

**MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
FACULTY OF AERONAVIGATIONS, ELECTRONICS AND
TELECOMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATION AND RADIO ENGINEERING
SYSTEMS**

ADMIT TO DEFENCE
Head of the Department

R. Odarchenko
“ _____ ” _____ 2022

**DIPLOMA WORK
(EXPLANATORY NOTE)**

**BACHELOR'S DEGREE GRADUATE
BY SPECIALITY "TELECOMMUNICATIONS AND RADIO ENGINEERING"**

Topic: «Information and communication system for Online banking»

Performer: _____ M. Kolchyn
(signature)

Supervisor: _____ O. Plyushch
(signature)

N-controller: _____ D. Bakhtiyarov
(signature)

Kyiv 2022

NATIONAL AVIATION UNIVERSITY

Faculty of aeronavigations, electronics and telecommunications

Department of telecommunication and radio engineering systems

Speciality: 172 "Telecommunications and radio engineering"

Educational professional program: Telecommunication systems and networks

ADMIT TO DEFENCE

Head of the Department

R. Odarchenko

“ ” 2022

TASK
for execution of bachelor diploma work

Kolchyn Mykola

(full name)

1. Topic of diploma work: «Information and communication system for Online banking» approved by the order of the rector from « 25» March 2022 №433/сr.
2. The term of the work: from 25 April 2022 to 10 June 2022.
3. Initial work data: Memory – 2 GB, 4 GB. Port bandwidth – 8 Gbit/s. Number of routes – 800,000 with default 4 GB, up to 4M with 32 GB. Wi-Fi speed – 1.3 Gbps. Speed of LAN ports – 1 Gbps. Wi-Fi frequency – 2.4 GHz and 5 GHz (dual band).
4. Explanatory note content: Introduction. Research of typical architecture of Online banking. Information security subsystem for Online banking. Protection of information in the electronic document system. Development of the architecture of the information and communication system of the Online banking.
5. List of required illustrative material: figures, tables.

6. Work schedule

№ n/p	Task	Term implementation	Performance note
1.	Develop a detailed content of the sections of diploma work	25.04.2022- 30.04.2022	Done
2.	Introduction	01.05.2022- 06.05.2022	Done
3.	Research of typical architecture of Online banking	07.05.2022- 16.05.2022	Done
4.	Information security subsystem for Online banking	17.05.2022- 23.05.2022	Done
5.	Protection of information in the electronic document system	24.05.2022- 02.06.2022	Done
6.	Development of the architecture of the information and communication system of the Online banking	03.06.2022- 06.06.2022	Done
7.	Elimination of shortcomings	06.06.2022- 10.06.2022	Done
8.	Preparing the electronic report and illustrations	11.06.2022- 12.06.2022	Done

7. Date of issue of the assignment: “25” April 2022.

Supervisor _____ O. Plyushch
(signature) (full name)

Accepted task for execution _____ M. Kolchyn
(signature) (full name)

ABSTRACT

Graduate work on the topic «Information and communication system for Online banking». It contains 75 p., 7 tables., 26 figures., 25 references.

Keywords: Demilitarized Zone, Electronic document management system, Online banking, Open Systems Interconnection, Security

The object of study is the Online banking and equipment for the development of the banking network.

The subject of research is the information and communication architecture of the bank.

The purpose of the thesis is to analyze one of the types of banking services - Online banking, identify problems of its implementation and prospects for development in Ukraine, as well as development opportunities, taking into account the rapid spread of information technology in the field of finance. Identify the advantages and disadvantages of Online banking. Develop the architecture of the information and communication network of the bank.

Research of methods – the Alfresco system for the operation and storage of information in the electronic document management system and the architecture of the banking network was presented. The architecture of the banking network consists of Core router with memory 2 GB, Core switch with bandwidth 8Gbit/sec, ATM router , Branch router with memory 4 GB and Internet router with frequency 2.4 GHz and 5 GHz (dual band).

CONTENTS

LIST OF ABBREVIATIONS	7
INTRODUCTION	8
CHAPTER 1	10
RESEARCH OF TYPICAL ARCHITECTURE OF ONLINE BANKING.....	10
1.1. The concept of Online banking	10
1.2. Advantages and disadvantages of Online banking.....	16
1.3. Typical solutions for deploying Online banking.....	18
1.4. Communication network architecture for Online banking	22
CONCLUSION TO CHAPTER 1.....	24
CHAPTER 2.....	26
INFORMATION SECURITY SUBSYSTEM FOR ONLINE BANKING	26
2.1. Cybersecurity in Online banking.....	26
2.2. Systems and mechanisms for the security of Online banking	31
2.3 Security software for Online banking	34
2.4 Information security of Online banking	34
CONCLUSION TO CHAPTER 2.....	36
CHAPTER 3.....	38
PROTECTION OF INFORMATION FOR ELECTRONIC DOCUMENT SYSTEM	38
3.1 Characteristics of threats	38
3.2 Comprehensive information protection in the EDMS	42
3.3 Ways to solve the problems of electronic document management.....	46
3.4 Creating users in the system and grouping	49
CONCLUSION TO CHAPTER 3.....	58
CHAPTER 4.....	59
DEVELOPMENT OF THE ARCHITECTURE OF THE INFORMATION AND COMMUNICATION SYSTEM OF THE ONLINE BANKING.....	59
4.1 Presentation of electronic banking services	59

4.2 The use and importance of ICS in online banking	60
4.3 Banking network architecture	62
4.4 Technical characteristics and cost of equipment used in the banking network	64
CONCLUSION	71
REFERENCES	73

LIST OF ABBREVIATIONS

API – Application Programming Interface

AS – Automated system

ATM – Asynchronous Transfer Mode

DLL – Dynamic Link Library

DMZ – Demilitarized Zone

ICS technologies – Information and communication technologies

IP – Internet Protocol

LSASS – Local Security Authority Subsystem Service

ND – Network displays

OSI – Open Systems Interconnection

SAM – Security Account Manager

SRM – Supplier relationship management

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

USB – Universal Serial Bus

VLAN – Virtual Local Area Network

INTRODUCTION

Actuality of theme. The dynamic development of information and communication technologies in recent years has significantly changed the banking industry. The technology gives banks new benefits and opportunities to expand their customer base and reduce costs, offering customers a more convenient way to access their products and services. Issues of understanding the direction of development of modern banking technologies and the possibility of their effective implementation in banking are relevant for all banking institutions. Their implementation in the bank's activities will determine not only the profit and competitiveness of the bank in the market of financial and banking services, but also its functioning as a whole.

The purpose and objectives of the study. Analyze one of the types of banking services - Online banking, identify problems of its implementation and prospects for development in Ukraine, as well as development opportunities, taking into account the rapid spread of information technology in the field of finance. Identify the advantages and disadvantages of Online banking. Develop the architecture of the information and communication network of the bank.

To achieve this goal, the following scientific problems are solved.

1. To reveal the essence, the concept of remote banking, to identify a number of advantages and disadvantages.
2. Analyze current solutions for the deployment of Online banking.
3. Consider current network solutions for the banking system.

The object of study is the Online banking and equipment for the development of the banking network.

The subject of research is the information and communication architecture of the bank.

Research methods. In this paper, the Alfresco system for the operation and storage of information in the electronic document management system and the architecture of the

banking network was presented. The architecture of the banking network consists of Core router, Core switch, ATM router, Branch router and Internet router.

The practical significance of the results obtained. Materials of the diploma work are recommended to be used in interaction with the electronic document management system and its databases and in the development of information and communication network for the Online bank.

Approbation of the obtained results. The main provisions of the work were reported and discussed at the following conferences:

Scientific and practical conference "Problems of operation and protection of information and communication systems", Kyiv, 2022.

CHAPTER 1

RESEARCH OF TYPICAL ARCHITECTURE OF ONLINE BANKING

1.1. The concept of Online banking

Online banking or Web-banking is one of the types of remote banking, by means of which access to accounts and account transactions is provided at any time and from any computer via the Internet. The Internet, as a financial tool, provides banks with excellent opportunities to save on standard transactions related to payment turnover. The cost of the transaction carried out by means of e-business systems is reduced by 80-90%, i.e. the bank does not bear the costs of visual control of submitted documents and communication with the client, and only controls the transaction by means of electronic systems [1].

Remote banking is an interconnected set of information and Internet technologies, as well as tools for providing banking services through self-service. Of course, in the scientific literature there is only an interpretation of the concept of "banking service". For example, V.I. Mishchenko and N.G. Slavyanska gives the following definition of banking services: "Banking service is the result of a banking operation aimed at meeting the needs of consumers-customers of the banking institution" [2]. Shpyliovyi V.A. The concept of "banking service" is defined as a complex result of the banking institution, to maximize the growing customer requirements for banking operations or to attract temporarily free resources aimed at making a profit [3, p. 28].

Of course, the activities of a banking institution are commercial, so any type of service must bring some benefits to the bank, so, as already mentioned, e-banking can be classified as a separate type of banking institution, and give it the following definition - a commercial type of remote banking to meet the needs of customers through an electronic server around the clock with the maximum possible distance from the branch.

At the heart of the emergence and development of Internet banking are a variety of remote banking, used in the earlier stages of banking [1]:

- PC banking (access to a bank account using a personal computer, carried out using a direct modem connection to the banking network);
- Telephone banking (telephone billing);
- Video banking (system of interactive communication of the client with the bank staff).

Today, we can distinguish the following types of remote banking services [4, 5]:

1. Internet banking is the most convenient, modern and advanced technology of remote banking. Since its inception, it has quickly gained popularity in the world of banking, and the development of computer technology has provided great opportunities for the development and implementation of new ideas.

2. Telephone (mobile) banking - one of the most common types, but still not quite convenient at present. It provides the same capabilities as Internet banking, but is less productive compared to it.

3. SMS-banking is a kind of telephone banking. Suitable for fairly primitive tasks: transfer funds, view balances, etc. As a rule, the possibilities of this type of service are quite limited.

4. Video banking - a little common in the Ukrainian market of services. It is an opportunity for the client to interact with the bank's employees. Communication with the bank is through special devices that work through secure channels of interaction.

5. PC-banking (classic system "client-bank") - this system provides access to the bank account (product) using a personal computer and a direct modem connection to the bank's system. In most cases, systems of this type are chosen by legal entities and corporate clients. They work locally with financial documents. The inconvenience of the system is that it is possible to use this system only from one workplace. In turn, this provides reliable security, which is most important for corporate clients.

Internet banking is a type of "home banking" technology remote banking service, which allows the client to receive banking services without visiting the bank office. This technology appeared in the early 80's and has changed significantly since then. There are three main stages in the development of Home banking services:

- Telephone banking - a banking service based on the use of telephones with tone dialing;
- PC-banking, which allows the client with the help of a personal computer and modem to directly connect to the bank's servers and perform banking operations (not via the Internet);
- Electronic banking differs from PC-banking in that extensive Internet capabilities are used to organize interaction with the bank. Is the most promising embodiment of "Home banking" technology.

To work in the Internet banking system requires: any modern computer, any operating system (Windows, Linux, Mac OS, Solaris, FreeBSD, etc.) and Web-browser (Internet Explorer, Mozilla, Netscape, Opera, etc. .), Internet connection. The SoftUpdate caching mechanism is used to speed up the loading of the Java applet.

The idea of creating Internet banking as a system originated in the United States (October 18, 1995 Security First Network Bank). One reason was the then restriction on banks opening branches in other states and finding options for providing services to customers in another state or country.

The main purpose of implementing the use of electronic banking services is the availability for customers to cooperate with the bank through the electronic banking system. The client's means of access to remote services are a mobile phone, a personal computer, an ATM and other means of communication.

Possibilities of remote service simplify and optimize economic activity. It should be noted that the first steps in the introduction of electronic banking by the bank were business requirements to simplify settlement operations with the bank. The result was the emergence of so-called "Client Bank" services. The advantages of this service are:

- comprehensive remote banking, which allows you to generate payment documents in the system, without time;
- protection of private information of clients and volumes of transactions, for example, use of digital signatures, coding of information, different levels of access to information, etc .;

- reducing the likelihood of operational errors - the use of templates, fixing the frequency of payments, etc .;
- tariffs for payments using the "Client-Bank" system are usually lower than tariffs for payments on paper;
- making payments from anywhere in the world, even during non-business hours.

The main reasons that encourage banks to implement Internet banking in their activities are:

- significant demand among customers for this service;
- minimum fees for one transaction in the Internet banking system. For example, the cost of financial transactions in the office is \$ 1.07, in the mail - \$ 0.73, by phone - \$ 0.35, through an ATM - \$ 0.27, through the global network - \$ 0.10 [6];
- significant competitive advantage.

The following basic principles of banking service must be observed when servicing clients via the Internet bank:

- availability. Like any other banking product, services provided over the Internet should be available to everyone. This means that there should be no restrictions for customers, for example, the size of the statutory fund, the type of business, etc .;
- ease of use. Each of the proposed banking products should be as simple as possible. Working with it should not take the client much time, the learning process should be fast and accessible;
- confidentiality. The bank must guarantee the client the protection of information directly related to the client, work and its counterparties from unauthorized access. This principle is especially relevant for customer service via the Internet;
- efficiency. All transactions performed by the client must be reflected in the bank "in real time". Otherwise, services over the Internet lose their meaning;
- complexity. The ideal option is when the bank completely duplicates its services via the Internet, ie provides the same services via the Internet as through the bank's branch. Today, the practical observance of this principle is a matter of the future due to the imperfection of domestic legislation, which does not allow to identify a person without visiting the bank;

- maintaining the integrity of information. The information about the operation cannot be changed, corrected or supplemented by anyone;
- authentication. Buyers and sellers need to be sure that all parties involved in the transaction are who they claim to be;
- seller's risk guarantees. When trading online, the seller is exposed to many risks associated with the rejection of the product and the dishonesty of the buyer. The magnitude of risks must be agreed with the payment system provider and other organizations involved in retail chains through special agreements;
- minimization of transaction fees. Transaction processing fees, orders and payment for goods are, of course, included in their value, so lowering the transaction price increases competitiveness. It is important to note that the transaction must be paid in any case, even for the buyer's refusal of the goods [7].

