23] *Cloudflare for Teams provides fast, secure and seamless access to any application and the Internet from any device, anywhere*. [Online]. Available: https://www.cloudflare.com/ru-ru/teams/ (access date: March 31, 2020).

[24] *Zero Trust Network Access for your Private Apps*. [Online]. Available: https://www.zscaler.com/products/zscaler-private-access (access date: March 31, 2020).

[25] The White House, *Digital Government: Building a 21st Century Platform to Better Serve the American People*. May 23, 2012. [Online]. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/egov/digital-government/digital-government-strategy.pdf (access date: March 12, 2015).

[26] V.P. Gulov, V.P. Kosolapov, A.V. Khvostov, and G.V. Sych, "To the question of the choice of the system of protection of personal data in medical information systems by quality criteria", *Journal of New Medical Technologies, eEdition*, Vol. 3, 2018, pp. 117-123.

[27] V.P. Gulov, V.A. Khvostov, A.V. Skrypnikov, V.P. Kosolapov, and G.V. Sych, "Methods of ensuring the security of personal data in medical information systems using mobile technologies", *System Analysis and Management in Biomedical Systems*, Vol. 19, No. 4, 2020, pp. 132-140.

[28] I.G. Drovnikova, E.A. Rogozin, A.V. Hvostov, and A.A. Zmeev, Analysis of architecture and clustering structure of automatic systems at the substantiation of the requirements to information security, *Technology of technosphere safety*, Vol. 3, No. 67, 2016, pp. 277-283.