In Ukraine, it is enshrined in law that Internet banking (client-Internet-banking system) is an element of remote banking. The concept of remote banking is considered in paragraph 11.1. Resolutions of the NBU dated 21.01.2004 № 22 "On approval of the Instruction on non-cash payments in Ukraine in national currency": remote banking systems allow the client to quickly maintain their bank accounts and exchange technological information specified in the agreement between the bank and the client. The client can remotely service the account using the systems "client - bank", "client - Internet - bank", "telephone banking", etc. [8]. Not only banks but also specialized companies can provide Internet banking services.

The main features of Internet banking include:

- currency exchange;
- opening deposit accounts;
- sale of insurance and mutual fund units;
- order a payment card;
- review of account balances;
- payment of utility bills;
- receiving statements on the movement of funds on accounts;
- consultations of the bank's specialists on-line;

- SMS and e-mail notifications about account transactions;
- money transfers and interbank payments to the accounts of individuals and legal entities;
- interbank payments in the national currency of Ukraine [9].

In Ukraine, the Web-banking market is in its infancy. The domestic system allows you to send the following financial documents to the bank:

- payment order and payment requirements;
- payment order in foreign currency, with the support of the directory of SWIFT-codes;
- application for purchase or sale of foreign currency;
- application for currency conversion;
- salary information (for salary projects) and letters, etc.

Users of this system can perform the following types of operations:

- send payments for write-off during the bank's business day;
- receive current information on crediting and debiting funds from accounts;
- receive statements of cash flows on accounts;
- receive information on exchange rates of the National Bank;
- receive notifications of crediting or debiting funds, etc.

The first bank in Ukraine to offer an Internet banking service was Privat-Bank in 1998 [10]. The number of banks that have Internet banking in Ukraine is insignificant - less than 20 banks. The reason for this situation is the underdeveloped regulatory framework that regulates the work of banks on the Internet.

The most important positive quality of Internet banking is the ability to control your accounts from anywhere in the world. The main condition is to have access to the Internet. The second important quality is speed and convenience. It is possible to save time and money due to the lack of need to visit bank branches, stand in line, etc. The main advantage of the service is the security of operations.

Domestic banks mainly use three types of protection:

- by means of an electronic digital signature (analog of a handwritten signature on paper, which is encrypted with a numerical code and cannot be falsified);

- one-time passwords (they usually require a special generator);
- SMS-confirmations, which are close in principle to the one-time password authentication.

Remote banking is gaining more momentum in its popularity, so it is worth analyzing which of the services are more active in the Internet banking system among all Ukrainian banks (Fig. 1).

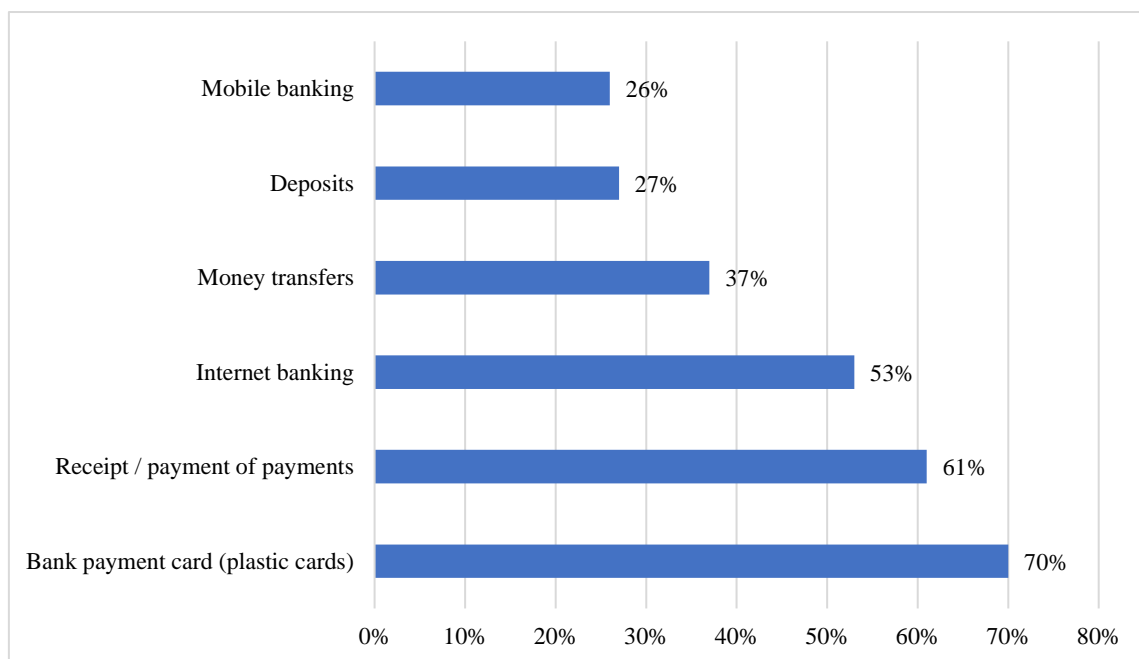


Fig. 1.1. The most used banking services on the Internet

1.2. Advantages and disadvantages of Online banking

The advantages of Internet banking for the bank include [10]:

- minimization of operating costs;
- reduction of investments in the development of the branch network;
- expanding the customer base;
- elimination of geographical and temporal barriers to the provision of services.

The advantages of Internet banking for the bank's clients are due to the following provisions:

- using the Internet, the client gets the opportunity in real time to track the receipt of funds to his accounts and quickly make all necessary payments. This allows him to use

financial resources more efficiently, increases the competitiveness of his business, and as a result - provides additional resources to the bank;

- using Internet service systems, gaining remote access to the account, the bank's client avoids the need to visit the bank's office every day, which is a prerequisite for saving working time;

- new systems due to a more accessible and user-friendly interface allow with minimal effort to prepare payment documents for the bank, avoid possible errors in their preparation, as well as real-time control of the process of passing the document in the bank;

- new systems provide previously unattainable opportunities for mobility and scalability, using which the user will be able to choose the most convenient and efficient procedures for managing their own finances. The system allows you to organize simultaneous work with an unlimited number of jobs in the office, to distribute the powers of employees involved in the preparation of documents, control of financial flows, etc. [7];

- simplicity of the payment scheme.

The disadvantages of Internet banking include:

- the problem of ensuring the security of operations. According to research, despite all security measures, every fifth transaction performed by customers online is still vulnerable to fraud. The technology of phishing is to send text messages as if on behalf of financial institutions with a request to confirm the password or send a PIN code, which is then used for criminal purposes; hackers can intercept keyboard data while typing or redirect users to bogus sites that are very similar to real banking sites; - the cost of the service is minimal, but not always (some banks charge a regular subscription fee);

- some service functions often require good computer knowledge;

- for Internet banking services, there is also such a thing as a transaction day (transactions are still limited in time) [11].

Thus, remote customer service through

Internet banking has both positive aspects (speed and convenience of operations) and negative ones (fraud) (Table 1.1).

Advantages and disadvantages of Internet banking

Advantages	Disadvantages
Convenience	Possible system failures
Control over accounts and payments	Lack of appropriate legal system
Efficiency	Possibility of fraud
Time saving	Lack of Internet
Cheapness	Lack of necessary knowledge

1.3. Typical solutions for deploying Online banking

The democratization of financial services has not only affected consumers, but also opened up a wide range of opportunities for entrepreneurs to launch and support online banking without the involvement of IT resources. Banking software companies have played an important role both in improving existing infrastructure and in almost eliminating barriers to entry in a short time and low development costs. Here are some examples of solutions for deploying online banking:

1) User-friendly Design

One of the most important parts of launching an internet banking program is a simple and convenient design. An application that is difficult to use can be a nuisance for users. User-friendly here means:

Based on navigation templates familiar to users. All functions are available with just a few buttons.

Settings and personalization settings (theme color, personalized avatar, etc.).

In addition, all transactions and actions through your program must be fast and well organized.

2) Taking into account the differences of devices

Different customers use different operating systems, so you need to create a product for Android and iOS to make the banking program optimized for both of these major platforms.

But it's not just the OS that matters. Screen size, phone features (for example, users may have phones that are not optimized for biometric authentication), etc. - all this must be taken into account. Some people may also use an older version of the OS, and some may be constantly updated.

To make sure that the program is optimized for each OS and gadget size, the following is possible:

- Run pre-tests on different devices and simulations. It helps not only optimize the app but also test security and simplicity.
- Analyze app by gathering metrics, running surveys, and getting feedback on user experience [12].

3) Target audience

There is no news that you need to analyze the target audience. You need to understand what services are usually used by potential customers; what they like or dislike about the services they have received before; what they worry about when they use the Internet or make online payments.

But more importantly, at this stage is to obtain factual data and conduct statistical analysis. Only this can help launch a successful product. Here's what you can do:

- You need to create a focus group and a list of questions to answer before setting up your own online bank to make sure everything is right.
- If you are not sure that it is possible to do it yourself, find an agency that conducts research and statistical analysis.
- Build predictive models of possible consumer behavior.
- Use social networks and forums. For example, on Reddit, you can post questions, chat with potential customers, and find out what their struggles are about digital banking.
- Analyzing your target audience helps you find out the important details about their desires and needs that you need to know before setting up a bank.

4) Competition analysis

Target audience analysis also answers the question of "who are the competitors". This is an important detail to know before opening a digital bank. In addition, need:

- Create a list of criteria and a system for evaluating your competitors;
- Examine their strengths and weaknesses;
- Find out what technologies they use and how they sell their products;
- Analyze what their customers think of their services, good or bad;
- Compare your digital banking ideas with competitors' products.
- Analyzing competitors can help you successfully create a valuable digital

banking proposition - a statement of the benefits of why customers should use your services and how you are going to solve their problems and improve their lives.

5) Creating a bank MVP: Definition and Value

MVP is a version of the product that collects enough data to find out how potential customers interact with the product. In essence, this is a business concept focused on:

- Learning how consumers interact with a product without having to fully develop a digital bank;
- Early fixes and improvements with limited money, time and effort;
- Decide if future product has potential (a common practice is to reevaluate goals or abandon the project altogether).

What an MVP is not. This is not a prototype with limited functionality as it won't give enough training data. It is also not a Minimum Marketable Product (MMP) or Minimum Realizable Function (MMF) as they are focused on earnings rather than learning. Also, it would be a mistake to focus on "minimum" other than "viable" when building a bank, as that won't give you enough information to assess whether consumers will use your product.

6) Types of business models

Another thing to figure out before launching a virtual bank is how the product will be structured. Here are the four most prominent types of digital banking business models.

Aggregators — distribution of financial services from an ecosystem of partners. If you decide to build a virtual bank according to this model, it is:

- Reduce the cost of providing services.
- Offer more types of services that one bank cannot do, including non-financial services.

- Will provide its partner banks with advice on making better financial decisions based on data collected from clients.

Open platforms - open banking APIs; a strategy that facilitated the exchange of value, expanded the client and partner base, and provided more opportunities for capital acquisition. If you want to build a bank around this model, keep in mind that there are four main models of banking platforms:

- Ownership: one sponsor and one supplier; APIs are used as an intermediary between developers (gives access to data) and clients (gives access to the final product).

- Licensing: one sponsor and multiple vendors; provides a visible interface for consumers and developers.

- General: many sponsors and many providers; several partners control the development process.

- Joint venture: many sponsors and individual suppliers; a common interface that encourages collaboration between sponsors (for example, fintech companies).

Banking as a Service (BaaS) is a cloud-based model where technology companies can operate like banks after obtaining the appropriate licenses. If you are considering building a bank on the BaaS model, you should know that it has several layers:

- Infrastructure as a Service (IaaS): on-demand financial technology and other services (such as legal or accounting services); it includes hardware and a server for communication.

- Banking as a Platform (BaaP): A fully licensed platform or bank that other businesses use to provide their services.

- Fintech SaaS: on-demand financial services delivered through BaaP; it also allows you to connect services provided by other banks (for example, traditional banking services).

- Human as a Service (HaaS): The behind-the-scenes, top layer representing the services provided by cloud workers.

Traditional universal banking is a model in which traditional banks create a digital banking solution (providing all or certain services). This is usually done to improve

customer service, who prefer to use the Internet or do not have time to be physically present at the bank [13].

1.4. Communication network architecture for Online banking

Building a system network is becoming more widespread and accepted because not only does the business environment build networks, but people build small home or office networks because network devices are low cost.

There are more players in the market that offer network solutions for the banking system:

IBM

BANKING SOLUTION IBM is a modular design philosophy that requires components of the existing architecture for individual building blocks: basic data sets for customers, products and contracts; remote and external business processes, business logic and relevant business rules. With an example of branch system solution (Fig. 1.4.1). It also transfers multichannel mode to additional multichannel [14].

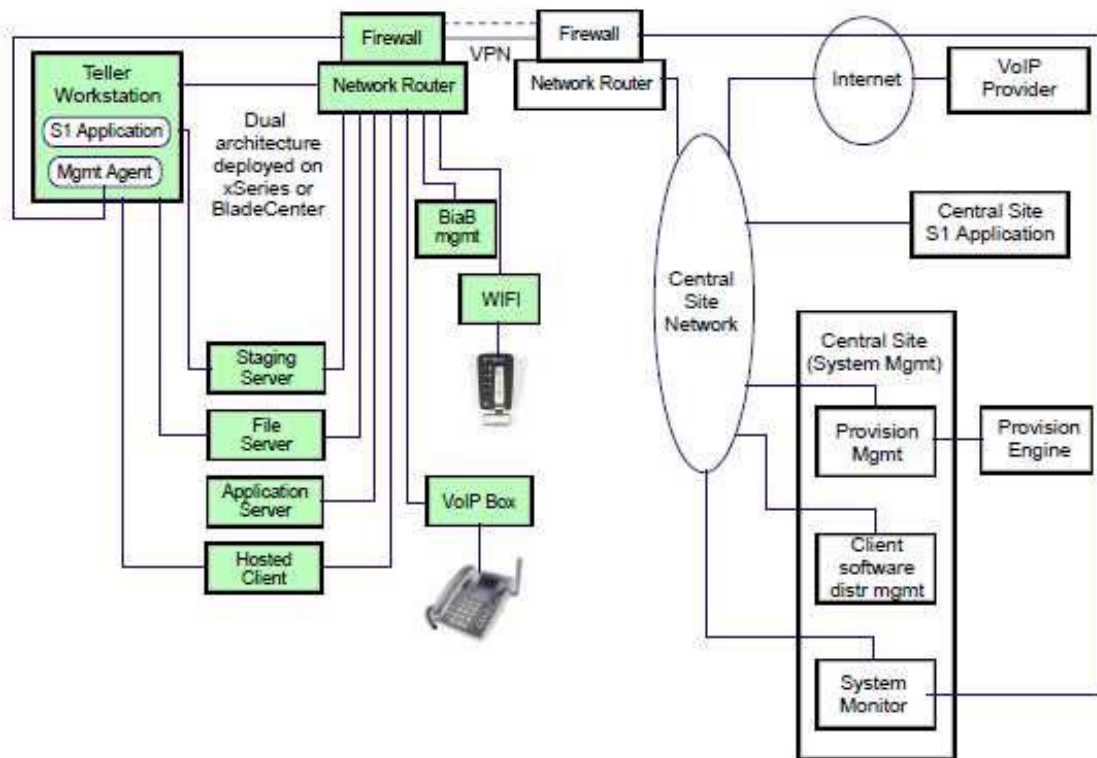


Fig. 1.2. Physical architecture of the solution [14]

Oracle

Infosys Finacle is the cutting-edge advantage of basic banking solutions with SPARC T-Series Servers technology, providing a comprehensive, integrated, yet modular and flexible approach to core banking (Fig. 1.4.2) [15].

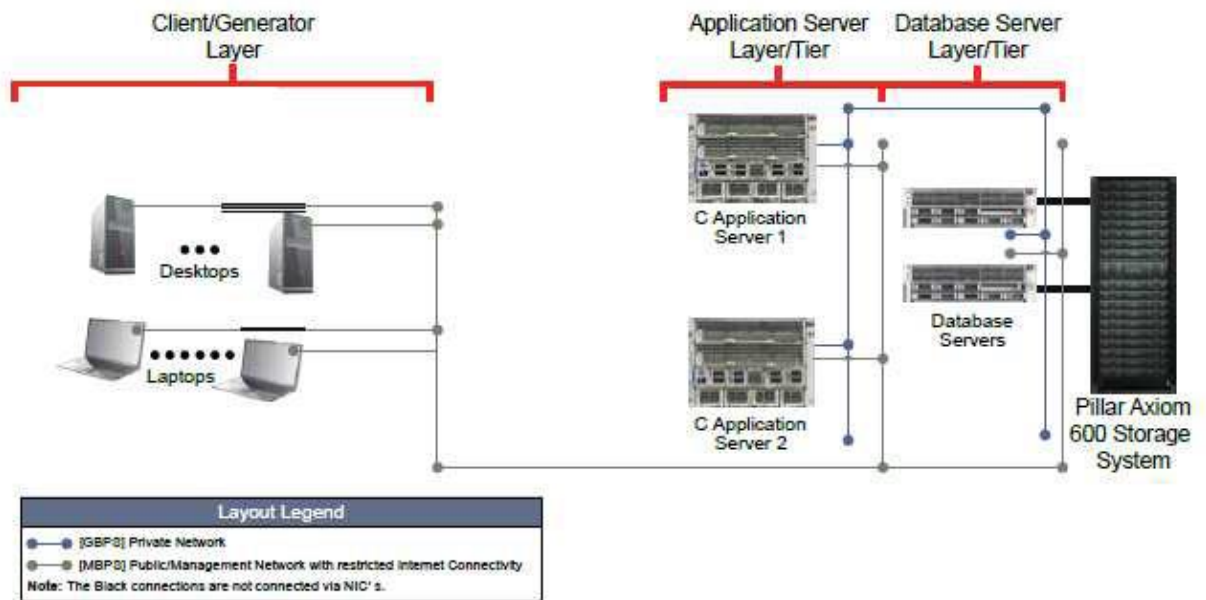


Fig. 1.3. SPARC T4-4 server batch configuration as tested for FINACLE core banking solution [15]

BT

BT MPLS is a multi-protocol label switching network that supports any of the bank's sites, but also allows centralized applications with broadband voice and data convergence to achieve the One Group - One System vision in the case of Danske bank in Ireland (Fig. 1.4.3) [16].

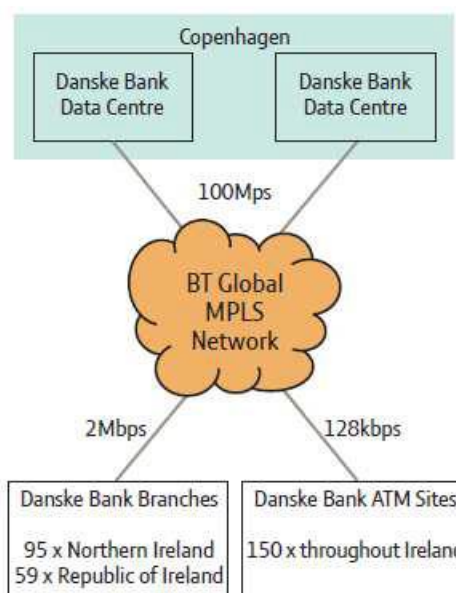


Fig. 1.4. BT`s managed global MPLS network links Danske bank sites [16]

CONCLUSION TO CHAPTER 1

Ukraine is at the stage of formation and development of the information society and digital infrastructure. At the same time, rating indicators show that on the one hand, the country has a positive dynamics of growth in the number of Internet users - potential participants in electronic services, and on the other hand - a significant lag in the state's readiness to provide a full electronic society.

One can firmly predict the further active development of Internet banking in Ukraine. Its future potential is great, as society is increasingly moving to "online life". Experts say that in the near future through the personal account customers will be able to fully obtain loans by providing all necessary information to the bank online, as well as remotely receive official statements of account (meaning official certificates such as visas). Moreover, one can expect that Internet banking will soon become an integral part of all banking institutions, as customers will expect them to do so.

It is worth noting that if this trend continues, then Ukrainian banks will have the opportunity to increase competitiveness in the global services market, and this will have a positive impact on improving the quality and speed of service delivery.

In this case, if each service is the maximum close to customer needs, this will have a positive impact on both the banking system and the economy as a whole.

CHAPTER 2

INFORMATION SECURITY SUBSYSTEM FOR ONLINE BANKING

2.1. Cybersecurity in Online banking

As digitalisation grows, so do the threats to cybersecurity. As the world becomes more digital, it also opens entry points for cybercriminals; therefore, cybersecurity in digital banking is an urgent need.

The main purpose of cybersecurity in digital banking is to protect the client's assets. As people switch to cashless payments, more and more actions or transactions are taking place online. People use their digital money, such as credit and debit cards, for transactions that require protection through cybersecurity.

Cybercrime in digital banking affects not only customers but also banks trying to recover data. Banks may require you to spend a significant amount to recover data or information.

Reliable cybersecurity is a must for banks, as data leaks can make it difficult to trust financial institutions. This can cause serious problems for banks. Cybersecurity in digital banking ensures that your sensitive data is secure, which in the event of disclosure can cause many problems, such as fraud.

Your data can be easily hacked if it is not protected by cybersecurity. This can lead to significant financial losses for the person and mental stress in the event of a cybercrime [17].

Threats for Cybersecurity in Digital Banking

Without reliable cybersecurity measures, sensitive data may be compromised.

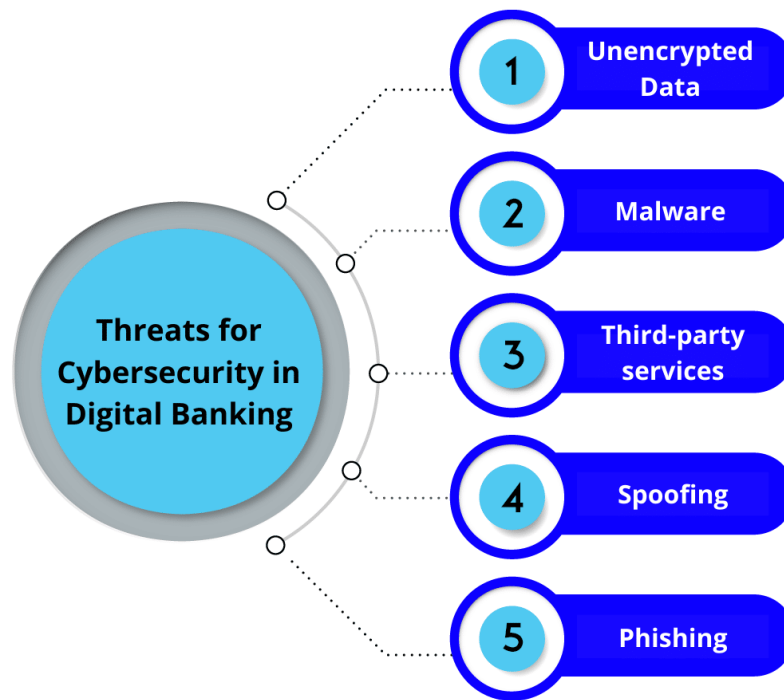


Fig. 2.1 Threats for cybersecurity in digital banking [17]

Unencrypted data

This is one of the common threats faced by banks when data remains unencrypted and hackers or cybercriminals immediately use the data, thus creating serious problems for the financial institution. All data stored on computers in financial institutions or on the Internet must be fully encrypted. This ensures that even if your data is stolen, cybercriminals will not be able to use it.

Malware

End-user devices, such as computers and mobile devices, are mainly used for digital transactions; therefore it must be protected. If it is compromised by malicious software, it can pose a serious risk to the bank's cybersecurity when it connects to your network.

Confidential data passes through this network, and if malicious software is installed on a user's device without any security, it can pose a serious threat to your bank's network.

Third-party services

Many banks and financial institutions use third-party services from other providers to better serve their customers. However, if these providers do not have strict cybersecurity measures, the bank that hired them will suffer greatly.

Spoofting

This is one of the newest forms of cyber threat faced by banks. Cybercriminals will pass the URL of the banking website as a website similar to the original and work in the same way, and when a user enters their login credentials, the login credentials are stolen by these criminals and used later.

This cyber threat reached the next level when these criminals used new methods of forgery. They use a similar URL and target users who visit the correct URL.

Phishing

Phishing is an attempt to obtain confidential information, such as credit card information, etc., for malicious activity disguised as a reliable target in electronic communications. Phishing scams of online banking are constantly evolving. They look real and authentic, but they deceive you when you disclose access information [17].

Challenges relating to Cybersecurity in digital banking

Some of the factors have created a serious challenge to cybersecurity in digital banking. They are mentioned below:

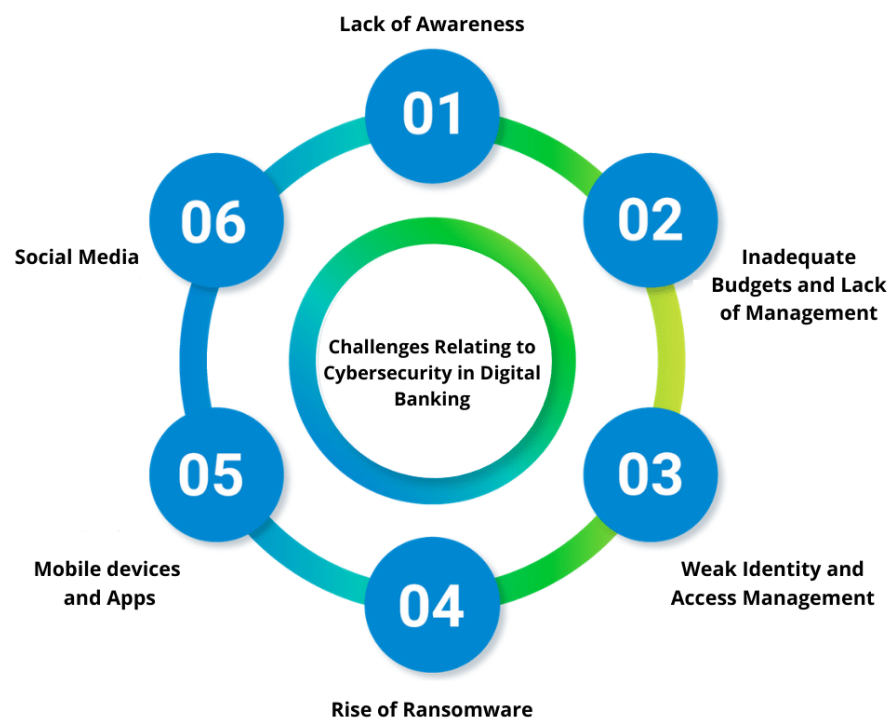


Fig. 2.2 Challenges relating to Cybersecurity in digital banking [17]

Lack of Awareness

People's awareness of cybersecurity has been relatively low, and not many companies are investing in educating and raising people's general awareness of cybersecurity.

Inadequate Budgets and Lack of Management

Cybersecurity is given low priority; therefore, they are in most cases ignored in budgets. Top management also does not focus on cybersecurity, and supporting such projects is a low priority. This may be because they misjudge the impact of these threats.

Weak Identity and Access Management

Identifying and controlling access was a key element of cybersecurity, especially at a time when hackers were gaining ground; You may only need one hacked account to log in to the corporate network. There are few improvements in this regard, but much remains to be done.

Rise of Ransomware

Recent malware developments have drawn attention to the growing threat of ransomware. Cybercriminals are beginning to use methods to avoid detection by using endpoint security code that targets executable files.

Mobile devices and Apps

Most banking institutions use mobile phones as a business. As the base grows every day, it becomes an ideal choice for operators. Mobile phones have become an attractive target for hackers as we see an increase in mobile phone transactions.

Social Media

The introduction of social networks has forced hackers to use them even more. Less knowledgeable customers share their data so everyone can see which attackers are using it [17].

Solution to the threat to the Cybersecurity in digital banking

There are certain approaches that can be used to curb the threat of cybersecurity in digital banking.

Some of the measures are specified below:

Integrated Security

As banking, financial services and insurance are tightly regulated, banks invest time, money and effort in using the best technologies, which are sometimes difficult to manage together. The transition to integrated security, where all components work and interact together, is more cost-effective.

Machine Learning and big data analytics

Analytics is an important element in the use of cyber resilience. A new generation of security analytics has been released that can store and evaluate vast amounts of security data in real time.

Understanding the importance of security

Thinking, when security is seen as a value, must give way to security as a plus. Security risks and their impact need to be analyzed, then only the importance of security can be truly understood.

Investing in the protection of new generation endpoints

Banks and institutions need to invest in technologies that can recognize and eliminate practices and actions used in exploits.

Protect information

Today, data is stored on a variety of devices and in the cloud, so any system that stores sensitive data must be protected.

Consumer Awareness

This is one of the important aspects when the consumer should know that he should not disclose his bank details to anyone. They should notify the cybersecurity department as soon as possible in the event of any suspicious event in their transactions or in their bank account.

Anti-virus and Anti-malware applications

A firewall can increase protection, but it will not stop an attack unless you use updated antivirus and anti-malware programs. Upgrading to the latest program can prevent potentially catastrophic attacks on your system [17].

2.2. Systems and mechanisms for the security of Online banking

The main and most important threat that lurks in any Internet banking user is the risk of fraudulent hacking and unauthorized access to funds in the account. The only significant danger that may lie in wait for users of these systems is the risk of misappropriation of their funds by attackers, using the capabilities of Internet banking systems, however, as well as any other type of remote service systems.

That is why banks are trying to use different systems and mechanisms designed to, if not guarantee, then, as a last resort, increase the security of online banking.

Data encryption

Today, all banks that provide Internet banking services use SSL encryption of data transmitted from the user's computer to the bank's system and back. This security measure eliminates the previously common type of fraud "man in the middle": payment data was intercepted at the stage when they were sent from the client, but not yet reached the bank, the fraudster changed the data and only then sent them to the bank.

To take full advantage of secure data transmission, you should follow basic security measures on the Internet - do not respond to suspicious messages (allegedly received from the bank) and do not go from unknown links.

One-time passwords received at an ATM

With such a security system, in addition to the usual login and password, to log in and confirm transactions, the user must enter a one-time password, a list of which he can get at the ATM of your bank.

From the point of view of security, such a system has an advantage - to carry out card account transactions via Internet banking, a person must at least have the card itself, as well as know the PIN code to get a list of passwords at the ATM.

However, it should be noted a number of shortcomings of this protection system. First, the list of passwords printed as an ATM check will have to be kept to confirm future transactions. This means that if you accidentally lose or drop a check (or just use all the passwords), you will have to go for a new one. Most often, the list of passwords can be

obtained not in every ATM of the bank, and it is likely that you will have to follow him to the other end of town. In addition, the list can be seized by attackers.

If your internet banking system involves the use of a one-time password list, try to follow simple rules. First, don't throw away your password list and try not to lose it if possible. Second, don't save a list of one-time passwords with your login and password. The latter is not recommended to write, it is better to remember.

One-time SMS passwords

This method of user authentication in the Internet banking system is perhaps the most common in the proposals of Ukrainian banks. With this system, every transaction you make with online banking must be confirmed by a one-time password, which you will receive in an SMS message to your mobile phone. In this case, your mobile number must be "linked" to the account number.

This system has a number of advantages. First, it is quite easy to use - you do not need special equipment, and the procedure to confirm the operation takes only a couple of minutes. Second, it protects your account from being used by attackers - even if scammers find out your login and password, they will not be able to access your money, and you will learn about an attempt to make an unauthorized SMS transaction.

This is the end of the system's benefits. Indeed, it is difficult for attackers to acquire a one-time password valid for a short time. Unless they have taken possession of your mobile phone. And the system will be completely useless if you use Internet banking from a mobile phone and save passwords in the browser. Then, stealing your phone, the scammer will receive your account in full.

If your bank uses SMS user authentication, try the following rules:

- do not use Internet banking from a mobile phone;
- never save passwords in your browser.
- in case of loss or theft of a mobile phone - immediately ask the bank to block your Internet banking account.

Electronic digital signature (EDS)

This mechanism is more often used when servicing companies, but sometimes it is offered to the public. The advantage of EDS is that it allows you to uniquely identify the

user. The disadvantage is that EDS can also be vulnerable to fraud. Intruders can gain access to the key to your digital signature by infecting your computer with malware. There are "Trojans" that can find and steal on the infected computer authentication data (identifiers, passwords and even EDS keys) of users to access various services, including remote service servers for bank customers.

External electronic devices

Some banks offer online banking users to buy (or rent) a special device - a one-time password generator. The generator connects to a computer via a USB port and does not require special software.

Other institutions offer to use a foreign electronic key, which is generated when first connected to the Internet banking system, recorded on external media and then used for transactions in the system.

Such systems are, in fact, a simplified version of the EDS. Among the disadvantages are that you will not be able to access your account without having a "key" at hand, and always carry it with you may not be very convenient and safe.

In addition to the above, banks often take additional measures to ensure the safe use of Internet banking:

1) Restriction of the use of personal certificate - the system of some banks allows you to use the electronic key (electronic certificate) only on the computer on which it was generated. Thus, you can make payments via Internet banking only from your personal computer (although view account statements are also possible on other devices);

2) Virtual keyboard - designed to prevent fraudsters from "reading" your credentials when entering them from a regular keyboard using computer viruses ("Trojans");

3) Session duration limit - in case of user inactivity, the session in the Internet banking system will be closed after a certain time (usually 10-15 minutes). After that, you need to re-authenticate to resume work;

4) Connection history - with this function the Internet banking user will find out if someone other than him has connected to the system, and will be able to track all unauthorized transactions, if they were made [18].

2.3 Security software for Online banking

The bank that provides e-banking services must ensure the security of the software used by it. Security software for online banking should minimize the success rate of the above types of attacks.

For online banking, user authentication is considered key. The security of online banking largely depends on whether it is reliable, which will make the user's account inaccessible to cybercriminals. Tokens are the most common software for protecting online banking.

After entering the login and password, the user must also provide additional code generated by the token, ie a one-time password generator. Tokens come in two versions, ie hardware tokens and mobile solutions. Some of the most popular tokens:

- tPro ECC is a hardware token that uses elliptic curve cryptography. The advantage of this solution is also the mechanism of HPD (Human Presence Detection). The user authorizes each transaction by pressing a button on the body of the device. This token is not protected from remote attacks;
- tPro Mobile is an advanced mobile tool. This solution complies with the recommendations of the above-mentioned PSD2 directive and due to its structure and design it can be integrated with the operating system and used as an additional authentication factor.

In addition, banks use PUSH messages and biometric data. In the latter case, the most popular solutions are FaceID and biometric fingerprint data [19].

2.4 Information security of Online banking

Using the Online banking system becomes safer. Information security is being improved taking into account the constantly changing infrastructure, as well as in connection with the development of information technology.

Safe use of Online banking is based on modern and reliable technologies presented below.

Internet Banking Server Authentication

To protect against attacks aimed at replacing the banking Web server and modifying its content during transmission, the SSL (Secure Sockets Layer) protocol and a public key certificate issued by one of the authoritative Internet certificate authorities (Certificate Authority) - VeriSign are used.

Internet Banking User Authentication

For secure access to the system, two-factor user authentication technology is used. This technology is based on two factors: the user has a valid private (secret) cryptographic key, which is stored in a file container or on a token, and knowledge of the password (PIN code) to access this key.

Confidentiality of transmitted data

To ensure the confidentiality of data exchanged between users and the bank through Online Banking channels, this data is encrypted. Thus, the possibility of interception and unauthorized reading of payment and other information is excluded.

Authorization of payment documents

To ensure authenticity (authorship confirmation), non-repudiation of authorship and integrity of electronic payment documents that are generated by customers and transferred to the bank, an electronic digital signature mechanism is used. The validity of the electronic digital signature is checked before any operation on document processing. Cryptographic protection tools integrated into the Online Banking system for the operations of generating and verifying an electronic digital signature, certified in accordance with the requirements of Ukrainian legislation.

Using a USB-token (eToken) as a carrier of an electronic key

To ensure reliable storage and use of private keys, it is recommended to use hardware devices for generating signatures (tokens) provided by the bank. A hardware device for generating a signature (token) is a means of cryptographic information protection, the technical implementation of which ensures the storage of a private key in a secure memory and the performance of cryptographic operations in such a way that it makes it impossible to copy the private key or its location outside the protected memory of the device.

Restrictions on the list of IP addresses and IP subnets when accessing Internet banking

If Online Banking is accessed from a static IP address or a range of addresses, we recommend that you contact the bank to set a limit on the list of IP addresses and/or IP subnets from which the Online Banking system can be accessed. In this case, all attempts to connect to the Online Banking system from IP addresses and/or IP subnets other than those specified will be blocked.

Using a group of two or more signatures to generate an electronic settlement document

To minimize the risk of fraudulent actions with the client's accounts by third parties in case of loss or compromise of one of the EDS keys, it is recommended to use the group signature mechanism. In this case, only those payment documents that contain a complete group of signatures and match the specified signatures in the signature sample card will be processed [20].

CONCLUSION TO CHAPTER 2

The methods used by cybercriminals are constantly evolving. It also means that security software for online banking must consider increasingly effective means of protection so that money and customer data are secure and inaccessible to hackers.

Online banking security software can also use artificial intelligence to prevent fraud. During its development, AI technology will control the behavior of customers in terms of their location, devices and authentication methods. Based on the observed behavior, the software will provide analysts with recommendations and reliable risk assessment.

Although the security of online banking is constantly improving, keep in mind that the user remains the weakest link in the system. By implementing cutting-edge solutions, banks must also promote customer education. Only then will the fight against cybercrime make sense.

Cybersecurity in Online banking is something that cannot be compromised. With the growing digitalization of the banking industry, it has become more prone to attacks by

cybercriminals. Therefore, there must be reliable cybersecurity that does not jeopardize the security of data and money of customers and financial institutions.

CHAPTER 3

PROTECTION OF INFORMATION FOR ELECTRONIC DOCUMENT SYSTEM

3.1 Characteristics of threats

According to the Law of Ukraine "On Information Protection in Information and Telecommunication Systems", the basic terminology of information protection systems uses the following concepts:

- blocking information in the system - actions that exclude access to information in the system;
- leakage of information - the result of actions as a result of which information in the system becomes known or available to individuals and / or legal entities that do not have the right to access it;
- access to information in the system - the user gets the opportunity to process information in the system;
- protection of information in the system - activities aimed at preventing unauthorized actions on information in the system;
- destruction of information in the system - actions as a result of which information in the system disappears;
- information (automated) system - organizational and technical system, which implements the technology of information processing using hardware and software;
- information and telecommunication system - a set of information and telecommunication systems, in the process of information processing act as a whole;
- complex information protection system - an interconnected set of organizational and engineering measures, means and methods of information protection;
- user of information in the system (hereinafter - the user) - a natural or legal person, in the manner prescribed by law received the right to access information in the system;

- cryptographic protection of information - a type of information protection, implemented by transforming information using special (key) data in order to hide / restore the content of information, confirm its authenticity, integrity, authorship, etc.;
- unauthorized actions with information in the system - actions carried out in violation of the procedure for access to this information, established in accordance with the law;
- information processing in the system - the implementation of one or more operations, including: collection, input, recording, conversion, reading, storage, destruction, registration, reception, receipt, transmission, which are carried out in the system using hardware and software;
- violation of the integrity of information in the system - unauthorized actions with information in the system, which changes its content;
- the procedure for access to information in the system - the conditions for the user to process information in the system and the rules of processing this information;
- telecommunication system - a set of hardware and software designed to exchange information by transmission,
- radiation or reception in the form of signals, signs, sounds, moving or still images or otherwise;
- technical protection of information - a type of information protection aimed at providing with the help of engineering measures and / or software and hardware means to prevent leakage, destruction and blocking of information, violation of the integrity and mode of access to information.

The objects of protection in the system are the information processed in it and the software and hardware designed to process this information.

The subjects of relations related to the protection of information in the information systems of the authorities are:

- information owners;
- system owners;
- users;

- specially authorized central executive body for special communication and information protection and subordinate regional bodies.

To ensure the protection of information with limited access, the protection of which is required by law, in information, telecommunications and information and telecommunications systems (hereinafter - the system) must follow the following procedures:

- Authentication - the procedure for establishing ownership of information in the system (hereinafter - the user) to the user of the identifier provided to him;
- Identification - the procedure of recognizing the user in the system, usually using a predetermined name (identifier) or other a priori information about him, which is perceived by the system.

During the processing of confidential and secret information, its protection from unauthorized and uncontrolled access, modification, destruction, copying, distribution must be ensured.

Access to confidential information is provided only to identified and verified. Attempts to access such information by unidentified persons or users with a matching ID not verified during authentication should be blocked.

The transfer of confidential and confidential information from one system to another is carried out in encrypted form or through secure communication channels in accordance with the requirements of the legislation on technical and cryptographic protection of information.

CISS includes measures and tools that implement methods, techniques, mechanisms to protect information from:

- sources of technical channels, which include channels of lateral electromagnetic radiation, acoustoelectric and other channels;
- Unauthorized actions and unauthorized access to information that can be carried out by connecting to equipment and communication lines, issuing to a registered user, overcoming security measures to use information or imposing false information, using embedded devices or programs, using computers third-party viruses, etc.

- special influence on the information which can be carried out by formation of fields and signals for the purpose of violation of integrity of the information or destruction of protection system.

For each specific information system, the composition, structure and requirements for CISS are determined by the properties of the processed information, the class of the automated system (AS) and the conditions of its operation.

One of the requirements for ensuring the protection of information in the AS is that the processing of confidential information should be carried out using secure technologies, includes software and hardware protection and organizational measures to ensure compliance with general requirements for information protection. General requirements include:

- availability of a list of confidential information subject to automated processing; if necessary, it can be classified within the category by purpose, the degree of restriction of access to a certain category of users and other features of classification;
- the presence of a responsible unit, which is authorized to organize and implement information security technologies, monitor the state of information security (security service in the AS, information security system)

Creation of CISS, which is a set of organizational and engineering measures, software and hardware aimed at ensuring the protection of information during the operation of AES;

- development of an information protection plan at the AES;
- availability of the certificate of conformity of CISS in the automated system to normative documents on information protection;
- the ability to determine with the help of CISS several hierarchical levels of authority of the user and several levels of classification of information;
- mandatory registration in the AS of all users and their actions regarding confidential information;
- the ability to provide users only with permitted and controlled access to confidential information processed in the AS;

- Prohibition of unauthorized and uncontrolled changes to confidential information at AES;
 - accounting for the initial data obtained during the solution of the functional task, in the form of printed documents containing confidential information, in accordance with the governing documents;
 - prohibition of unauthorized copying, reproduction, dissemination of confidential information in electronic form;
 - providing with the help of information protection systems control over the permitted copying, reproduction, dissemination of confidential information in electronic form;
 - possibility of unambiguous identification and authentication of each registered user;
- Providing CISS with the possibility of timely access of registered users of the AU to confidential information.

These requirements are basic and are used to protect information from unauthorized access in all types of AS.

Thus, taking into account the above, access to information in the subjective sense is a state-guaranteed opportunity for individuals, legal entities and government agencies to freely obtain the information they need to exercise their rights, freedoms and legitimate interests, to perform tasks and functions. violates the rights, freedoms and legitimate interests of other citizens, the rights and interests of legal entities [21].

3.2 Comprehensive information protection in the EDMS

A systematic approach to the protection of computer systems requires the consideration of all interrelated, interacting and time-varying elements, conditions and factors that are important for understanding and solving the problem of security. When creating a security system, you must take into account all the weaknesses, vulnerabilities of the information processing system, as well as the nature, possible objects and directions of attacks on the system of attackers, ways to penetrate distributed systems and unauthorized access to information. The protection system must be built not only on the basis of all known

channels of intrusion and unauthorized access to information, but also taking into account the possibility of the emergence of fundamentally new ways to implement security threats.

Any information, regardless of whether it is the property of the state, of society as a whole or of individual organizations or individuals, is of some value. Therefore, information resources need to be protected from various influences that can lead to a decrease in their integrity and value at the level of securities representation.

Late classifications of threats are used to identify and analyze possible threats to the security of information, as well as to develop means of counteraction. The classifications used during the creation of theoretical models and the analysis of hazards are based on numerous features of hazards. Some classifications involve a relatively small number of threat signs, and they use software companies. For example, these include the STRIDE methodology, which has been developed, substantiated, and actively promoted by Microsoft specialists.

In modern information and communication systems, various means and measures of protection are used. Protection measures include, first of all, the development of information security policy in the system and the design of ICS taking into account the requirements of this policy. It is also necessary to designate persons who could be responsible for the protection of information in a particular system, which would define their responsibilities and powers, or create a special structural unit - the information protection service. There are basic measures that can protect the corporate network from attacks: firewalling and detection of vulnerabilities and attacks. Each means of protection is aimed at preventing a specific security threat in the system or a certain set of such threats and has its advantages and disadvantages. Only a combination of means of protection makes it possible to defend against a wide range of attacks.

In order to build protected ICS, the network architect must meet certain requirements. The main requirement is the refusal to use such physical and logical topologies of networks, in which direct listening to the traffic of the whole segment of the network from any network is possible. Typical examples are the Ethernet networks 10BASE-2 and 10BASE-5 ("thin" and "thick" Ethernet), which use a physical topology common bus connection - all stations

in the segment are connected to a data connection. These technologies are already obsolete, and they are almost never used in modern ICS.

In order to restrict access to certain resources in the network, they use its segmentation, which, moreover, allows to significantly increase the scalability of the network. For the segmentation of the network at the channel level, a very powerful tool is used - virtual local area networks, VLAN (Virtual Local Area Network). A virtual local area network is a subset of network nodes, the traffic between which is completely isolated from other nodes at the channel level. That is, the frame from the VLAN (in particular, broadband) the switch does not transmit outside it. Virtual local networks are created by configuring the switches accordingly [22].

An important component of security of information in the network is to ensure the availability of nodes. Usually, this task is not seen in the context of information security, but in the context of improving the reliability and productivity of computer networks.

As any equipment cannot be 100% reliable, during the creation of sensitive to the availability of certain ICS resources, the provision of network equipment and communication channels is envisaged. In this case, it is desirable to provide the possibility of automatic reconfiguration of the network from the main channels and switching nodes on the stage.

In such circumstances, there may be some problems at the channel level. If you look at the topology of a network that has backup switching nodes and communication channels, rings will inevitably appear in such a network. But the presence of rings is incompatible with the algorithm of the bridge on which the switches operate. If there are rings in the network, broadband packets will start to multiply quickly, and in a very short time (a few seconds) the network will be overloaded.

Network displays (ND) or firewalls are designed to protect internal resources between them by limiting the ability to exchange between them. A computer running interscreen software, or a specialized software and hardware device that implements ND functions, acts as a gateway between two interfaces.

A screen-like device is sometimes used to protect a specific computer. In this case, a screen is installed on the computer to be protected in the form of specialized software to control all incoming and outgoing traffic. Such a firewall is often called a personal firewall.

There are three levels of ND functionality.

1. Packet filters, or control routers - operate mainly at the third (network) level of the model of interaction of open systems (OSI); As a rule, the information from the titles of the protocols of the fourth (transport) level is also analyzed.

2. Session-level gateways, also called operational transport, mostly operate at the fifth (session) level of the OSI model.

3. Application or external gateways - work at the application level of the OSI model.

Firewalls that implement the functionality of any of the levels usually implement the functionality of the lower levels.

Packet filters analyze packet headers for TCP, UDP, and IP. According to the set of rules set by the security administrator, decide to act with the package. Each package is analyzed separately from the others, taking the following parameters:

- packet fragmentation program;
- TCP (UDP) port numbers of the sender and recipient;
- SYN message (indication of the first packet when establishing a connection);

The protection of the bank's system should start with anti-virus programs, protection at the level of the operating system, at the level of the network, as well as providing access. It is distributed depending on the level of availability, position of the person who will send the request to the system or program.

Windows has a well-defined set of security features. The following are the components and databases that make up Windows.

A security monitor is a component of the system that runs in kernel mode and provides access to objects, privilege operations (user rights), and the creation of security audit messages.

The local authentication subsystem is a copier mode process that depends on the security policy of the local system (determines the range of copiers to be logged. The main

functionality is implemented by the local authentication service - DLL, which is loaded by the Lsass user.

The Lsass policy database is a database of local system security policy settings located in the registry section. It contains information about which domains have been authenticated to log in, who has access to the system and how and to whom certain privileges are granted, as well as what types of checks. The Lsass policy database stores "secrets": login data used to log in to the domain and when calling services.

Active Directory is a directory service that stores a database of objects in a domain. A domain is a set of computers and related security groups that are managed as a whole. Active Directory stores information about the domain object, users, groups, and computers. Information about the passwords and privileges of domain users and their groups is stored in Active Directory and copied to computers running the domain management field [23].

Authentication packages are DLLs that run in the context of the Lsass process and implement the authentication policy. They transmit the password and username and provide updates for the Lsass process (if successful) with details of user rights.

The login process is a customizable mode that is responsible for supporting SAS and managing interactive login sessions. During the user registration process, Winlogon creates a shell - a user interface.

3.3 Ways to solve the problems of electronic document management

In the general set of measures to ensure the national security of the state, an important place is occupied by measures related to the direct protection of information from threats, the implementation of which may cause political, economic, financial and other damage to individuals, society and the state. Among the threats to information, in terms of their dangerous consequences, a special place is occupied by:

1. Obtaining information on technical research in the field of defense, economics, science and technology, external relations, state security and law enforcement

Despite the positive changes in the international situation around Ukraine, the activities of technical intelligence services of foreign countries continue with the receipt of

information. Intelligence is continuously conducted against Ukraine with the help of multifunctional space, air, ground, sea systems and technical intelligence complexes. The world's leading countries continue to modernize their intelligence services, improve technical intelligence and increase their capabilities.

The existing capabilities of technical research allow to ensure continuous monitoring of the entire territory of Ukraine, and in the future technical intelligence, including the space component, will have exceptionally high characteristics, which will ensure continuous monitoring throughout the country in real time.

2. Unauthorized access to information processed and circulating in information and telecommunications systems, as well as special influence on information in order to distort, destroy, destroy, disrupt the proper functioning of information processing systems.

In case of insufficient nomenclature of information processing means and software of domestic development in information telecommunication systems foreign products are widely used, which generally do not have objective assessments of protection mechanisms, and also creates preconditions for introduction of information technologies in all spheres of life, society and state.

At the same time, in the absence of competitive domestic models, preference is given to information technologies and technical means of information processing of foreign origin, which generally do not protect information, and create conditions for uncontrolled use of special software and hardware ("embedded devices").

There is a tendency in the world to spread computer crimes, the spread of computer viruses, primarily due to the use of the Internet, the danger of illegal actions, technical and technological errors and failures in the use of information and telecommunications systems, especially relevant in the context of widespread domestic information and telecommunication systems to global.

Some states are implementing the "concept of information confrontation", which is to implement measures to have a special impact on the information infrastructure in order to destroy information resources and destroy the management system in the fields of defense, economy, security, finance and more.

3. Leakage of information with limited access to technical channels due to the occurrence of falsified electromagnetic radiation and interference, conducting acoustic and optoelectronic reconnaissance in the immediate vicinity of the object of information activities.

In the process of information activities for storage, processing and transmission of information, including information with limited access, widely used technical means for various purposes (computers, office equipment, communications, automated systems, etc.). At the facilities of information activities, official issues are discussed in various areas of the institution, during which information with limited access can be voiced.

However, certain physical processes that occur in technical means and when discussing information and other factors create objective preconditions for the emergence of technical channels of information leakage, which necessitates measures to create complexes (systems) for technical protection of information aimed at preventing leakage. information through these channels.

Active development of international cooperation with foreign countries in political, military, economic and other spheres leads to the wide opening of foreign diplomatic missions and missions, foreign commercial institutions, the location of which in close proximity to government agencies and institutions creates the conditions for obtaining information through technical means of intelligence. with limited access circulating in the objects of information activities, which is especially important due to the widespread use of unprotected imported technical means of information processing.

All these factors significantly increase the vulnerability of information and, as a result, determine the need for appropriate measures by the state. At the same time, the importance of the negative consequences of information threats, especially those with limited access, for national security determines the national importance of measures to prevent such threats, and requires the transition from a fragmented departmental approach to the formation and implementation of technical protection measures. systematic and comprehensive approach, attracting the necessary human resources, accumulation of necessary resources to solve the problem of information security.

To counter these threats, the state has created, operates and develops a system of technical information protection, which is a set of organizational structures united by the goals and objectives of information protection, regulatory and logistical base.

3.4 Creating users in the system and grouping

During the thesis, the Alfresco system was considered - a powerful electronic document management system that combines the functionality of a content management platform and a shared work environment. Alfresco allows you to systematize the process of electronic document management, significantly speed up and simplify the creation, editing and design of any document.

The Alfresco system is built on open source, it is reliable, fast, easily scalable and customizable for individual business needs. Alfresco is used by Cisco, NASA, FOX, Scania and other leading companies around the world.

To use the electronic document management system, you must have an account in the operating system. Authorization for the administrator and other users is performed using this account. In the electronic document management system itself, a user who has certain rights to do so, ie who can add users to this system by filling in his data, indicating the last name, first name, patronymic, Identificational tax number, indicates the type of contractor and his place of residence.

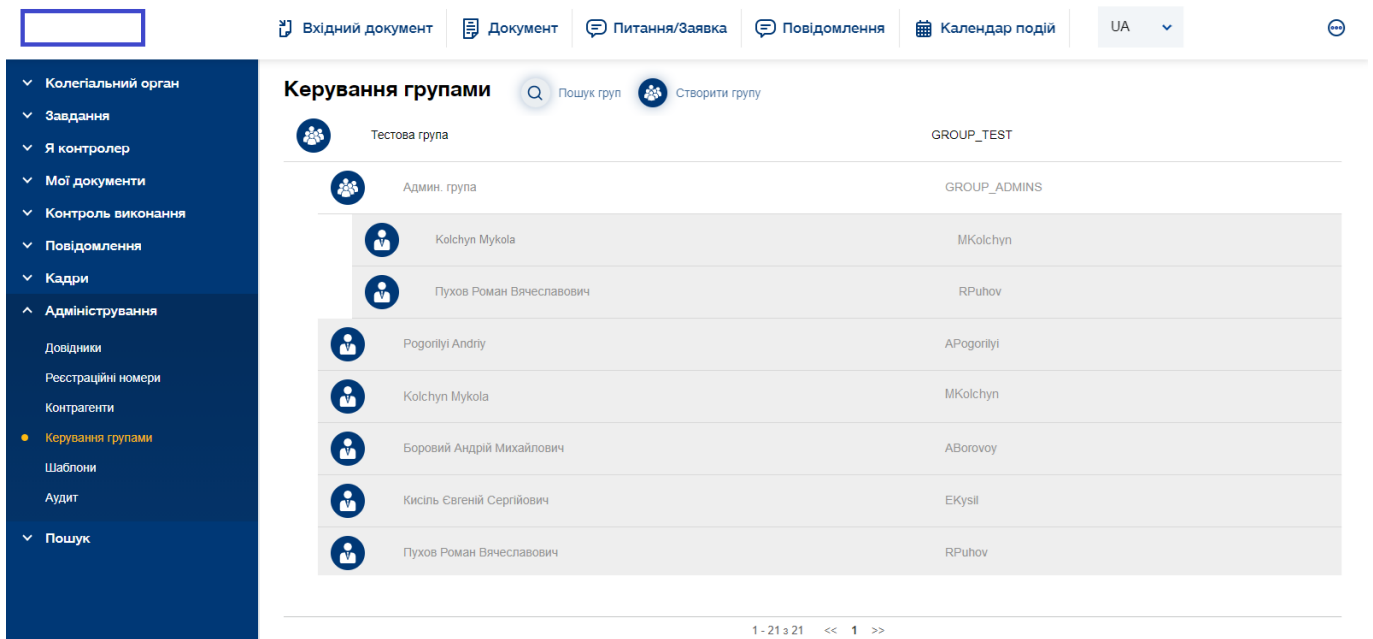


Fig. 3.1. General view of the electronic document management system

The creation of a new user in the system as indicated above is carried out by the administrator (the user who has the rights to perform this operation).

The form is titled 'Тип заявника-контрагента: *'. A dropdown menu is open, showing the following options:

- Інші
- Фізична особа
- Фізична особа - підприємець
- Юридична особа

Below the dropdown, there are several input fields:

- Прізвище: [input field]
- Ім'я: [input field]
- По батькові: [input field]
- Назва контрагента: [input field]
- ІПН/ЄДРПОУ: * [input field]
- Країна: [input field with 'Україна' selected]
- Місто: [input field]
- Область: [input field with dropdown arrow]
- Район: [input field]
- Вулиця: [input field with 'вул.' selected]
- Будинок: [input field]
- Квартира: [input field]
- Індекс: [input field]

At the bottom, there is a blue button labeled 'Заповнити фактичну адресу з юридичної'.

Fig. 3.2. Creating a counterparty



Тип заявника-контрагента: *

Фізична особа

Пошук Очистити

Уповноважена особа:

Прізвище: Щукін Ім'я: Олександр По батькові: Валерійович

Назва контрагента: ShOleksandr

ІПН/ЄДРПОУ: * 54545235

Країна: Україна Місто: Київ Область: Київська область Район: Солом'янський

Вулиця: вул. Освіти Будинок: 7 Квартира: Індекс:

Заповнити фактичну адресу з юридичної

Fig. 3.3. Creating a counterparty

According to this scheme, a user is created for example.

ShOleksandr	Фізична особа	+38
-------------	---------------	-----

Fig. 3.4. Created counterparties

To create a group you need to go to the menu - Administration and select the group management item, then on the page that opens select the item - create a group. Groups are created to restrict users' access to information about which groups it is hosted and distributed among group users.

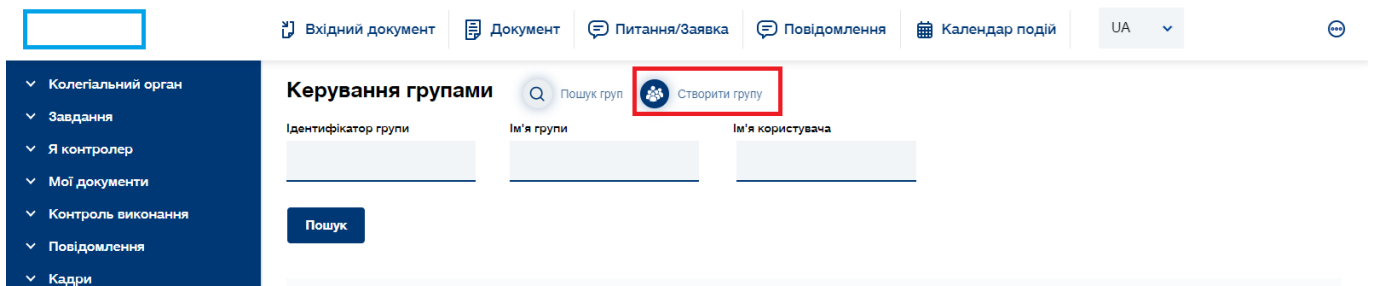


Fig. 3.5. Create a group

When creating a group, you must specify its group ID and group name, and you can later search for these criteria.

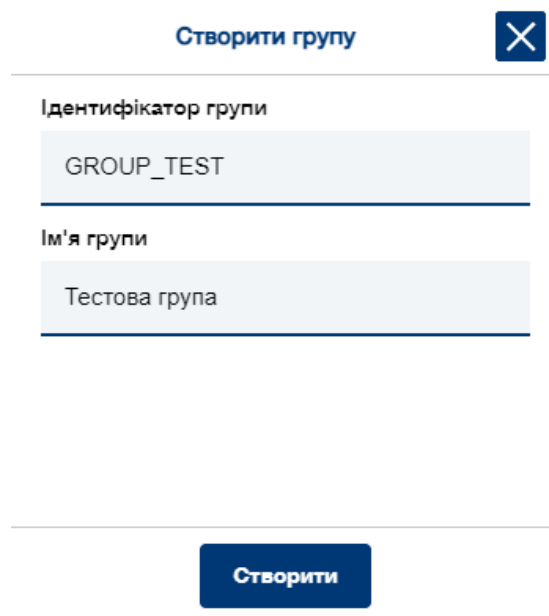


Fig. 3.6. Creating a group

Each group has the ability to create a nested group, or add an existing nested group, add a user to the group or edit group users, and edit or delete a group.

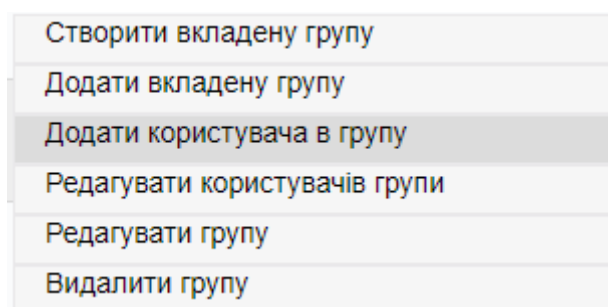
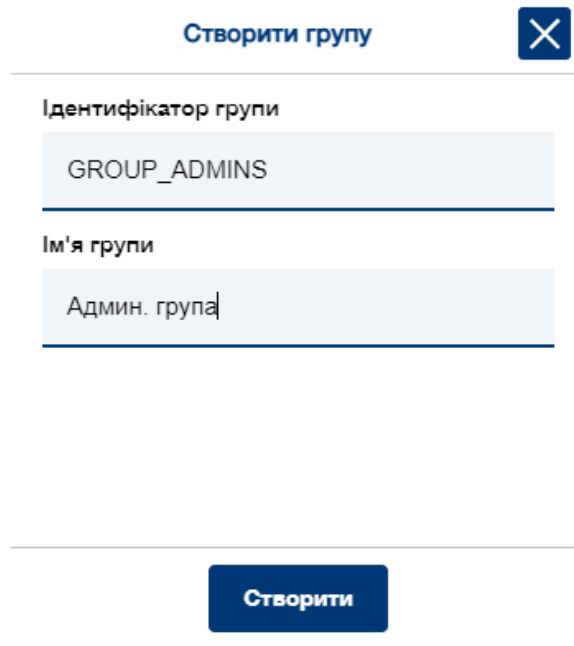


Fig. 3.7. Possible functions in the group

After clicking on the function that adds a user to the group, a window will open with a list of all users who have access to the electronic document management system and have an account in the operating system. If necessary, you can search for users.

Then a group was created, which includes users who will be able to access information and folders.



Створити групу

Ідентифікатор групи

GROUP_ADMINS

Ім'я групи

Админ. група

Створити

Fig. 3.8. Creating a group of administrators

The information that will be sent to both the admin group and the test group will be available to users who have been added to the admin group. Test group users are not allowed to view and use files and information sent and processed in the admin group.

To create a document, click on the tab - Document and select the internal document. A page will open with the data you need to fill in, as well as marked fields for mandatory filling.

Створення документа

Загальна інформація Узгодження Виконання Зв'язки Архівування

Тип документа: Стан: Автор:

Внутрішній документ Підготовка Kolchyn Mykola

Назва: *

Budget

Тип інформації: Бізнес-процес: *

Публічна інформація ІТ підтримка інформаційних систем




Вид документа: * Підгрупа/Підвид: *

Навчальні матеріали Презентація Power Point

Fig. 3.9. Creating a document


The following is the recipient (author of the document) and signatories, you can select multiple signatories from different groups and select the type of file to attach and download this file. At the bottom of the page, select the functions you want to perform when executing the file.

Адресат: *

  Kolchyn Mykola 

Підписанти: *

Підписант

Пухов Роман Вячеславович Аналітик операційного та прикладного програмного забезпечення 

Тип прикріплюваного файла: Документ:

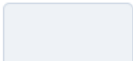
Документ з файлової системи 

Fig. 3.10. Addressee and signatory

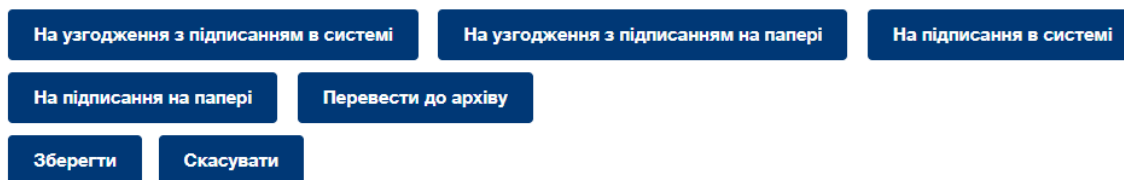


Fig. 3.11. Functions

After selecting the required function, the user who was specified as a signatory will receive a message in the section - Tasks, item - To the signature, to which you can see the sent document.

На підпис Пошук у розділі Зберегти у CSV Налаштування колонок Увага: зміни

Назва завдання	Тип документа	Вид документа	Назва документа	Отримано
Завдання на підписання	Внутрішній документ	Реєстраційні документи	Budget adjustment Approval (between Dpt) test	22.05.2022

Fig. 3.12. Document for signature

Next, you need to click on the selected document - Task to sign and take it to work, the document the signatory can view all the information who is the author, file type, type of information contained in the file, the state in which it is at the time of signing.

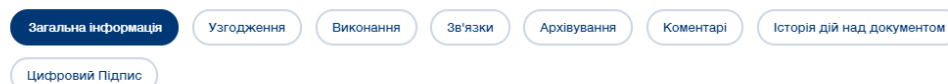
Завдання на підписання

Візьміть завдання в роботу. Ознайомтеся з документом та прийміть рішення щодо підписання:

- У разі підписання документа з ЕЦП, на вкладці Цифровий Підпис накладіть цифровий підпис на документ та завершіть обробку завдання, натиснувши «Підтвердити»;
- У разі підписання документа без ЕЦП, завершіть обробку завдання, натиснувши «Підтвердити»;
- У разі відмови від підписання, додайте своє зауваження та завершіть обробку завдання, натиснувши «Відхилити».



Перегляд



Тип документа:	Автор:	Стан:
Внутрішній документ	Пухов Роман Вячеславович	На підписанні

Назва: Budget adjustment Approval (between Dpt) test

Fig. 3.13. Take a document to work

The file must be signed to continue working with it. To do this, go to the tab - Digital Signature and select Sign Document. In the open window, fill in the required information, such as: choose an accredited key certification authority, private key, and password to decrypt and sign the document. Failure to decrypt will result in an error.

Підписання

АЦСК: КНЕДП/АЦСК ТОВ "Центр сертифікації ключів "Україна" ▾

Особистий ключ: 99000430_3214565457_DU200225120831.Z

Пароль: ...

Fig. 3.14. Signature

Error that occurs when signing the document incorrectly.

Помилка

Для виконання завдання необхідне накладня КЕП / Please sign doc by qualified electronic signature for complete this task.

Fig. 3.15. Error

To verify the authenticity of the signed document, you can do the following: find the document by name or if it was sent to the recipient, find the document can only be a user in the group to which it was sent or a user with less limited rights.

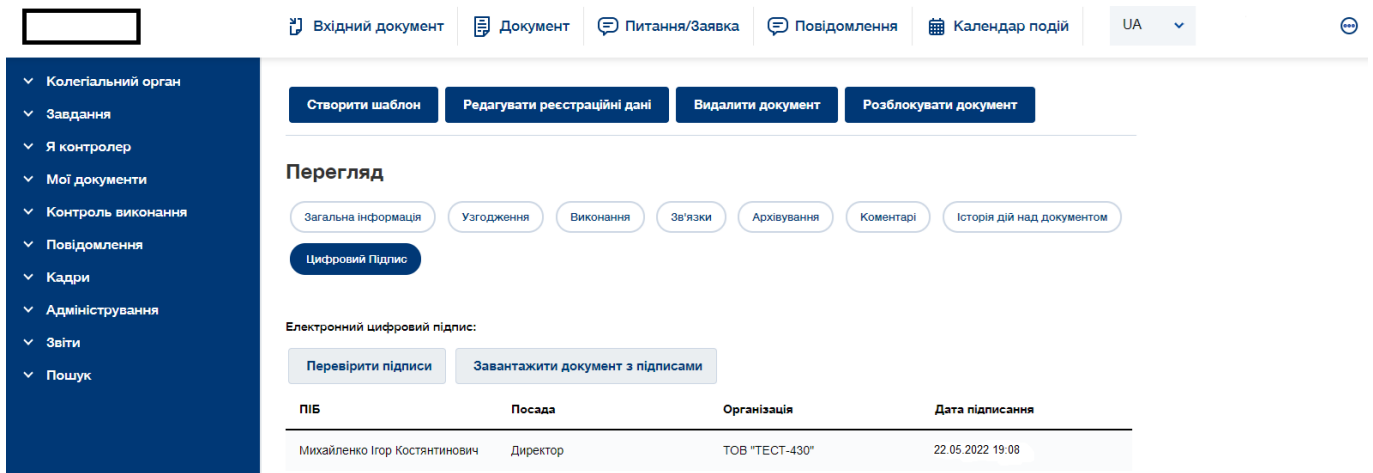


Fig. 3.16. Digital signature tab

After going to the tab, you need to click on - Check signatures, the system will create a request to the ACSC (accredited key certification authority) which, in response, will highlight green information about the signature, otherwise - red, which means that the signature is not valid and not passed the inspection in the ACSC.

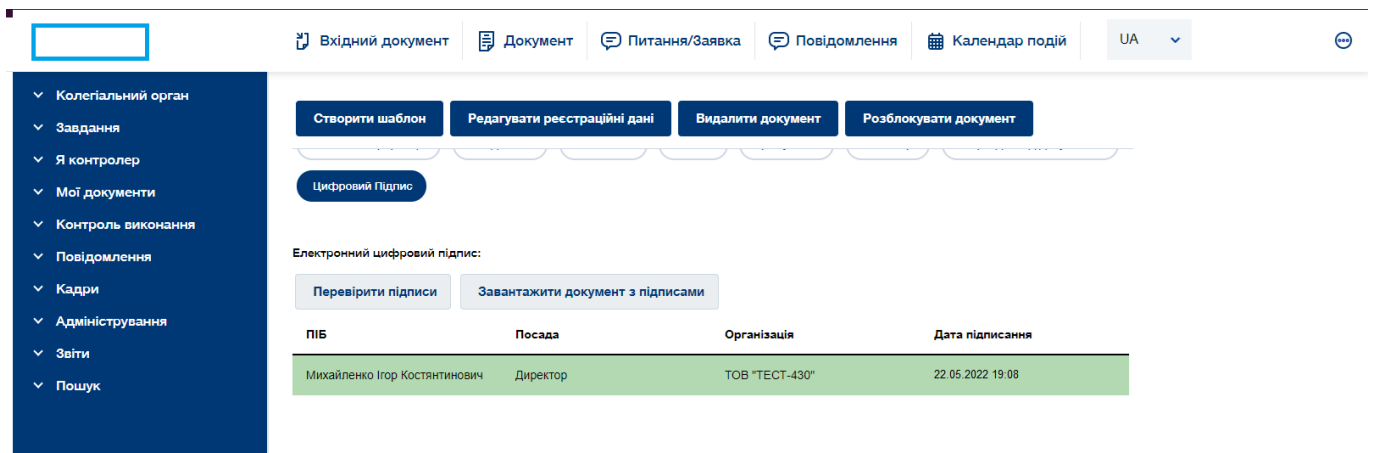


Fig. 3.17. Verified digital signature

When the document is signed, the addressee creates a resolution (if necessary), which can be seen in the Tasks tab, Resolutions to me.

The screenshot shows a web application interface for 'Резолюції мени' (Resolutions). The interface includes a sidebar with navigation options, a top navigation bar with filters and search, and a table of resolution items.

Назва завдання	Реєстраційний номер	Назва документа	Отримано	Тип документа	Вид документа
Виконання доручень згідно резолюції	42	Budget adjustment Approval (between Dpt) test	22.05.2022	Внутрішній документ	Реєстраційні документи

Fig. 3.18. Resolution

Then, the user to whom the resolution was sent clicks on the item - Execution of orders according to the resolution. As a result, the signing and life cycle of the document in the electronic document management system is completed.

CONCLUSION TO CHAPTER 3

The problem of information security is a very common and relevant topic both for conversations and for writing various applications, creating security tools. Information on the Internet and in various electronic systems is gaining more and more volume, this information may be different: available to each user, personal, late levels. The banking system is no exception, often documents that are processed in the document management system or in the electronic document management system, constantly need protection from unauthorized seizure or otherwise. Computer information processing technology poses certain threats that can lead to unwanted loss or temporary unavailability of important data.

If we talk about banks, the information circulating in the electronic document management system is very important for both the bank and its customers. For example, these are documents certifying the personal data of the client or the data of the company serviced by the bank, contracts and agreements, which once again confirms the fact and relevance of information protection.

CHAPTER 4

DEVELOPMENT OF THE ARCHITECTURE OF THE INFORMATION AND COMMUNICATION SYSTEM OF THE ONLINE BANKING

4.1 Presentation of electronic banking services

E-banking can be implemented in three main categories of e-commerce business models: business-to-consumer (B2C) (for example, a customer withdraws cash from his bank), business-to-business (B2B) (for example, funds transferred from one bank to the other) and from consumer to consumer (B2C) (for example, funds transferred between two customer accounts). One of the popular types of e-banking services in the B2C business model category are ATM-based banking, telebanking, SMS-based banking and Online banking.

ATM-based banking

An ATM is a virtual cashier of a bank that performs most of the cashier's tasks, including depositing / issuing cash, requesting a balance, displaying a statement, and so on. The number of ATMs in Ukraine is steadily declining: in 2020, banks withdrew 1,175 ATMs from their network. In addition, in the fourth quarter, state and foreign banks closed 205 branches (mostly Oschadbank - 94). Ukrgasbank opened the most branches (7).

In 2020, the number of bank branches decreased by 868 units, the largest in Dnipropetrovsk region (71). In the fourth quarter, banks, with the exception of private ones, continued to lay off employees: mostly foreign banks. In 2020, the number of full-time employees decreased by 5,000 people [24].

Tele-banking

To access telebanking services, customers need to dial a specific phone number provided by the bank. The identity of the client is confirmed by checking the PIN code or secret questions. Full service can be automated, although sometimes you can contact the operator. With telebanking, you can provide a range of banking services, including detailed

account information, balance request, product or service information, ATM card activation, checkbook services, bill payment, credit card services, and more.

SMS-based banking

SMS-banking is a type of mobile banking, a technological service that banks offer to their customers, which allows them to use selected banking services via their mobile phone via SMS-messages. SMS-banking services work both with the help of push-messages and messages. Push messages are messages that the bank decides to send to the customer's mobile phone without the customer initiating a request for information. Typically, push notifications can be either mobile marketing messages or notifications about an event that occurs in the customer's bank account, such as withdrawing a large amount from an ATM or a large payment by customer's credit card, and so on.

Online banking

Online banking began with the launch of banks' websites to provide customers with various banking information (for example, different types of accounts, deposit schemes, interest rates, foreign exchange rates, locations of nearby branches, etc.). Shortly after its creation, customer accounts were integrated and thus could work after proper customer authentication. Online banking, if implemented in full, will be highly appreciated by both customers and the bank's bodies. This will provide seamless, 24-hour, secure e-banking services from anywhere with a minimum cost. Through Internet banking, you can implement a number of banking services, including request for account balance, transfer of funds, opening or changing a term deposit account, request for a checkbook or payment order, request for exchange rate or interest rate, bill payment and more.

4.2 The use and importance of ICS in online banking

ICS means information and communication technologies that provide access to information through telecommunications and a diverse set of technological tools and resources used to communicate, create, disseminate, store and manage information.

ICS is a technology that consists of electronic devices and related interactive materials that allow the user to use them for a wide range of teaching and learning processes in addition to personal use.

Banks that use information and communication technologies include basic web portals and electronic databases, as well as composite information management systems aimed at improving management efficiency. And the use of information and communication technologies is a stimulus for economic growth. The real goal or task of information and communication technologies in the banking sector is not only to provide access to modern technologies, but also the role of ICS in the banking sector is to develop connecting communities in the long run.

Banks around the world are still trying to find a technological solution that meets the challenges of a rapidly changing environment and customer demand for products and services. New technological changes caused by the banking sector have a huge impact on bank officials, employees and customers. The development of technology allows the banking sector to provide banking products and services to customers more conveniently and successfully than ever before the banking products and services are delivered to the customer. Quick access to important information and the bank's ability to act quickly and effectively will distinguish successful banks of the future. The Bank is gaining a dynamic competitive advantage through the use of ICS and a responsible customer service environment, direct marketing and new streamlined business processes. Today, banks are aware of the need for customers who need new products and services, and plan to make them available to customers. ICS have intensified competition between banks and forced them to integrate new technologies to compete and satisfy their customers.

Information and communication technologies have played a significant role in the development of the banking sector for many years. ICS have made the banking sector more innovative and competitive through the development of information and communication technologies. The use of ICS in banking enables the banking sector to meet customer needs by strengthening their internal control systems.

Extensive use of ATMs, Internet banking, mobile banking, smart cards, 24/7 services, as well as the ability to offer a wide range of products and services have allowed banks to improve their services provided by the banking sector to customers [25].

4.3 Banking network architecture

Like other network institutions, the banking network must be equipped to communicate at two borders: the communication required between internal nodes and the interaction with external nodes. Figure 4.1 shows the architecture of a typical banking network, which deploys the various nodes required to provide electronic banking services.

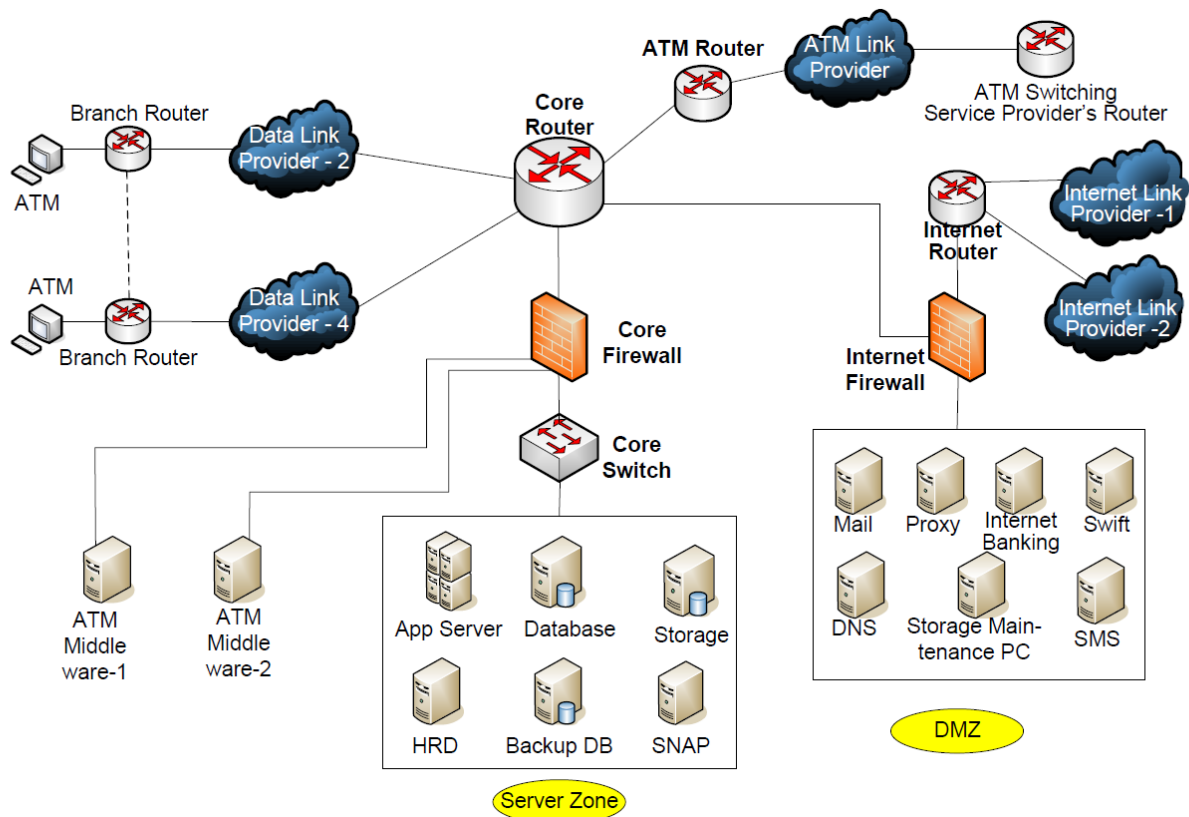


Fig. 4.1. The architecture of the banking network

For electronic transactions that are restricted in the bank, the internal network is protected by the main firewall, which is connected to the main router. Various application servers, database servers, repositories, and network analysis tools (such as SNAP) are deployed in the server area. DMZ (Demilitarized Zone) deploys a number of servers called

by external organizations over the Internet. In general practice, confidential information and internal data of the bank are never disclosed within the DMZ.

ATMs are installed both in branches and on the street. The branch office and server area are connected through a private, secure point-to-point connection, which is shown as the network provider's network between the branch router and the main router in Figure 4.1. ATMs installed inside the branch connected to the server area through it are secure point-to-point connection.

The architecture of Online banking is shown in Figure 4.2.

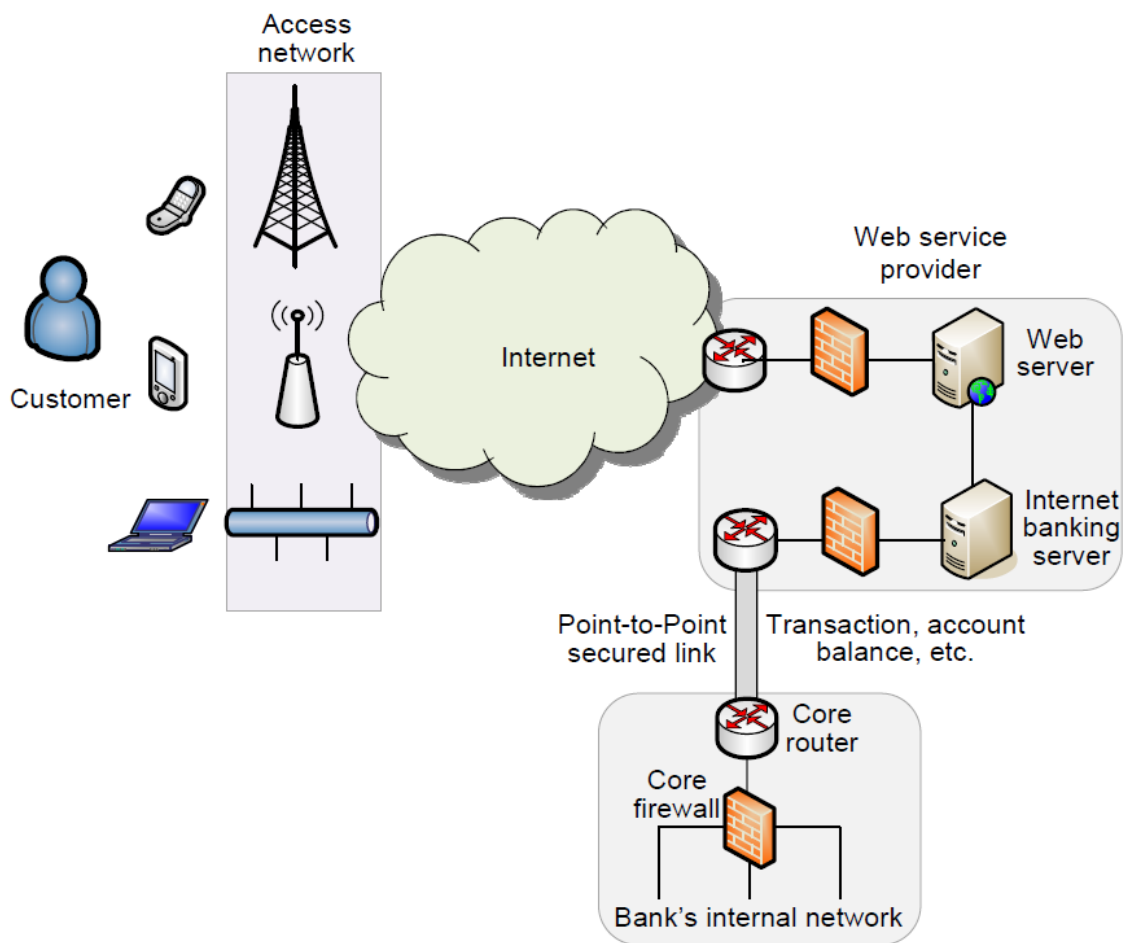


Fig. 4.2. The Online banking architecture

The Online banking customer can access the bank's website from any device that can connect to the Internet through the access network. In the web service provider's network, the web server contains the bank's website. The customer accesses the website through one

of the web browsers. The web service provider's network connects to the bank's network via a secure point-to-point connection. This connection can be provided by a third party. Through this secure private connection, the Online banking server (located between the web server and the bank's internal network) transmits confidential information that performs transactions, account balances, bill payments, and more. Therefore, information associated with a customer account is never transmitted through the supported public Internet and the security of the customer account.

4.4 Technical characteristics and cost of equipment used in the banking network

Core Router

It is designed to work in the backbone or core of the Internet. It supports several telecommunication interfaces with the highest speed and use mainly on the Internet. It can send IP packets at full speed to all of them. It supports the routing protocol used in the kernel. It will distribute Internet data packets within the network. But the kernel will not distribute Internet data packets between networks.

Core routers are commonly used by service providers (such as AT&T, Verizon, Vodafone) or cloud providers (such as Google, Amazon, Microsoft). They provide maximum bandwidth to connect additional routers or switches. Most small businesses do not need basic routers. But very large businesses that have many employees working in different buildings or locations can use core routers as part of their network architecture.

Core Router CCR1016-12G Mikrotik equipment was taken during the development of the banking network architecture.

Table 4.1

Specifications of CCR1016-12G

CPU	Tilera Tile-Gx16 CPU (16-cores, 1.2Ghz per core)
Memory	Two SODIMM DDR slots, 2x 1GB installed (no hw or software max limit)

Ethernet	Twelve 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X
Expansion	microUSB port, host and device mode
Storage	512MB Onboard NAND
Serial port	One DB9 RS232C asynchronous serial port
Extras	Reset switch; beeper; voltage, current and temperature monitoring; speed controlled fan
Power options	IEC C14 standard connector 110/220V, Power jack (BU model only) and Passive PoE 24V. PSU included in both models.
Board dimensions	355x145mm55mm
Temperature	Max ambient temperature 50° @ 1.2GHz; 70° @ 1GHz CPU core frequency
OS	MikroTik RouterOS v6 (64bit), Level 6 license
Included	CCR1016-12G: router in a 1U case with LCD, PSU, power cable, usb cable CCR1016-12G-BU: router, PSU, power cable, mounted LCD screen, usb cable

Core Switch

A core switch is a network switch installed on the basis of a multilayer network or a network with a hierarchy. These data switches are responsible for routing and switching data at the core network level. Data that is routed and switched by the core switch is transferred to lower levels of the network, such as the distribution and access layer. This means that the performance of the entire network depends on the data transmitted and switched by the main switch. Typically, multiple data switches are used at the base network level, so large amounts of data can be routed at the hierarchy level. Another reason to use multiple data switches at a basic level is to prevent data packets from accumulating. If data packets are very crowded at the distribution and access levels, the reverse flow of data can lead to a

malfunction of the primary layer. That is why the choice of basic high-capacity switches is important in hierarchical Ethernet networks.

Core Switch HP StorageWorks 8/40 AM870A equipment was taken during the development of the banking network architecture.

Table 4.2

Specifications of HP StorageWorks 8/40 AM870A

Targeted Environment	Workgroups, Departments
Port Bandwidth	8Gbit/sec
Aggregate device bandwidth	384 - 640 Gbit/sec end-to-end
Storage system support	XP, EVA, MSA
Ports	24 Enabled 40 Max
SFP	B-series
Advanced Trunking	Included with Power Pack+ or Optional Upgrade
Adaptive Networking	Included with Power Pack+ or Optional Upgrade
Form factor	1U
Zoning Software	Yes (Included)

ATM Router

ATM (Asynchronous Transfer Mode) is a high-performance network-based switching and multiplexing technology based on data transmission in the form of fixed-size micropackets (53 bytes), of which 5 bytes are used for the header. This is different from

Internet Protocol or Ethernet, which uses packets or frames of variable size. ATM provides channel-level services using a wide range of means of communication at the physical level.

ATM Router WL-R100LF1 equipment was taken during the development of the banking network architecture.

Table 4.3

Specifications of WL-R100LF1

Supports Mobile network	FDD / TDD 4G DC-SHPA+/SHPA+/SHPA/SHDPA/WCDMA/UMTC EDGE/GPRS CDMA2000 EVDO/CDMA 1X
Interface	1×10/100 Mb LAN interface 1×RS-232 console port 2×SMA-K antenna interface 1×Standard SIM/R-UIM interface 1×Standard DC power interface
Route protocol	RIPv2/OSPF dynamic route
Device management	Local or remote web browser CLI/Telnet command M2M management platform SSH configure
Firewall & Filter	IP packet/Domain/MAC filter NAT DMZ
Ethernet Standard	IEEE 802.3 IEEE 802.3u
Power supply	5 ~ 32VDC
VPN	IPSec PPTP/L2TP client GRE/IPIP

Branch Router

The term branch router usually refers to a router that exists in a remote branch of the enterprise network. They interact mainly with other network routers, which distinguishes them from end-to-end routers. However, they do this from a remote branch, which distinguishes them from the main routers, which mainly route information in centralized subnets. A remote branch can be defined as a part of a network that has been segmented by a virtual local area network (VLAN) or as one local area network. Branch routers often exist on remote sites on the edge of the WAN and connect to the corporate LAN. Many vendors that sell branch routers integrate multiple services into one platform, eliminating the need for additional equipment to run their product.

Branch Router Cisco C8200L-1N-4T equipment was taken during the development of the banking network architecture.

Table 4.4

Specifications of Cisco C8200L-1N-4T

Slots	1 NIM 1 PIM
Memory (DRAM)	4 GB
IPv4 forwarding throughput (1400 bytes)	Up to 3.8 Gbps
Number of IPv4 routes	800,000 with default 4 GB, up to 4M with 32 GB
Number of IPv6 routes	800,000 with default 4 GB, up to 4M with 32 GB
Number of queues	16,000
Number of Network Address Translation (NAT) sessions	600,000 with default 4 GB, up to 2M with 32 GB

Internet Router

A router is a network device that transmits data packets between computer networks. Routers perform the functions of directing traffic on the Internet. Data sent over the Internet,

such as a web page or e-mail, takes the form of data packets. The packet is usually forwarded from one router to another router through the networks that make up the network until it reaches the destination node.

The router is connected to two or more data lines from different IP networks. When a data packet arrives on one of the lines, the router reads the network address information in the packet header to determine the final destination. Then, using the information in its routing table or routing policy, it forwards the packet to the next network on its way.

Internet Router TP-Link Archer C80 equipment was taken during the development of the banking network architecture.

Table 4.5

Specifications of TP-Link Archer C80

WAN port	Ethernet
Interfaces	1 x WAN 10/100/1000 Mbit/s 4 x LAN 10/100/1000 Mbit/s
Wi-Fi speed standard	AC1900
Wi-Fi standards	802.11 g/n/ac
Maximum Wi-Fi speed	1.3 Gbps
Maximum speed of LAN ports	1 Gbps
Wi-Fi frequency	2.4 GHz and 5 GHz (dual band)
Protocol support	PPPoE, L2TP, PPTP, DHCP
Information protection	WPA, WPA2, WEP, WPA-Enterprise, WPA2-Enterprise

Calculation of the cost of equipment for the architecture of the bank's network

To develop the architecture of the banking network, we need to buy 64 Core routers, 150 Core switches, 500 ATM routers, 1500 Branch routers and 1 Internet router. The cost of this equipment is given in Table 4.6.

Table 4.6

The cost of equipment for the banking network

Device type	The price of the device	The total cost of the required number of devices
Core router (CCR1016-12G Mikrotik)	21 164 UAH	1 354 496 UAH
Core switch (HP StorageWorks 8/40 AM870A)	23 167 UAH	3 475 050 UAH
ATM router (WL-R100LF1)	12 120 UAH	6 060 000 UAH
Branch router (Cisco C8200L-1N-4T)	7000 UAH	1 050 000 UAH
Internet router (TP-Link Archer C80)	1750 UAH	1750 UAH

Taking into account the cost of the equipment presented in Table 4.6, we can say that to create the architecture of the banking network you need to spend at least 11941296 hryvnias. Also, we should not save on this equipment, because it provides continuous network operation and protection of information stored on bank servers.

CONCLUSION

In the course of the thesis the information - communication system of online banking was considered and the protection of information in the electronic document management system of the banking institution was analyzed.

The dynamic development of information and communication technologies in recent years has significantly changed the banking industry. Technology provides new benefits and opportunities for banks to expand their customer base and reduce costs while offering customers a more convenient way to access their products and services. Issues of understanding the direction of development of modern banking technologies and the possibility of their effective implementation in banking are relevant for all banking institutions. Their introduction into the bank's activities will determine not only the profits and competitiveness of the bank in the market of financial and banking services, but also its operation in general.

Online banking is a new form of banking that complements and restores its traditional concept by providing electronic access via the Internet. It provides for the possibility of carrying out several banking operations without the need for a physical branch for this purpose.

Almost all traditional banks already have Internet banking. They have taken advantage of the rapid growth of this type of service in recent years and saw this as another way to expand their business. Thus, they seek to reach new consumers, mainly for the younger population.

The problem of information protection is considered. Nowadays, this is a very common and relevant topic both for conversations and for writing various applications, creating protection tools. Information on the Internet and in various electronic systems is gaining more and more volume, this information may be different: available to each user, personal, late levels. The banking system is no exception, often, documents that are processed in the document management system or in the electronic document management system constantly need protection from unauthorized seizure or other. Computer

information processing technology poses certain threats that can lead to undesirable losses or temporary unavailability of important data.

Speaking of banks, the information circulating in the electronic document management system is very important for both the bank and its customers. For example, these are documents that certify the personal data of the client or the data of the company served by the bank, contracts and agreements, which once again confirms the fact and relevance of information protection.

The structure of information protection systems has been determined, protection has been organized on the basis of delimitation of access rights to a certain system or information.

In the electronic document management system of the banking institution, as shown above, there are different ways to work with the document, these are: sending the document for approval with signing in the system, for approval with signing on paper, signing in the system, signing on paper, transfer to archive document. The signing or approval of the document is sent to specific users, or can be sent to one who is included in different groups with different access rights. In case of signing the document, it is possible to verify the authenticity of the digital signature and who signed the document.

Thus, it was demonstrated how to create a document in the electronic document management system, its signing or possible approval of the document and added users with different access rights in groups.

The architecture of the banking network and the architecture of the online bank with a description of the connection and operation of banking equipment were also developed.

The total cost of equipment were calculated, which is needed on average to develop the architecture of the banking network for full and continuous operation.

REFERENCES

1. Сербина О. Г. Інтернет-банкінг: українська практика та світовий досвід / О. Г. Сербина, О. М. Загурова., 2014. – 125 с. – (Молодий вчений).
2. Міщенко В. І. Банківські операції / В. І. Міщенко, Н. Г. Слав'янська, О. Г. Коренєва., 2016. – 796 с. – (Знання). – (2).
3. Шпильовий В. А. Підходи до класифікації банківських послуг / В. А. Шпильовий // Економіка та держава / В. А. Шпильовий., 2016. – С. 27–30.
4. Мошенець О. В. Фінансовий ринок України / О. В. Мошенець // Інноваційні продукти і технології на ринку банківських послуг / О. В. Мошенець., 2014. – С. 7–8.
5. Страхарчук А. Я. Інформаційні системи і технології в банках / А. Я. Страхарчук, В. П. Страхарчук., 2014. – 515 с.
6. Михайлюк Г. О. Розвиток Інтернет-банкінгу як нетрадиційної банківської операції [Електронний ресурс] / Г. О. Михайлюк – Режим доступу до ресурсу: http://www.rusnauka.com/1_KAND_2010/Pravo/9_57264.doc.htm.
7. Деменков М. Інтернет-технології в обслуговуванні клієнтів банку / М. Деменков // Банківська справа / М. Деменков., 2015. – С. 58–64.
8. Інструкція про безготівкові розрахунки в Україні в національній валюті [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: <http://zakon4.rada.gov.ua/laws/show/z0377-04>.
9. Огієнко В. І. Інтернет-банкінг як перспективний напрям розвитку ринку фінансових послуг [Електронний ресурс] / В. І. Огієнко. – 2016. – Режим доступу до ресурсу: <http://www.economy.nauka.com.ua/?op=1&z=1217>.
10. Чуб О. О. Розвиток інтернет-банкінгу в глобальному середовищі / О. О. Чуб // Вісник Української академії банківської справи / О. О. Чуб., 2016. – С. 62–67.
11. Засадна Х. О. Про захист послуг Інтернет-банкінгу / Х. О. Засадна // Вісник університету банківської справи національного банку України / Х. О. Засадна., 2015. – С. 225–229.

12. How to Make a Banking App [Електронний ресурс] // 2019 – Режим доступу до ресурсу: <https://stormotion.io/blog/how-to-create-an-online-banking-app/>.

13. How to start a Digital bank: 9 things you need to know [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: <https://gearheart.io/articles/9-things-you-need-know-starting-digital-bank/>.

14. IBM Systems Solution for Branch Banking: Installation guide [Електронний ресурс] – Режим доступу до ресурсу: www.redbooks.ibm.com/redbooks/pdfs/sg247396.pdf.

15. Infosys Finacle Core Banking Solution on Oracle Super Cluster and Oracle SPARC T-Series Servers [Електронний ресурс] – Режим доступу до ресурсу: <http://www.oracle.com/technetwork/server-storage/hardware-solutions/o13-063-infosys-finacle-2014261.pdf>.

16. Convergence drives improved efficiency, enhanced customer service and business growth [Електронний ресурс] – Режим доступу до ресурсу: http://www.btireland.com/casestudy_danske.shtml.

17. Cybersecurity in Digital Banking: Threats, Challenges and Solution [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://enterslice.com/learning/cybersecurity-in-digital-banking-threats-challenges-and-solution/>.

18. Безпека Інтернет-банкінгу в Україні: практичні аспекти [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_v_ukrayini_praktichni_aspekti.

19. Online banking security software [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://www.comarch.com/cyber-security/articles/online-banking-security-software-what-do-the-banks-use/>.

20. Information security of Internet banking [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: <https://raiffeisen.ua/en/data-protection/informacijna-bezpeka-internet-bankingu>.

21. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

22. Example of VLAN integration [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://studopedia.su/5_26610_priklad-obiednannya-VLAN.html.

23. Preventing Windows Storage in Active Directory Databases and Local SAM Databases [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: <https://docs.microsoft.com/ru-ru/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password>.

24. Comparison of the number of ATMs and PIC terminals in Ukraine [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://www.ukrinform.ua/rubric-economy/3192589-v-ukraini-torik-pomensalo-bankomativ-natomist-zroslo-kilkist-posterminaliv-nbu.html>.

25. What is ICT How ICT Has Transformed in Banking World [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: <https://medium.com/@mabdulbasit01/what-is-ict-how-ict-has-transformed-in-banking-world-2813b7b7d383>.